Journal of Law and Technology at Texas

Volume 4 Spring 2020 Pages 1 to 70

Published by The University of Texas School of Law

First printing, 2020.

JOURNAL OF LAW AND TECHNOLOGY AT TEXAS

Volume 4 • Spring 2020

THE POTENTIAL OF HEALTH DATA: EXPLORING CONSUMER GENERATED DATA AND THE BIG DATA ECOSYSTEM

AND

CONSTRAINING THE CYBERMOB: USING A DOXING NOTICE AND TAKEDOWN REGIME TO OPTIMIZE THE SOCIAL UTILITY OF SOCIAL SHAMING

Staff Editors (cont'd)

JULIE BALOGH
CHARLIE BLAND
MELITA CHAN
KYLE CLENDENON
KELLY COMBS
ZACHARY ANDREW COPLEN
PRONOMA DEBNATH
ROY FALIK
MELANIE FROH
ADRIENN ILLESH
RICHA KALOLA
ELIZABETH KNUPPEL
CHELSEA LAUDERDALE
AUSTIN LEE
LEO LI
ANDREW LING
NICK MARKWORDT
BRANDON MAXWELL
KATE NELSON
GRAHAM POUGH
JACOB PRZADA
SHLOKA RAGHAVAN
GABRIELLA REGARD
SYDNEY SALTERS
PATRICK SIPE
WHITNEY WENDEL
PATRICK WROE
ZACH ZHAO

TABLE OF CONTENTS

THE POTENTIAL OF HEALTH DATA: EXPLORING CONSUMER GENERATED DATA AND THE BIG DATA ECOSYSTEM

Elijah Roden

TABLE OF CONTENTS

I. INTRODUCTION

In an industry study performed by Aruba Networks, 87% of healthcare companies will have integrated connected devices, typically referred to as the Internet of Things ("IoT") by the end of 2019.[1] Healthcare organizations use devices for patient monitoring, maintenance, energy meters, imaging devices, remote operation and monitoring, and location services[2] through internally embedded medical devices,[3] wearable external medical devices,[4] assisting accessories,[5] or stationary medical devices.[6] Beyond healthcare organizations, innovations are appearing in consumer wearable devices, from smart watches[7] and "lifestyle remote[s]"[8] to sleep tracking headbands[9] and stress tracking patches,[10] providing a variety of health benefits. Mobile applications (hereinafter "apps"), like those on the Apple App Store and Google Play, are spreading prolifically as individuals download them to their smartphones, tablets, and smart watches, and the data these apps share with third parties, in many cases, is remarkably similar to the Protected Health Information ("PHI") collected by healthcare organizations. Yet, the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and

---

1 *87% of Healthcare Organizations Will Adopt Internet of Things Technology by 2019,* HIPAA J. (Mar. 1, 2017), https://www.hipaajournal.com/87pc-healthcare-org.anizations-adopt-internet-of-things-technology-2019-8712.

2 *Id.*

3 JASON HEALEY ET AL., ATL. COUNCIL, THE HEALTHCARE INTERNET OF THINGS REWARDS AND RISKS 7 (2015).

4 James P. Dieffenderfer et al., *Wearable Wireless Sensors for Chronic Respiratory Disease Monitoring,* 2015 IEEE 12TH INT'L CONFE. WEARABLE & IMPLANTABLE BODY SENSOR NETWORKS (BSN) (2015).

5 Kyu Jin Cho & H. Harry Asada, *Wireless, Battery-less Stethoscope for Wearable Health Monitoring,* PROC. IEEE 28TH ANN. NORTHEAST BIOENGINEERING CONF. 187 (2002).

6 HEALEY ET AL., *supra* note 3, at 7.

7 *See* Adam Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J. L. & TECH. 6 (2015).

8 Rachel Metz, *The Internet of You,* MIT TECH. REV. (May 20, 2014), https://www.technologyreview.com/s/527386/the-internet-of-you.

9 Sam Draper, *Sleep Trackers Took the Center Stage at the IFA 2018 in Berlin,* WEARABLE TECHNOLOGIES (Sept. 12, 2018), https://www.wearable-technologies.com/2018/09/sleep-trackers-took-the-center-stage-at-the-ifa-2018-in-berlin.

10 Cathy Russey, *These Smart Patches Monitor Your Stress to Help You Lead a Happier, Healthier Life,* WEARABLE TECHNOLOGIES (Nov. 30, 2018), https://www.wearable-technologies.com/2018/11/these-smart-patches-monitor-your-stress-to-help-you-lead-a-happier-healthier-life.

Clinical Health Act ("HITECH") statutes typically applicable to the management of health information are largely inapplicable to consumer medical devices or mobile apps.[11] Ultimately, this inapplicability results in a largely unrestricted market of data processing and data collection, and consumers face extreme difficulty in understanding who processes their data and for what purposes. This danger extends beyond the information gathered at the point of collection as data analytics companies can utilize this information to hone their analytics tools and gain actionable insights into the lives of the subjects of the data they collected. Given the lack of transparency surrounding data collection and processing, the personal information collected in addition to the insights gathered can be used to make decisions affecting consumers who are largely unaware of the decisions being made about them. While some of these decisions may violate the law, the current framework in the United States for data privacy and processing does not provide individuals with sufficient methods to detect such illegal processing, and even if it does, "[T]here are ample pretexts to mask suspect or illegal behavior."[12]

Accordingly, this paper will be divided into three main parts. First, it will explore the general legal framework that applies to information privacy in the United States, the implementation and enforcement of HIPAA and HITECH, and the role that the Federal Trade Commission ("FTC") plays in privacy enforcement. Second, it will illustrate how data sharing occurs in practice, highlighting the degree of third-party involvement, and third, discuss potential real-world consequences of unprotected data collection for users.

II. PRIVACY LAWS AND REGULATIONS

Though there has been discussion of a trans-substantive privacy law in the United States,[13] akin to Europe's General Data Privacy Regulation, it is not clear whether or not there will be any forceful push for legislative reform in the area of privacy and cybersecurity. Absent any substantive

---

[11] *See* Jennifer R. Flynn, *Break the Internet, Break the Stigma: The Promise of Emerging Technology & Media in Mental Health*, 20 QUINNIPIAC HEALTH L. J. 1, 36 (2017).

[12] Frank Pasquale, *Redescribing Health Privacy: The Importance of Health Policy*, 14 HOUS. J. HEALTH L. & POLICY 95, 108 (2014) [hereinafter Pasquale, *Redescribing Health Privacy*].

[13] Press Release, U.S. Chamber of Commerce, U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Fed. Privacy Law (Feb. 13, 2019), https://www.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law.

reform, the United States operates under a sectoral privacy regime, in which a myriad of laws and regulations apply to different industries in different ways with different protections. The enforcement obligations of these laws are shared or divided between federal agencies, state agencies, and private parties. For example, The Gramm-Leach-Bliley Act ("GLBA") requires financial institutions, or companies that offer consumer financial products and services, to explain their information-sharing provisions and safeguard such data.[14] Enforcement of the GLBA is performed by "the FTC, the federal banking agencies, other federal regulatory authorities, and state insurance authorities . . . ."[15] Similarly for private parties, the Video Privacy Protection Act ("VPPA") enables consumers to pursue a private right of action against a service provider who "knowingly discloses, to any person, personally identifiable information" concerning the consumer's rental history.[16] Although the VPPA enables private rights of action,[17] most privacy statutes rely only on government enforcement. State-specific data privacy laws, like data breach notification laws,[18] are typically ineffective, though California's Consumer Privacy Act of 2018 ("CCPA") may change that inefficacy in 2020.[19] Still, such privacy laws enable state Attorneys General to pursue companies when they breach the representations they make to consumers.[20]

While this sectoral approach enables both personal information and industry to be regulated in a more nuanced way that focuses on particular needs, it can create unnecessary complexity and uncertainty; it also leaves

---

[14] *Gramm-Leach-Bliley Act*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act (last visited Feb. 17, 2020).

[15] FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT: A GUIDE FOR SMALL BUSINESS FROM THE FEDERAL TRADE COMMISSION 14 (July 2002), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

[16] Video Privacy Protection Act § 2(a)(2), 18 U.S.C. § 2710 (2018).

[17] *Id.*

[18] *State Breach Notification Laws*, NAT'L. CONF. ST. LEGISLATURES (Mar. 8, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[19] *See* Rachael Myrow, *California Rings in the New Year With a New Data Privacy Law*, NPR (Dec. 30, 2019, 9:00 AM), https://www.npr.org/2019/12/30/791190150/california-rings-in-the-new-year-with-a-new-data-privacy-law.

[20] *See, e.g.*, *Privacy Enforcement Actions*, OFF. CAL. ATT'Y GEN., https://oag.ca.gov/privacy/privacy-enforcement-actions (last visited Apr. 11, 2020). However, this paper will primarily focus on the FTC as the de facto privacy regulator.

large areas of the economy unaddressed by statute.[21] There is no federal privacy statute governing data collection by Facebook, Amazon, or Google, nor is there a federal privacy statute on the use of data by merchants, such as Walmart or Target.[22] The lack of a federal statute covering a specific industry does not mean that it is entirely unregulated. Through § 5 of the Federal Trade Commission Act, the FTC enforces privacy policies and advertisements put forth by companies by asserting that violations of representations made by the companies are deceptive trade practices.[23] Mobile apps are usually not covered by a sectoral privacy statute, such as HIPAA,[24] so the regulation of that information falls primarily to the FTC's privacy policy enforcement.

a. HIPAA and HITECH Are Too Narrow in Scope

HIPAA and HITECH and their associated regulations (hereinafter, collectively "HIPAA") contain provisions that apply to the use, processing, and storage of health-related information, even though HIPAA was not initially designed to be a data privacy and security statute.[25] Given the importance of healthcare, the drafters of HIPAA sought to modernize the healthcare profession by enabling the electronic transmission of health information, and in the process of drafting the statute, realized the potential harms inherent in electronic transmissions, causing them to add in privacy and security provisions.[26]

---

[21] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

[22] Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?,* N.Y. TIMES (Nov. 2, 2019), https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html.

[23] *See* FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE, LAW ENFORCEMENT, AND RULEMAKING AUTHORITY § II.1 (Oct. 2019), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[24] INST. OF MED. OF THE NAT'L ACADS., BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH 157–58 (Sharyl J. Nass et al. eds, 2009), https://www.ncbi.nlm.nih.gov/books/NBK9578/pdf/Bookshelf_NBK9578.pdf.

[25] Jordan Harrod, *Health Data Privacy: Updating HIPAA to Match Today's Technology Challenges*, SCI. IN THE NEWS, HARV. UNIV. (May 15, 2019), http://sitn.hms.harvard.edu/flash/2019/health-data-privacy.

[26] INST. OF MED. OF THE NAT'L ACADS, *supra* note 24, at 155 (explaining that "[a]lthough privacy protections were not a primary objective of the Act, Congress recognized that

Under HIPAA, only "individually identifiable health information" that is "(i) transmitted by electronic media, (ii) maintained in electronic media, or (iii) transmitted or maintained in any other form or medium" is PHI under the scope of the Privacy Rule.[27] Individually identifiable health information is information that relates to the condition of an individual, provision of healthcare, or payment of healthcare, which identifies or could potentially identify an individual.[28] However, the Privacy Rule only applies to "covered entities" and "business associate[s]."[29] "If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with the HIPAA Rules."[30]

The Privacy Rule imposes a number of restrictions on the uses and disclosures of PHI. As a general rule, a covered entity may only use or disclose PHI to the individual for the payment or provision of services or to a business associate with appropriate safeguards and contracts.[31] Certain uses or disclosures, however, are prohibited outright, such as the use of genetic information to determine eligibility for benefits, compute a premium, exclude based on preexisting conditions, or make a plan renewal.[32] Similarly, the sale of PHI to a third party is typically prohibited, but a covered entity may do so if they obtain consent that specifically mentions the sale and payment to the covered entity.[33]

---

advances in electronic technology could erode the privacy of health information, and included the privacy provision in HIPAA").

27 45 C.F.R. § 160.103 (2019).

28 *Id.*

29 *Id*. (explaining that Covered Entities are health care providers, health plans, and health care clearinghouses that electronically transmit health information in the course of their normal health care practices. Health care providers include doctors, clinics, psychologists, chiropractors, nursing homes, and pharmacies; a health plan includes health-insurance companies, HMOs, company health plans, and government programs that pay for health care, such as Medicare and Medicaid. A health care clearinghouse includes entities that process nonstandard health information they receive from another entity into a standard form. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity, through benefit management, data aggregation, or cloud hosting services).

30 *Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Apr. 16, 2015), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

31 45 C.F.R. § 164.502 (2019).

32 *Id*.

33 45 C.F.R. § 164.508 (2019).

Finally, the "Privacy Rule also confers rights on individuals with respect to their PHI."[34] Individuals have a right to receive notice of privacy practices, specifically information regarding "the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information."[35] Section 164.522 enables individuals to "request restriction of uses and disclosures."[36] However, the covered entity is only required to agree to the restriction if either "the disclosure is for the purpose of carrying out payment or healthcare operations and is not otherwise required by law" or the PHI "pertains solely to a health care item or service for which the individual, or person . . . on behalf of the individual, has paid the covered entity in full."[37]

Though the Privacy and Security Rule in HIPAA initially represented a genuine exercise to protect the confidentiality, availability, and integrity of patient data,[38] technological innovation has exposed the systemic issues within HIPAA's statutory and regulatory framework. The generation and use of health information extends beyond covered entities. Even as mobile devices proliferate through society, the use of apps by users to monitor their own health, increase their exercise performance, or store other sensitive health information still is not covered by HIPAA.[39] Similarly, at-home paternity tests, genetic testing like 23andMe, and online repositories also fall outside the scope of jurisdiction of the Department of Health and Human Services ("DHHS"), which meant that when a woman found the results of her at-home paternity test easily accessible in a directory online, DHHS could do nothing about it.[40] Thus, in its current state, the bulk of privacy regulation for these services falls to the FTC.

---

34 INST. OF MED. OF THE NAT'L ACADS,, *supra* note 24, at 160.

35 45 C.F.R. § 164.520(a)(1) (2019).

36 45 C.F.R. § 164.522 (2019).

37 *Id.*

38 *See* Karen Colorafi & Bryan Bailey, *It's Time for Innovation in the Health Insurance Portability and Accountability Act (HIPAA)*, JMIR MED. INFORMATICS, Oct.–Dec. 2016, at e34.

39 Latena Hazard, *Is Your Health Data Really Private? The Need to Update HIPAA Regulations to Incorporate Third-Party and Non-Covered Entities*, 25 CATH. U. J. L. & TECH. 447, 457–58 (2017).

40 Charles Ornstein, *Privacy Not Included: Federal Law Lags Way Behind New Health-Care Technology,* PAC. STANDARD MAG. (June 14, 2017), https://psmag.com/social-justice/privacy-not-included-federal-law-lags-way-behind-new-health-care-technology ; Letter from Kurt T. Temple, Assoc. Deputy Dir. for Reg'l Operations, Dep't. of Health & Hum.

b. The Federal Trade Commission as a Catch-All

i. The Federal Trade Commission as a Regulator

The mission of the FTC is to protect "consumers and competition by preventing anticompetitive, deceptive, and unfair business practices" through legal action, promote consumer choice, and increase education while encouraging business activity.[41] The roles privacy and security play in commerce have grown tremendously with the advent of information technology. In the past decade, the FTC has sought to address this through § 5 of the FTC Act, which enforces a company's privacy policies through its ability to regulate unfair and deceptive trade practices.[42] Misleading statements or omissions to consumers, including statements about data privacy, may expose the company to litigation or action from the FTC.[43]

In 2013, for example, the FTC filed suit against LabMD, asserting that a lapse in security measures allowed an employee to install an external peer-to-peer file-sharing program called LimeWire on a company computer.[44] A LabMD company computer's "My Documents" folder contained the personal information of approximately 9,300 consumers and was available to LimeWire.[45] While the FTC ultimately lost on appeal in 2018 for reasons related to the scope of the FTC's order,[46] the case serves as an example of the FTC using its authority to enforce privacy policies against HIPAA-covered entities.[47]

Serv., to Jacqueline Stokes (June 5, 2015), *available at* https://www.documentcloud.org/documents/2511636-hhs-stokes.html.

41 *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc (last visited Apr. 2, 2020).

42 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L. REV. 583, 599 (2011).

43 Hazard, *supra* note 39, at 464.

44 *In re* LabMD, Inc., No. 9357 (F.T.C. Nov. 13, 2015) (initial decision), https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf.

45 *Id.* at 24–25.

46 Diane Bartz, *U.S. Agency Loses Appeal Over Alleged LabMD Data Security Lapses*, REUTERS (June 6, 2018, 4:43 PM), https://www.reuters.com/article/us-ftc-datasecurity-labmd/u-s-agency-loses-appeal-over-alleged-labmd-data-security-lapses-idUSKCN1J22XD.

47 Kirk Nahra, *Takeaways from the 11th Circuit FTC v. LabMD Decision,* IAPP (June 7, 2018), https://iapp.org/news/a/takeaways-from-the-11th-circuit-ftc-vs-labmd-decision.

Given the FTC's role in enforcing and administering more than 70 laws, including the Children's Online Privacy Protection Act ("COPPA"),[48] the Fair Credit Reporting Act ("FCRA"),[49] and the Identity Theft Act,[50] as well as its use of the FTC Act to enforce privacy policies, the FTC is the primary source of regulation for this area.[51] The vast majority of actions brought against companies for violations of their own privacy policies settle, but the settlement agreements nevertheless form a unique body of law and standards, not unlike common law.[52] Companies look to these settlement agreements to guide their actions, enabling the FTC to become the "most influential regulating force on information privacy in the United States—more so than nearly any privacy statute or common law tort."[53]

ii. Privacy Policies as Enforcement Mechanisms and Consumer Education

Privacy policies typically focus on the disclosure of how an entity handles consumer data by making certain representations and promises to consumers; unlike an entity's terms of use, which are contracts of adhesion, privacy policies are rarely enforced as contracts.[54] While some laws require certain institutions to provide privacy policies to consumers,[55] the bulk of privacy policies arose through norms and consumer expectations as consumers began to worry about the use of their data online.[56] Privacy policies were a way to maintain self-regulation in light of Congressional attention.[57] In 1998 "only 2% of all websites had some form of privacy policies," and by 2001, "virtually all of the most popular commercial websites had privacy notices, with the number continuing to increase through 2005."[58] Within these policies, the issue is largely a matter of "procedure rather than

---

48 Children's Online Privacy Protection Act § 1302, 15 U.S.C. §§ 6505(a) (2020).

49 Fair Credit Reporting Act § 601, 15 U.S.C. § 1681 (2018).

50 18 U.S.C. § 1001 (2018).

51 *See Enforcement,* FED. TRADE COMM'N, https://www.ftc.gov/enforcement (last visited Apr. 2, 2020).

52 Solove & Hartzog, *supra* note 42, at 586.

53 *Id.* at 587.

54 *Id.* at 589.

55 *Id.* at 587.

56 *See id.* at 593–94.

57 *Id.*

58 Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control of Personal Information?*, 111 PENN. ST. L. REV. 587, 593 (2007).

substance."[59] The question is whether the company properly disclosed its policy to the consumer, not if the company can sell or manage data the way it currently does.[60] There are no laws that "regulate the substance of that policy" unless it pertains to a specific type of data or institution, such as HIPAA,[61] COPPA,[62] GLBA,[63] FCRA,[64] and the California Online Privacy Act.[65]

One argument in favor of privacy policies and self-regulation, that the business provides notice and choice to the consumer, is known as the "notice and choice model." The business gives the customer notice by communicating their information disclosure and management practice through their privacy policy. Then, customers can make informed choices about whether to purchase products, visit websites, or trust businesses. This argument favors self-regulation and is inherently skewed in favor of the business. Consumers rarely take the time to read the privacy policies, terms and conditions, or other documents associated with the websites, products, or other services they utilize. In 2008, scholars estimated that it would take the average American 244 hours per year to read all of the privacy policies on the websites they visited.[66] But that was at a time when Facebook only had 100 million users,[67] smartphones were just taking off,[68] and IoT devices had not entered mainstream adoption.[69] Today, in *Contracting for the Internet of Things,* Guido Noto La Diega and Ian Walden highlight that a consumer purchasing a Nest digital thermostat would have to read 13 different legal documents in order "to have a comprehensive picture of the rights,

---

59 *Id.* at 597 n.57 (citing Juliet M. Moringiello & William L. Reynolds, *Survey of the Law of Cyberspace: Internet Contracting Cases 2004-2005*, 61 BUS. LAW. 433, 434 (2005)).

60 *See id.* at 597.

61 *See* 42 U.S.C. § 1320d (2018).

62 *See* 15 U.S.C. §§ 6501–6506.

63 *See* Gramm-Leach-Bliley Act §§ 501–509, 15 U.S.C. §§ 6801–6809 (2018).

64 *See* 15 U.S.C. § 1681.

65 James Graves, *An Exploratory Study of Mobile Application Privacy Policies*, TECH. SCI. (Oct. 30, 2015), https://techscience.org/a/2015103002.

66 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J. L. & POL'Y. FOR INFO. SOC'Y. 543, 563 (2008).

67 Jefferson Graham, *5 Top Ways Tech Has Changed Since 2008,* USA TODAY (Nov. 13, 2016, 10:32 AM), https://www.usatoday.com/story/tech/2016/11/13/5-top-ways-tech-has-changed-since-2008/93527624.

68 *Id.*

69 *Internet of Things (IoT) History,* POSTSCAPES, https://www.postscapes.com/internet-of-things-history (last visited Apr. 2, 2020).

obligations and responsibilities of the various parties in the supply chain."[70] Yet, once Nest discloses information to a third party, the use of the information "will be governed by the third party's privacy policy and not by Nest's privacy documentation."[71] In essence, the resulting web of documents necessary to understand the obligations, responsibilities, and rights of the relevant parties continues to expand. With no limitations on reselling information, the difficulties faced by consumers are highlighted when trying to understand how their data is collected, managed, and protected.

The effort to understand a company's disclosure practices is further complicated by the choice of language used in the policies. Phrases like "affiliates" or "third parties" are littered throughout privacy policies, but "only 7% define them."[72] Conditional language, such as "may" or "might" further obfuscates the meaning and intentions of the privacy policies and presents a challenge in understanding a company's information management practices.[73] Even if a consumer were to develop an adequate understanding of the legal obligations in the web of privacy policies, a review of practices within businesses "points to a sustained failure of business to provide reasonable privacy protections" or comply with their own privacy policies.[74]

In many instances, businesses do not adequately or accurately describe their data-sharing habits in their privacy policies. So even if a consumer were to read them, the consumer would still not be aware of the degree to which information is being shared. In 2013, Privacy Rights Clearinghouse conducted a study of 43 different health and fitness apps. They found that "the majority of the technical practices that [they] considered a risk to users' privacy were not accurately disclosed,"[75] and "39% of

---

[70] Guido Noto La Diega & Ian Walden, *Contracting for the 'Internet of Things': Looking into the Nest,* 7 EUR. J. L. & TECH., no. 2, 2016, at 1, 6.

[71] NEST, TERMS OF SERVICE § 3(c) (last updated Mar. 5, 2020), https://nest.com/legal/terms-of-service.

[72] Florencia Marotta-Wurgler, *Does "Notice and Choice" Disclosure Regulation Work? An Empirical Study of Privacy Policies* 5 (Univ. of Mich. L. Sch., L. & Econ. Workshop, Apr. 16, 2015), *available at* https://www.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf.

[73] *Id.*

[74] Haynes, *supra* note 58, at 610.

[75] LINDA ACKERMAN, PRIVACY RIGHTS CLEARINGHOUSE, MOBILE HEALTH AND FITNESS APPLICATIONS AND INFORMATION PRIVACY: REPORT TO CALIFORNIA CONSUMER

the free apps and 30% of the paid apps sent data to someone not disclosed by the developer either in the app or in any privacy policy . . . ."[76] In *Automated Analysis of Privacy Requirements*, researchers analyzed 9,050 mobile apps, and they found that only 1,461 adhered completely to their policy.[77]

Despite the lack of compliance or legal requirements on the substance of privacy policies, consumers often believe that privacy policies protect them, rather than just disclose specific practices.[78] For example, a report from the Annenberg Public Policy Center of the University of Pennsylvania "found that 75% of consumers believed that just because a site ha[d] a privacy policy, it is not allowed to sell to others the personal information customers disclosed to it."[79] A 2014 poll by Pew Research Center gave the following proposition on a survey: "When a company posts a privacy policy, it ensures that the company keeps confidential all the information it collects on users."[80] Fifty-two percent of those surveyed responded that this statement was true.[81] This misconception is likely "compounded by the fact that most people skip over the privacy policies or take too little time to read them in enough depth to extract their intended meaning."[82]

Though our current notice and choice paradigm has its benefits, it succeeds only when two conditions are satisfied. First, consumers need to be aware of how their information is being collected, managed, and sold to others. A companies' lack of transparency makes it difficult, and when companies make disclosures, the disclosures are not effective. The disclosures

---

PROTECTION FOUNDATION 22 (July 15, 2013), *available at* https://privacyrights.org/sites/default/files/pdfs/mobile-medical-apps-privacy-consumer-report.pdf.

[76] *Id.* at 5.

[77] Sebastian Zimmeck et al., *Automated Analysis of Privacy Requirements for Mobile Apps*, 2016 AAAI FALL SYMP. SERIES, 2016, at 286, 294, *available at* https://www.aaai.org/ocs/index.php/FSS/FSS16/paper/download/14113/13704.

[78] *See* Haynes, *supra* note 58, at 611.

[79] *Id.* (citing JOSEPH TUROW ET AL., ANNENBERG PUB. POLICY CTR., UNIV. OF PA., OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE 3 (2005)).

[80] Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is,* PEW RESEARCH CTR. (Dec. 4, 2014), https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is.

[81] *Id.*

[82] Joseph Turow et al., *Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies, 2003-2015*, 62 J. BROAD. & ELEC. MEDIA 461, 463 (2018).

need to be accurate, clear, concise, and readable for the consumer. The complexity of modern data collection practices presents a unique problem, and the challenge of providing enough understandable, accurate information to make an informed decision without exhausting the reader is difficult even for the best drafters. However, thinking about privacy from the outset can provide huge returns in consumer education, such as through "just-in-time" disclosures.[83]

Second, notice and choice relies on the availability of actual choice in making the decision to utilize the service or not. Companies typically rely on a zero-sum approach to the use of data in which the protection or benefit of one party occurs at the expense of another.[84] In other words, choice, either to enable sharing or restrict certain uses, is viewed as a cost to the company because the company benefits from the ability to use the consumer's data. Companies then predicate the use of the product on the transfer of information in order to maximize their potential gain. When market competition is vibrant, this may not be an issue, as consumers can factor privacy into their choice of companies. However, network effects tend to reduce market competition,[85] and the commercialization of information incentivizes developers to monetize the information they can collect.[86] As more consumers gravitate towards a single platform, device, or app, the bargaining power of consumers to gain substantive privacy protections tends to decrease because the platform's utility increases, and consumers are less likely

---

[83] Just-in-time disclosures are disclosures presented to the consumer at the point of data collection, where the consumer immediately sees information about how the information they enter will be used. This provides information in discrete portions, rather than an aggregated form common in typical privacy policies. *See* FED. TRADE COMM'N, STAFF REPORT, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 15–16 (Feb. 2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[84] *See* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES 3 (2011), http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf.

[85] *See* Justus Haucap, *Competition and Competition Policy in a Data-Driven Economy*, 54 INTERECONOMICS REV. EUR. ECON. POL'Y 201, 202 (2019); *see also* David S. Evans & Richard Schmalensee, *The Antitrust Analysis of Multi-Sided Platform Businesses* 14 (Nat'l Bureau of Econ. Research, Working Paper No. 18783, 2013).

[86] *See* Suketu Gandhi et al., *Demystifying Data Monetization*, MIT SLOAN MGMT. REV. (Nov. 27, 2018), https://sloanreview.mit.edu/article/demystifying-data-monetization.

to leave.[87] Factoring in the lack of transparency in data collection and the lack of bargaining power inherent in the market, it is incredibly unlikely that there will be a substantive change absent any policy changes. In order to see the extent of data collection taking place through the user's apps and devices, many think-tanks, university researchers, and government agencies conduct studies to shed light on this complex, rapidly expanding ecosystem.

III. DATA COLLECTION AND SHARING PRACTICES

With the rise in connected devices and software apps that accompany them, data is being collected and distributed as never before. In each smart device, data can be collected from consumers themselves through direct entry, the sensors present in the device, and the network the device is connected to. The sensors present in smart watches may include accelerometers, Wi-Fi sensors, heart rate sensors, GPS, gyroscopes, microphones, barometers, altimeters, cameras, thermometers, compasses, and others.[88] Although the specific collections will vary between app and device, the key data components, in addition to consumer-entered information, can broadly be categorized into five types, as stated by Ann Cavoukian and Abhik Chaudhuri:

> (a) Data collected by edge devices like wireless sensors, IP camera, barcode readers, RFID readers, GPS devices.
> (b) Data at the gateway devices flushed periodically from the edge devices by wired and wireless network
> (c) Data sent to the cloud by gateway devices for analytical processing, storage and application based output
> (d) API based data interchange for various smart service offerings between machine to machines (M2M) and between machines and users

---

87 *See generally* Haucap, *supra* note 85.

88 *See* Kyle Wiggers, *Apple Watch Series 4 Can Detect Falls, Take ECGs, and Lead You Through Breathing Exercises,* VENTUREBEAT (Sept. 12, 2018, 10:54 AM), https://venturebeat.com/2018/09/12/apple-watch-series-4-can-detect-falls-take-ecgs-and-lead-you-through-breathing-exercises.

(e) 'Control' data sent back to the edge devices and sensors for controlling or fine-tuning the context of data gathering.[89]

This data can then be transferred to a number of different systems from the smart watch, including smartphones, devices, computers, and servers/cloud services.[90] This is further distinguished between proprietary systems of the wearable vendor's own apps and data and third-party systems, which are developed and maintained by external entities to provide specific functionalities.[91]

To fully grasp how difficult it is to follow from a consumer's perspective, it is important to understand how the apps collect data from a technical viewpoint. At a basic level, consumers would expect data to be transmitted from their phones for the performance of the app unless the app is known to be independent. A running app, for example, may send the consumer's location to a server run by the developers or the phone's manufacturer, and from there, use either that location information in conjunction with its own service or a vendor to map the running route, calculate calories burned, and suggest exercise routines for an upcoming race. However, beyond how companies handle consumer data rests the issue of how revealing that data can be for consumers.

a. Information Entered by Consumers Can Be Revealing

After downloading an app, consumers are often prompted to enter account information, shopping habits, or exercise routines, and apps can share this information as allowed by their privacy policy.[92] In 2013, the FTC conducted a study of consumer-generated and controlled data in various health apps that were available to the general public, using twelve apps, two wearables, and one primary device, such as a phone, specifying that it only

---

89 Abhik Chaudhuri & Ann Cavoukian, *The Proactive and Preventative (3P) Framework for IoT Privacy by Design,* 57 EDPACS 5 (2018).

90 Francisco de Arriba-Pérez et al., *Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios,* SENSORS, Sept. 2016, at 1, 5.

91 *Id.*

92 *See*, *e.g.*, Zack Whittaker, *Fitness App PumpUp Leaked Health Data, Private Messages,* ZDNET (May 31, 2018, 6:56 PM), https://www.zdnet.com/article/fitness-app-pumpup-leaked-health-data-private-messages (describing the data points entered by consumers that were exposed in a breach).

surveyed data available to the consumer.[93] In reviewing the apps, the FTC discovered data was sent to 76 third parties.[94] For example, one third party received information from four different apps in the study, and one app transmitted data to 18 third parties.[95] While the customer can restrict certain types of data by not giving the app permission, "[P]ermissions generally don't apply to the information users supply directly to the apps, which is sometimes the most personal."[96] As will be seen, consumer-entered information can trigger certain events causing sensitive data to be sent to third parties.

b. Excessive Permissions Can Undermine Privacy

When a consumer installs an app from a marketplace, such as the App Store or Google Play, the app requests certain permissions from the user.[97] App permissions are the privileges an app has to operate within the device, such as when Instagram gains access to a user's photos to upload them.[98] Generally, well-known developers try not to access more than they need for the app's service operations, which may include advertising, voice communication, or payment.[99] For consumers to really understand what the developers intend to use the data for in the app, they would need to turn to the app's privacy policy and its associated documents; but in doing so consumers will run into the same challenges discussed above.

These permissions can vary in the type of data accessed and potential threat levels. Determining permission trends within the two major mobile OS platforms may be accomplished using available research. While

---

93 FED. TRADE COMM'N, SPRING PRIVACY SERIES: CONSUMER GENERATED AND CONTROLLED HEALTH DATA (May 2014), https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf.

94 *Id.*

95 *Id.*

96 Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.,* WALL ST. J. (Feb. 22, 2019, 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

97 *See* David Nield, *How to See Everything Your Apps Are Allowed to Do,* WIRED (July 5, 2018, 7:00 AM), https://www.wired.com/story/how-to-check-app-permissions-ios-android-macos-windows.

98 *Id.*

99 *See* Lauren Goode, *App Permissions Don't Tell Us Nearly Enough About Our Apps*, WIRED (Apr. 14, 2018, 7:00 AM), https://www.wired.com/story/app-permissions/(discussing Apple and Google app permission guidelines and enforcement with developers).

Apple and Google make up approximately 96.3% of the smartphone market, 81.5% of devices shipped in 2014 had Android OS.[100] This consolidation is projected to continue as Android takes more of the market.[101] Accordingly, the vast majority of data covers Android devices,[102] so more research may need to be done to evaluate permission habits within iOS devices. In *Android Permissions Demystified* (2011), the authors explain that Android gives apps access to system resources at the time of installation.[103] Google only recently announced a departure from all-or-nothing permissions for an app, which allows consumers to have more control over permissions given to an app.[104] Android "defines 134 permissions" that are placed into one of the following three threat levels: Normal, Dangerous, and Signature/System permissions.[105] Developers declare the permissions their app will use when they submit it to the app store.[106] The study reviewed 940 apps from the Google Play store, and "identified 323 apps (35.8%) as having unnecessary permissions."[107] Within that subset, "9% of the overprivileged app[s] request unneeded Signature or SignatureOrSystem permissions."[108]

In *Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis,* the authors identified 24 apps available on the Google Pixel that pertained to medicine

---

100 John Kennedy, *Android and iOS Dominate Smartphone Economy – Own 96.3pc of Overall OS Market,* SILICON REPUBLIC (Feb. 25, 2015), https://www.siliconrepublic.com/companies/android-and-ios-dominate-smartphone-economy-own-96-3pc-of-overall-os-market.

101 Melissa Chau & Ryan Reith, *Smartphone Market Share,* INT'L DATA CORP. (updated Apr. 2, 2020), https://www.idc.com/promo/smartphone-market-share/os.

102 *See* Gabriella M. Harari, *Using Smartphones to Collect Behavioral Data in Psychological Science: Opportunities, Practical Considerations, and Challenges*, 11 PERSP. ON PSYCHOL. SCI., Nov. 2016, at 838, *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5572675/pdf/nihms862908.pdf.

103 Adrienne Porter Felt et al., *Android Permissions Demystified,* CCS' 11 PROC. 18TH ACM CONF. COMPUTER & COMM. SECURITY 627, 628 (2011).

104 Ben Smith, *Project Strobe: Protecting Your Data, Improving Our Third-Party APIs, and Sunsetting Consumer Google+,* GOOGLE (Oct. 8, 2018), https://www.blog.google/technology/safety-security/project-strobe.

105 Felt et al., *supra* note 103, at 628.

106 *Declare Permissions for Your App,* GOOGLE, https://support.google.com/googleplay/android-developer/answer/9214102 (last visited Apr. 16, 2020).

107 Felt et al., *supra* note 103, at 634.

108 *Id.* at 636.

information, dispensing, administration, or prescribing.[109] They analyzed the permissions requested and the data sent from the app.[110] Using the developer self-report on Google Play, the researchers found that the apps requested four permissions that involved a user's private information, stored data, or ability to affect other app operations, such as determining precise location (25% of the apps), reading, and editing device storage (79% of the apps), or receiving the phone's identity, including phone number and network information (29% of the apps).[111] In their study, over 67% of the entities that data was sent to were "analysis providers," which include those responsible for collecting, collating, analyzing, or commercializing user data.[112]

c. Third-Party Libraries and Software Development Kits Have Access to Data

When an app receives permissions from the user, those permissions are passed down to all the components of the apps, and because apps are usually developed with the assistance of third parties, this transfer of permissions can provide ways for third parties to collect data. Combining code from other sources enables the developers to save time, use pre-tested code and modular code (where a function is in an independent module from the rest of the code).[113] Modular code can provide a specific function, such as targeted ads, app maintenance, social network integration, or user engagement,[114] rather than being interwoven with the rest of the app.[115] To this end, developers often use third-party libraries and software development kits for modular code, and, in addition to the immense benefits these

---

109 Quinn Grundy et al., *Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis,* BMJ, Mar. 20, 2019, at 1, 4.

110 *Id.*

111 *Id.* at 4.

112 *Id.* at 5.

113 *See, e.g.*, Uroosa Sehar, *Third Party SDKs Used By Top Mobile Apps,* VIZTECK SOLUTIONS (Sept. 26, 2016), https://vizteck.com/blog/third-party-sdk-used-by-top-mobile-apps; *Importance of Modularity in Programming*, ASPECT-ORIENTED SOFTWARE DEV. (Jan. 18, 2018), http://aosd.net/importance-of-modularity-in-programming.

114 Abbas Razaghpanah et al., *Apps, Trackers, Privacy, and Regulators,* NETWORK & DISTRIBUTED SYSTEMS SECURITY SYMP. 1 (2018), https://haystack.mobi/papers/ndss18_ats.pdf.

115 *See generally* Saksham Chitkara et al., *Does this App Really Need my Location? Context-Aware Privacy Management on Smartphones,* PROC. ACM ON INTERACTIVE MOBILE WEARABLE & UBIQUITOUS TECHNOLOGIES, Sept. 2017, at 42:1 (2017).

libraries provide, the libraries are also able to collect sensitive data from consumers through the code that is implemented.[116] Because the libraries are used by various apps,[117] different apps may receive different sets of permissions from a single device; developers can utilize the diversity of apps to create digital profiles of the users.[118] The library or third-party services receive the same set of permissions the parent app receives, receiving large amounts of data usually beyond what was needed to provide a specific service to the app developer.[119] The specific device can then be identified through a unique device identification number.[120] Based on the top 1,000 apps in the App Store and Google Play, the average number of Software Development Kits per app was 19 for iOS and 28 for Android. 17.6% of those apps on the App Store and 25.4% of those on Google Play had at least one Facebook Software Development Kit.

In, *Does this App Really Need My Location? Context-Aware Privacy Management for Smartphones,* Yuvraj Agarwal et al. analyzed 1,321 users and found that the "most popular 30 libraries account for more than half of all private data accesses, while the top 100 account for 70%."[121] When incorporating ad-technology code or analytics packages, developers may not be aware of the details collected by the packages, and consumers are usually not provided any notice inside the app that it is "effectively tracking users without their knowledge or consent while remaining virtually invisible."[122] Often, when data is sent to a third party that is identifiable, the third party only functions as a subsidiary of another, and data is shared between the subsidiary and the parent, which further complicates those trying to piece together a map of how data is transmitted.[123] For example, Yahoo owns

---

116 Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data With Third-Party Services,* CONVERSATION (May 29, 2017, 9:48 PM), http://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404.

117 Chitkara et al., *supra* note 115, at 42:2.

118 Vallina-Rodriguez & Sundaresan, *supra* note 116.

119 Razaghpanah et al., *supra* note 114, at 1.

120 Chitkara et al., *supra* note 115, at 42:7.

121 *Id.* at 4

122 Razaghpanah et al., *supra* note 114, at 1.

123 *See* Reuben Binns et al., *Third Party Tracking in the Mobile Ecosystem,* WEBSCI '18 10TH ACM CONF. ON WEB SCI., Oct. 8, 2018, at 1, 3, *available at* https://arxiv.org/pdf/1804.03603.pdf.

Flurry, Flickr, and Interclick,[124] and AOL owns Convertro and Gravity Insights.[125] Both Yahoo and AOL are owned by Oath (now Verizon Media),[126] which is owned by Verizon, the "root parent."[127] The root parent has access to the data gathered by the subsidiaries; it can aggregate and manage the data as it sees fit.[128] In February of 2019, Sam Schechner and Mark Secada reported on how Flo Health Inc.'s "Flo Period and Ovulation" tracker, which claims to have over 25 million active users, informed Facebook when a user was having her period or was intending to get pregnant.[129] Their analytics kit, which is built into "thousands of apps," uses a tool called "App Events," which "allows developers to record their users' activity and report it back to Facebook regardless of whether users log in via Facebook or even have a profile."[130] Similarly, HR Monitor, a heart-rate app on Apple's iOS, sent a user's heart rate to Facebook immediately after it was recorded.[131] In a written statement, Flo remarked that the data sent to Facebook is "depersonalized," yet testing by the Wall Street Journal revealed that unique advertising identifiers, which can be matched to a device or profile, were sent

---

[124] Ingrid Lunden, *Yahoo Buys Mobile Analytics Firm Flurry For North of $200M,* TECHCRUNCH (July 21, 2014, 1:55 PM), https://techcrunch.com/2014/07/21/yahoo-is-buying-mobile-analytics-firm-flurry-for-north-of-200m/;
Mat Honan*, The Most Fascinating Profile You'll Ever Read About a Guy and His Boring Startup*, WIRED (Aug. 7, 2014, 6:38 AM), https://www.wired.com/2014/08/the-most-fascinating-profile-youll-ever-read-about-a-guy-and-his-boring-startup; Leena Rao, *Yahoo To Buy Data-Driven Advertising Network Intercick For $270 Million*, TECHCRUNCH, (Nov. 1, 2011, 8:10 AM), https://techcrunch.com/2011/11/01/yahoo-buys-data-driven-ad-company-interclick-for-270-million.

[125] Kara Swisher, *AOL Buys Personalization Startup Gravity for $90 Million in Cash*, VOX (Jan. 23, 2014, 4:31 AM), https://www.vox.com/2014/1/23/11622610/aol-buys-personalization-startup-gravity-for-90-million-in-cash; Ingrid Lunden, *AOL Buys Marketing Analytics Company Convertro for $101M*, TECHCRUNCH (May 6, 2014, 3:36 PM), https://techcrunch.com/2014/05/06/aol-buys-marketing-analytics-company-convertro-for-101m-memo.

[126] Brian Heater, *Oath Officially Becomes Verizon Media Group on January 8*, TECHCRUNCH (Dec. 18, 2018, 4:38 PM), https://techcrunch.com/2018/12/18/oath-officially-becomes-verizon-media-group-on-january-8.

[127] Nick Turner, *Verizon Kills Oath Brand After It Fails to Enliven Yahoo and AOL*, BLOOMBERG (Dec. 18, 2018, 4:46 PM), https://www.bloomberg.com/news/articles/2018-12-18/verizon-kills-oath-brand-after-it-fails-to-enliven-yahoo-and-aol.

[128] Razaghpanah et al., *supra* note 114, at 2.

[129] Schechner & Secada, *supra* note 96.

[130] *Id.*

[131] *Id.*

with the sensitive information.[132] For an Android app, the Wall Street Journal commissioned a cybersecurity firm named Defensive Lab Agency ("DLA") to determine what an app, called BetterMe: Weight Loss Workouts, was sending.[133] BetterMe, immediately after a consumer entered the information, sent a users' weight and height to Facebook.[134]

d. Cross-device Tracking is Difficult to Detect and Can Link Consumer Data

These examples are just a few highlights.[135] Dozens of other examples in news stories are available across the internet, and new examples arise every day.[136] The real concern with data comes with the collation of the data in third and fourth parties since they can use cross-device tracking to track users across platforms and devices, creating increasingly invasive and revealing profiles of individuals who are unaware of them.[137]

"Cross-device tracking occurs when platforms, publishers, and ad tech companies try to connect a consumer's activities across her smartphones, tablets, desktop computers, and other connected devices."[138] As with most technologies, tracking can provide a number of benefits to consumers, such as logging into a social media account across devices, "maintain[ing] state" to pick up where the user left off in a book, or preventing fraud.[139] However, tracking also allows companies that aggregate

---

132 *Id.*

133 *Id.*

134 *Id.*

135 *See also* Dave Muoio, *Most Popular Health Apps Routinely Share Data with Little Transparency*, MOBI HEALTH NEWS (Mar. 22, 2019), https://www.mobihealthnews.com/content/most-popular-health-apps-routinely-share-data-little-transparency.

136 *See* Sam Schechner, *Eleven Popular Apps That Shared Data With Facebook*, WALL ST. J. (Feb. 24, 2019, 7:45 PM), https://www.wsj.com/articles/eleven-popular-apps-that-shared-data-with-facebook-11551055132.

137 *See* Samantha Cole, *Health Apps Can Share Your Data Everywhere, New Study Shows*, VICE (Mar. 20, 2019, 5:30 PM), https://www.vice.com/en_us/article/pan9e8/health-apps-can-share-your-data-everywhere-new-study-shows (citing a number of health apps that sent data to Facebook).

138 FED. TRADE COMM'N, CROSS-DEVICE TRACKING: AN FTC STAFF REPORT i (Jan. 2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf [hereinafter CROSS-DEVICE TRACKING FTC REPORT].

139 *Id.*

the data to create an entire device map and analyze "an individual consumer's activities based not only on her habits on one browser or device," but also on all the devices linked to the consumer.[140] Combining this with data about a consumer's offline behavior collected from physical stores that sell their data sets, companies can create a more revealing picture of a person than just one app or device alone can.[141]

When engaging in cross-device tracking, companies use both "deterministic" and "probabilistic" techniques.[142] Deterministic techniques usually involve some form of consumer-identifying characteristic, like a login; typically, a consumer will log in on each device or app they use.[143] Probabilistic techniques require a company to infer which consumer uses a device.[144] This often happens through IP tracking or geolocation information, and because consumers do not have to take any affirmative identification action, it is less apparent to consumers.[145] Combining these two techniques results in more accurate information, so companies often work together to merge data sets. With the popularity of connected devices, the scope of this tracking may extend to include smart televisions, health data from wearable devices, and shopping habits collected through retail IoT practices, yet companies are usually not explicit in discussing these practices.[146] The FTC, in reviewing 100 privacy policies, only found three policies that reference "enabling third-party cross-device tracking . . . ."[147]

Cross-device tracking presents concerns about transparency, choice, and security—themes that have been recurring through this paper so far. Between consumer-entered information, excessive permissions, third party development kits, and cross-device tracking, the challenge to increase company transparency, consumer understanding, and data security will only become more difficult. When we consider the ways data can be used to increase our quality of life, it is apparent that we need to work towards a

---

140 *Id.*

141 *See* Linda Carroll, *Your Health App Could Be Sharing Your Medical Data*, REUTERS (Mar. 22, 2019, 11:51 AM), https://www.reuters.com/article/us-health-apps-privacy-idUSKCN1R326W.

142 CROSS-DEVICE TRACKING FTC REPORT, *supra* note 138, at 2.

143 *Id.* at 2–3.

144 *Id.* at 3.

145 *Id.*

146 *Id.* at 7.

147 *Id.* at 8.

solution that is both conducive to the use of data as well as the safety and choice of consumers.

IV. THE IMPACT OF HEALTH-RELATED DATA

At first glance, the data collected from connected devices that companies use largely appears to be limited to advertising and software companies, but on closer inspection, there is a deeper trend of data usage. Through the power of machine learning, large companies are able to sort through incredible amounts of data to reveal insights about each person. These analytic services are able to be employed by companies for a variety of purposes, such as identifying the onset of disease before the symptoms become critical or evaluating the health risk of a patient to make changes to their insurance plan. When looking at the impact of health-related data on consumers, it is important to broaden the scope to include targeted advertising, algorithmic processing, and the potential for combination with other readily available data sources.

a. Targeted Advertising Can Pose Substantial Risks

According to a report discovered by *The Australian*, Facebook's algorithms can enable advertisers to determine precisely when a teenager has low self-esteem, insecurity, depression, or lack of confidence.[148] Though Facebook claims the report has been misleading,[149] it has been corroborated by others who have felt first-hand how advertisers can prey on vulnerable individuals.[150] While the report should come as no surprise given Facebook's 2014 study where it claimed it could "make people feel more positive or negative through a process of 'emotional contagion,'"[151] it highlights the role data analytics can play in determining things the users themselves

---

[148] Sam Machkovech, *Report: Facebook Helped Advertisers Target Teens Who Feel "Worthless,"* ARS TECHNICA (May 1, 2017, 2:00 AM), https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless.

[149] Press Release, Facebook, Comments on Research and Ad Targeting (Apr. 30, 2017), *available at* https://newsroom.fb.com/news/h/comments-on-research-and-ad-targeting.

[150] *See, e.g.*, Kari Paul, *When Facebook and Instagram Think You're Depressed,* VICE (May 5, 2017, 11:16 AM), https://www.vice.com/en_us/article/pg7d59/when-facebook-and-instagram-thinks-youre-depressed.

[151] Robert Booth, *Facebook Reveals News Feed Experiment to Control Emotions,* GUARDIAN (June 29, 2014), https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds.

are not aware of or would not want to be shared. More importantly, it illustrates the detrimental effects that careless advertising can bring to an individual, particularly for vulnerable populations. When Kari Paul interviewed Caroline Sanders, a machine learning designer, Sanders commented that "while algorithmically they may seem related to what was served up before, there is a lot of harm in the causal effects of how these things manifest."[152] Having these advertisements escalate from promoting "meditation apps" to asking users "'are you bipolar' is really dangerous."[153]

In other cases, the harm from targeted advertising can arise from violations of privacy, errors in attribution, or directed political messaging at vulnerable populations. Facebook showed gay conversion therapy ads to young LGBT users on their network, which Facebook attributed to a "micro-targeting" blunder, despite the "evidence of the damage conversion therapy does to LGBT people's health and well-being."[154] The well-known story of Target predicting the pregnancy of a high school teenager based on her purchase history serves as another example of how data analytics have the potential to overstep boundaries, reveal personal information, and incentivize secrecy.[155] In the Target example, the company sent a coupon booklet for baby items to a high school girl whose father had not yet been told of her pregnancy.[156] After Target developed their pregnancy-prediction model, they sought to obfuscate their discovery by "piggyback[ing] on existing habits" and inserting baby items in other ads to make it look like they were "chosen by chance."[157] In a similar vein, Copley Advertising LLC was pursued by the Massachusetts Attorney General after they used geofencing technology to deliver targeted advertisements of anti-abortion messages to over 800,000 vulnerable women[158] as they visited abortion clinics. In the

---

152 Paul, *supra* note 150.

153 *Id.*

154 Helena Horton & James Cook, *Facebook Accused of Targeting Young LGBT Users with 'Gay Cure' Adverts*, TELEGRAPH (Aug. 28, 2018, 12:00 PM), https://www.telegraph.co.uk/news/2018/08/25/facebook-accused-targeting-young-lgbt-users-gay-cure-adverts**.**

155 *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

156 *Id.*

157 *Id.*

158 *See* Sharona Coutts, *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits*, REWIRE.NEWS (May 25, 2016, 6:52 PM), https://rewire.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits**;** Press Release, Office of Mass. Att'y

subsequent settlement, Copley agreed "not to use [geofencing] technology at or near Massachusetts healthcare facilities to infer the status, medical condition, or treatment of any person."[159]

b. Automated Decision Making and Data Brokers Can Harm Consumers.

Though they operate mostly out of the public eye, data brokers collect data about consumers from hundreds of different public and proprietary sources in order to make, analyze, package, and sell said data or insights derived from the data to other companies. These companies almost never have direct relationships with the subjects of the data they collect; as discussed earlier, it is remarkably difficult to track the data to the brokers. As a result, most consumers are not even aware these brokers have data on them or that their data is being collected. Generally, brokers can be divided into four types: people search sites, like Spokeo and ZoomInfo; advertising and marketing, like Acxiom; credit reporting, like Experian and Equifax; and risk mitigation, like LexisNexis Risk Solutions.[160] Each purchases data sets, scrapes public records, and/or participates in app-centric data collection. Acxiom, for example, provides "up to 3,000 attributes on 700 million people," and in 2018, "10,000, on 2.5 billion consumers."[161]

These companies often develop "risk scores" based on consumer data which can then be sold to doctors, insurance companies, and hospitals to identify at-risk patients.[162] In the process, these data brokers have partnered with health-insurance companies to process data on hundreds of

---

Gen., AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017), *available at* https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts.

159 Nate Raymond, *Firm Settles Massachusetts Probe Over Anti-Abortion Ads Sent to Phones*, REUTERS (Apr. 4, 2017), https://www.reuters.com/article/us-massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSKBN1761PX.

160 Steven Melendez & Alex Pasternack, *Here are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST COMPANY (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

161 *Id*.

162 *See, e.g.*, Mohana Ravindranath, *How Your Health Information is Sold and Turned into 'Risk Scores'*, POLITICO (Feb. 3, 2019, 6:56 AM), https://www.politico.com/story/2019/02/03/health-risk-scores-opioid-abuse-1139978.

millions of Americans.[163] LexisNexis Risk Solutions advertises its services by stating that it offers health risk prediction scores separate from protected health information covered under HIPAA.[164] ProPublica reported that LexisNexis "uses 442 non-medical personal attributes to predict a person's medical costs. Its cache includes more than 78 billion records from more than 10,000 public and proprietary sources . . . ."[165] Lexis went so far as to "validate[] its scores against insurance claims and clinical data. But it won't share its methods and hasn't published the work in peer-reviewed journals" to be verified.[166] Milliman MedInsight, one of the world's largest actuarial firms, is now using Lexis's scores, "[M]atch[ing] patient and member lists sent by healthcare organizations to approximately 280 million identities."[167] Marcos Dachary, Director of Product Management for Milliman, acknowledged that "there could also be negative potential."[168] In other words, it could be used to discriminate.

Similarly, Aetna purchased data on millions of Americans from a data broker that contained hundreds of details about each person, including a person's hobbies, such as whether they ride bikes or run marathons.[169] Frank Pasquale, a University of Maryland law professor who specializes in issues relating to machine learning, comments that the "health privacy machine" is in crisis, stating that while the United States has "a law that only covers one source of health information," and that there is rapid development of data from other sources.[170] He suggests that health-risk scores should be treated like credit scores, for "[t]he risk of improper use is

---

163 Marshall Allen, *Health Insurers Are Vacuuming Up Details About You – And It Could Raise Your Rates,* PROPUBLICA (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.

164 *See id;* U.S. DEP'T OF HEALTH & HUMAN SERVS., NAT'L COMM. ON VITAL AND HEALTH STATISTICS, HEALTH INFORMATION PRIVACY BEYOND HIPAA: A 2018 ENVIRONMENTAL SCAN OF MAJOR TRENDS AND CHALLENGES 23 (Dec. 2017) [hereinafter DHHS BEYOND HIPAA].

165 Allen, *supra* note 163.

166 *Id.*

167 *Milliman MedInsight to Use LexisNexis Risk Solutions Socioeconomic Health Attributes to Help Enhance Healthcare Intelligence,* LEXISNEXIS RISK SOLUTIONS (Oct. 24, 2017, 9:00 AM), https://www.prnewswire.com/news-releases/milliman-medinsight-to-use-lexisnexis-risk-solutions-socioeconomic-health-attributes-to-help-enhance-healthcare-intelligence-300541930.html.

168 Allen, *supra* note 163.

169 *Id.*

170 *Id.*

extremely high. And data scores are not properly vetted and validated and available for scrutiny."[171] This trend appears to have no sign of abating. Similarly, Optum, owned by UnitedHealth Group, was issued a patent in 2016 for an invention that links what consumers share on social media to their clinical and payment information.[172]

Certainly, this data could help patients get appropriate care, but "the industry has a history of boosting profits by signing up healthy people and finding ways to avoid sick people—called 'cherry picking.'"[173] Despite the Affordable Care Act, which prevents denials based on pre-existing conditions and is currently the subject of litigation,[174] insurance companies could still use the data to determine the prices of certain plans, which drugs to include in a plan, or which providers to limit from their network.[175]

Using these data sources, companies can utilize automated decision making with little to no transparency to make eligibility decisions for loans, provide less favorable services, increase interest rates, fees, and insurance premiums, or reject applicants for employment opportunities.[176] At any point in the process, automated decision making could filter out individuals with problematic characteristics; without a human participating in the process, the filtered individual would have little to no idea why they faced negative consequences.[177]

If regulators manage to prevent insurers' efforts to avoid certain patients, "[E]mployers may adopt pretextual tactics to drive them away as employees," and these methods won't be easy to detect.[178] Within the black box of an algorithm, it can be notoriously difficult to detect where the line is between one category and another.[179] If an employer was made aware of certain sensitive "health-related topics or conditions, such as 'Expectant

---

171 *Id.*

172 U.S. Patent No. 9,300,676B2 (filed Mar. 17, 2014) (issued Mar. 29, 2016).

173 Allen, *supra* note 163.

174 *See* Ailsa Chang & Sabrina Corlette, *How a Lawsuit Challenging Obamacare Could Affect People with Pre-Existing Conditions,* NPR (Mar. 28, 2019, 5:03 PM), https://www.npr.org/2019/03/28/707722585/how-a-lawsuit-challenging-obamacare-could-affect-people-with-pre-existing-condit.

175 Allen, *supra* note 163.

176 DHHS BEYOND HIPAA, *supra* note 164, at 23.

177 *Id.*

178 *See* Pasquale, *Redescribing Health Privacy*, *supra* note 12, at 107.

179 *See* FRANK PASQUALE, THE BLACK BOX SOCIETY 9 (Harv. Univ. Press 2015).

Parent,'" which can be triggered from their purchase patterns, browsing history, or other seemingly unrelated pieces of data, they could use this information for their hiring or firing decisions without the individual being aware.[180] Generally, the Americans with Disabilities Act prohibits an employer from investigating an employee's medical condition beyond what is necessary to assess the employee's ability to perform their occupational duties, because the introduction of varied sources of data and their associated insights can obfuscate the lines of legality and reduce employers' chances of being caught.[181]

To use Pasquale's example, an employee would be hard-pressed to know that the algorithm was being used at all, much less whether or not the algorithm was "characterizing a potential employee as 1) diabetic, 2) in a 'diabetic-focused household' . . . . , 3) concerned about diabetes, [or] 4) having a demanding home life . . . ."[182] Determining whether element (4) applies would likely require insight into the attributes of the algorithms of the first three elements.[183] Using an algorithm to ascertain indirectly that which the employer could not ask directly is certainly illegal,[184] but applicants will have a more difficult time discovering and litigating which characteristics were used to make an employment decision.[185] This is because applicants would need to review information from different data sources which have a correlation with a medical condition, such as exercise data, internet searches, or purchase history and determine that these sources critically affected the hiring decision.[186] Therefore, any effort to expand employment protections beyond the first box would run into challenges from

---

[180] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 5 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[181] *See* Pasquale, *Redescribing Health Privacy supra* note 12, at 124.

[182] *Id*. at 107 (internal parentheticals removed).

[183] *See id.* at 107.

[184] *See* U.S. EQUAL EMP'T OPPORTUNITY COMM'N, ADA ENFORCEMENT GUIDANCE: PREEMPLOYMENT DISABILITY-RELATED QUESTIONS AND MEDICAL EXAMINATIONS 2 (1995), https://www.eeoc.gov/policy/docs/preemp.html.

[185] *See* Pasquale, *Redescribing Health Privacy supra* note 12, at 124.

[186] *See* DHHS BEYOND HIPAA, *supra* note 164, at 49 (discussing hypothetical data company that can use data, such as food purchase and biofeedback information, to reasonably identify whether a person is diabetic).

businesses and analytics firms because it would "require extensive auditing of business records" to figure out.[187]

Because the data is collected from so many different sources, advertising companies, data brokers, and those who receive risk scores have no obligation and little incentive to allow consumers to rectify incorrect data points that could lead to incorrect conclusions, which could unknowingly affect how they live their lives.[188] As Samuel Finlayson of Harvard Medical School points out, in the context of artificial intelligence and automated decision making, "the inherent ambiguity in medical information, coupled with often-competing financial incentives, allows for high-stakes decisions to swing on very subtle bits of information."[189]

As algorithms become more prominent, transparency will become more difficult. While HIPAA requirements have been clarified through litigation, "[D]ata brokers continue gathering information, and making predictions based on it, entirely outside the HIPAA-protected zone."[190] The inferences from this data will become even more influential. These algorithms can make decisions about real-life people who are entirely unaware of how these decisions are being made.[191] Despite anti-discrimination statutes, individuals may be concerned that algorithms may make discriminatory decisions that are either not covered by statute, cannot be proven, or are undetectable by workers.[192]

---

187 Pasquale, *Redescribing Health Privacy supra* note 12, at 107.

188 *See* Cade Metz & Craig S. Smith, *Warnings of a Dark Side to A.I. in Health Care*, N.Y. TIMES (Mar. 21, 2019), https://www.nytimes.com/2019/03/21/science/health-medicine-artificial-intelligence.html.

189 *Id*; Milena A. Gianfracesco et al., *Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data*, JAMA INTERNAL MED., Nov. 2018, at 1544 , *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6347576; Carolyn Y. Johnson, *Racial Bias in a Medical Algorithm Favors White Patients over Sicker Black Patients*, WASH. POST (Oct. 24, 2019), https://www.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients.

190 Pasquale, *Redescribing Health Privacy supra* note 12, at 108.

191 *See generally* Sean Illing, *How Algorithms are Controlling Your Life*, VOX (Oct 1, 2018, 8:10 AM), https://www.vox.com/technology/2018/10/1/17882340/how-algorithms-control-your-life-hannah-fry.

192 Sharona Hoffman*, Employing E-health: The Impact Of Electronic Health Records On The Workplace,* 19 KAN. J.L. & PUB. POL'Y 409, 416 (2010).

V. CONCLUSION

In the three decades since Internet adoption began to climb, technology has changed dramatically, computing power has increased exponentially, and data is being generated at rates never before seen. The ability to process large amounts of data will be the hallmark of the 21st century; artificial intelligence and machine learning will revolutionize the way society operates. Not so long ago, mobile phones were reserved for the wealthy, and Facebook was "merely a database of profile pages of other people at Harvard."[193] Now, there are more mobile devices than people,[194] and Facebook has over 2 billion users.[195] As these technologies evolve, it will be vital to realize that, given the advent of machine learning and vast data generation, even the most innocuous pieces of data can be combined with others to generate new types of inferences previously thought impossible. Merely because information did not originate with a covered entity does not mean it cannot have dramatic impacts on the well-being of individuals or in the innovation of products.

Yet, the task of defining what constitutes health data is difficult, because data ostensibly unrelated to a person's health may ultimately be used to craft new conclusions about that person's sensitive health status; this can be considered a byproduct of a sectoral privacy regime based on data source and data type.[196] A particular data point may be used as health data in the evaluation of a person's exercise habits and medical screening; that same data point may also be processed as part of a rideshare service.[197] The development of new apps and products that use this data to diagnose and treat illnesses and conditions can benefit consumers and society at large, but companies may use this same data to engage in discriminatory practices without ever notifying the consumer.

Looking forward, companies, regulators, and legislators will need to develop a framework that encourages innovation, evaluating the purposes

---

193 Alexis Madrigal, *Before It Conquered the World, Facebook Conquered Harvard,* ATLANTIC (Feb. 4, 2019), https://www.theatlantic.com/technology/archive/2019/02/and-then-there-was-thefacebookcom/582004.

194 Zachary Davies Boren, *There Are Officially More Mobile Devices Than People in the World,* INDEP. (Oct. 7, 2014), https://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html.

195 Madrigal, *supra* note 193.

196 *See* O'Connor, *supra* note 21.

197 *Id*.

of processing, informing consumers, incentivizing business transparency, and protecting the security, privacy, and freedom of individuals. Further research should explore possible solutions, which educate consumers and give them more control over their data while promoting ethical innovation.

CONSTRAINING THE CYBERMOB: USING A DOXING NOTICE AND TAKEDOWN REGIME TO OPTIMIZE THE SOCIAL UTILITY OF ONLINE SHAMING

Erik Money*

Social media platforms have transformed an age-old institution, public shaming, into a new phenomenon known as "cybermobbing." Cybermobs cause outsized economic, reputational, and dignitary harm to their victims, resulting in a net negative social impact. Despite the severity of cybermobbing, no catch-all legal remedy is available to its victims. Even if a victim could overcome the practical barriers of getting individual mob members into the courtroom, current legal remedies are inadequate. Furthermore, § 230 of the Communications Decency Act immunizes Interactive Computer Service Providers ("ICSPs") against any potential liability. Cybermobbing victims are bereft of remedies.

After introducing the concept of cybermobbing, this Note examines case studies of cybermobbing, explains why victims cannot recover against cybermobs, considers the social utility provided by online shaming, and proposes statutory reform to optimize its social utility. This Note proposes sample legislation which uses the Digital Millennium Copyright Act as a template to create a notice and take-down regime for posts that expose personal information of private individuals (i.e., to "dox"). Under this Note's proposed sample legislation , entitled the Doxing Notice and Takedown Act ("DNTA"), ICSPs would be required to remove posts that dox private individuals upon notification. At that point, the poster could provide counter-notification showing that the individual is a public figure or that the messages do not dox the individual. Because the exposure of personal information is what allows cybermobs to cause real-world harm, the DNTA would be an affirmative first step to optimize the social utility of online shaming

---

*Juris Doctor candidate, University of St. Thomas School of Law, class of 2020. I would like to thank Professor Thomas Berg, Arlene Schuweiler, Alex Landreville, and Ryan Paukert for their valuable insights and assistance. The views expressed in this Note belong to the author alone.

TABLE OF CONTENTS

APPENDIX A

I. INTRODUCTION

Public shaming is nothing new. In the 1500s, transgressive individuals were met with scold's bridles, pillories, stockades, cucking stools, and other forms of corporal punishment.[1] A sign would often accompany the punishment, announcing the particular sin of the shamed community member.[2] Fortunately, physical public shaming fell out of favor in the 1600s, a development accredited to urbanization, industrialization, and the rise of the prison system.[3] With the advent of social media, however, public shaming has reared its ugly head with renewed vigor.[4] This digital shaming is a different beast from its predecessor.

The cybermob can attack anyone, anywhere, and for any reason.[5] The practice is known as "cybermobbing," a phenomenon where a group of people utilize an online platform to insult, dox,[6] threaten, and/or humiliate another individual.[7] A cybermobbing normally begins when an individual is shown in a controversial light, having said or done something inappropriate.[8] The controversy does not need to be recent; victims can be, and often

---

[1] Matthew Green, *A Grim and Gruesome History of Public Shaming in London: Part 1*, LONDONIST (Jan. 19, 2017), https://londonist.com/2015/12/publicshaming1.

[2] *See* Kristine L. Gallardo, *Taming the Internet Pitchfork Mob: Online Public Shaming, The Viral Media Age, and the Communications Decency Act*, 19 VAND. J. ENT. & TECH. L. 721, 725 (2017).

[3] *Id.*

[4] *Id.*

[5] *See* Kate Klonick, *Re-Shaming the Debate: Social Norms, Shame, and Regulation in an Internet Age*, 75 MD. L. REV. 1029, 1031 (2016). Klonick lucidly notes that "low cost, anonymous, instant, and easy access to the Internet has eviscerated whatever 'natural' limits there were to public shaming and has served to amplify its effects. Now, any perceived violation of a social norm—a racist Tweet, a sexist joke, taking up too much room on public transportation—can result in immediate, prolific condemnation from millions of people all over the world. Today, it is easier than ever to use shaming to enforce so-called social norms, and it is easier than ever for shaming to spin out of control." *Id.* (internal citations omitted).

[6] "[T]o publicly identify or publish private information about (someone) especially as a form of punishment or revenge." *Dox*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/dox (last visited Apr. 19, 2020).

[7] While the phenomenon has not yet been reduced to a formal definition, one writer has described "Cyber-mobbing" as "Cyber-cruelty that involves a group sharing the same malicious mindset or intent." Sue Scheff, *When Cyberbullying Turns Into Cybermobbing: Death by Suicide,* HUFFINGTON POST (Sept. 24, 2013), https://www.huffpost.com/entry/when-cyberbullying-turns-into-cyber-mobbing_b_3957416.

[8] *See infra* Section II.a.

are, mobbed for something they said or did years ago.[9] Typically, targets provoke a mob by saying something controversial online.[10] Nevertheless, targets may also be mobbed for expressing moderate but unpopular opinions,[11] making silly jokes in real life,[12] or for simply being in the wrong place at the wrong time.[13] The victim is then publicly excoriated on social media, insulted, doxed, threatened, and potentially fired by an employer caving to public pressure.[14] The impact is devastating, normally far outsizing whatever misdeed—if any—provoked the mob. Some have been fired from their jobs,[15] others have had their career prospects ruined entirely,[16] and still others have killed themselves.[17] Despite the life-altering impact of cybermobbing, victims have little recourse.

Pursuing individual mob members is impractical because of internet anonymity, jurisdictional issues, the number of defendants, the possibility of judgment-proof defendants, and the likelihood that, individually, each defendant's actions are not actionable. Attempts to hold Interactive Computer Service Providers ("ICSP") liable will be frustrated by § 230 of the

---

[9] *Id.*

[10] *Id.*

[11] *See* Daniella Greenbaum, *The Social Media Mob is a Danger to Society*, WASH. POST (July 12, 2018, 5:46 PM), https://www.washingtonpost.com/opinions/the-social-media-mob-is-a-danger-to-society/2018/07/12/eef13834-860b-11e8-9e80-403a221946a7_story.html (opinion columnist for Business Insider pressured into resigning for saying a female actress should be able to portray a transgender man); Michael Friscolanti, *Why Andrew Potter Lost his "Dream Job" at McGill*, MACLEAN'S (Mar. 23, 2017), https://www.macleans.ca/news/canada/why-andrew-potter-lost-his-dream-job-at-mcgill (professor forced to resign from "dream job" over article opining that "Quebec is an almost pathologically alienated and low trust society, deficient in many of the most basic forms of social capital that other Canadians take for granted.").

[12] *See* Klonick, *supra* note 5, at 1030–32 (discussing incident where a man was fired for making "dongles" joke at tech conference after a woman posted his picture online and that woman was subjected to threats of physical harm in a retaliatory mobbing).

[13] *See infra* Section II.a (discussing Cantrell and Tripathi case studies).

[14] *See generally infra* Section II.a discussion about cybermobbing case studies.

[15] *See infra* Section II.a regarding Justine Sacco.

[16] DANIELLE KEATS CITRON, HATE CRIMES IN CYBER SPACE 8 (Harv. Univ. Press, 2014) (noting that most employers, roughly 90 percent, rely on online reputation as an employment screen for prospective hires).

[17] *See infra* Section II.a regarding Cantrell. Even if the victim does not commit suicide, the individual is still at much higher risk for developing a mental illness, such as depression, anxiety, panic attacks, post-traumatic stress disorder, or anorexia nervosa. *See* CITRON, *supra* note 16, at 10–11.

Communications Decency Act ("CDA").[18] This Note proposes that Congress amend the CDA and pass legislation akin to this Note's proposed Doxing Notice and Takedown Act to curb cybermobbing.[19]

Section II of this Note describes case studies of cybermobbing and examines its social utility. In Section III, this Note explains why holding individual members of the mob is impracticable under current law. Section IV proposes that Congress amend the CDA and pass the Doxing Notice and Takedown Act.

II. THE PHENOMENON OF CYBERMOBBING

Online shaming is essential for normative role enforcement.[20] But oftentimes, such shaming devolves into cybermobbing, a practice which inflicts irreparable harm unrelated to a violated norm. This section discusses case studies of cybermobbing and evaluates its social utility. On balance, it concludes that cybermobbing has a net negative effect on society and requires a statutory solution.

a. Cybermobbing Case Studies

On December 20, 2013, Justine Sacco made an unforgettable Tweet before boarding a plane from London to Cape Town:

- "*Going to Africa. Hope I don't get AIDS. Just kidding. I'm white!*"[21]

Not only was this Tweet in poor taste, it was also a horrible career move, as Sacco was a corporate communications director at the time.[22] The post remained up while Sacco was in the air, and her account remained unresponsive during the Twitter uproar, which lasted roughly eleven hours.[23] The hashtag "#HasJustineLandedYet" began trending.[24] Days later, Sacco's employer fired her, commenting that it hoped that "time and action, and the

---

[18] Communications Decency Act, 47 U.S.C. § 230 (2018). The term "interactive computer service provider" refers to online platforms like Twitter, Facebook, and YouTube.

[19] *Id.*

[20] *See generally* Klonick, *supra* note 5.

[21] Ed Pilkington, *Justine Sacco, PR Executive Fired Over Racist Tweet, "Ashamed"*, GUARDIAN (Dec. 22, 2013, 6:26 PM), https://www.theguardian.com/world/2013/dec/22/pr-exec-fired-racist-tweet-aids-africa-apology.

[22] *Id.*

[23] *Id*.

[24] *Id.*

forgiving human spirit, will not result in the wholesale condemnation of an individual who we have otherwise known to be a decent person at core."[25]

James Gunn, the director for "Guardians of the Galaxy," was similarly fired after an organized political backlash resurfaced his year-old Tweets, which included pedophilic jokes. [26] After Gunn became a vocal critic of President Trump, Mike Cernovich, an conservative political pundit, dug up Gunn's Tweets and broadcast them on Twitter and on his personal website.[27] He concluded by stating "James Gunn works for Disney," provided Disney's e-mail address, and prompted users to email Disney to ask "why they trust James Gunn around children." Gunn was fired shortly thereafter.[28]

Sarah Jeong faced similar backlash for her Tweets. Jeong, a Harvard Law School graduate, is a writer specializing in the intersection of law and technology.[29] The New York Times's decision to appoint her as a lead technology writer for its editorial board was met with immediate backlash from certain news sites, which reposted her Tweets from years earlier, including:[30]

- *"White men are bullsh*t."*
- *"#cancelwhitepeople"*
- *"Dumb*ss f***ing white people marking up the internet with their opinions like dogs pissing on fire hydrants."*
- *"Are white people genetically disposed to burn faster in the sun, thus logically being only fit to live underground like groveling goblins."*

---

[25] *Id.*

[26] Brooks Barnes, *Disney Fires 'Guardians of the Galaxy' Director Over Offensive Tweets*, N.Y. TIMES (July 20, 2018), https://www.nytimes.com/2018/07/20/business/media/james-gunn-fired-offensive-Tweets.html.

[27] Mike Cernovich, *James Gunn Endorses Pedophilia in 10,000 Deleted Tweets*, CERNO (last accessed Oct. 20, 2019), https://www.cernovich.com/james-gunn-endorses-pedophilia-in-10000-deleted-Tweets/.

[28] Disney later rehired Gunn, but the backlash against Gunn is still referenced in political discussions. *Id.*

[29] *See Author Profile: Sarah Jeong*, FORBES, https://www.forbes.com/profile/sarah-jeong/#432ebf6436f6 (last visited June 1, 2020).

[30] *See, e.g.*, Jack Crowe, *Newest Member of NYT Editorial Board Has History of Racist Tweets*, NAT'L REV. (Aug. 2, 2018, 11:24 AM), https://www.nationalreview.com/news/sarah-jeong-new-york-times-hires-writer-racist-past/.

- *"Oh man it's kind of sick how much joy I get out of being cruel to old white men."*[31]

The cybermob quickly called for her firing.[32] Unlike other cybermobbing victims, though, Jeong's employer decided not to take action based on the social media reactions.[33]

While these thoughtless Tweets speak volumes about their authors, the statement by Sacco's employer rings true. Otherwise decent people say thoughtless things. In the past, such statements might have made for upset water-cooler conversation.[34] The offender might have been fired and could have sought work elsewhere. At worst, the offender could have moved to a different city, where he or she could have started anew. Cybermobs, however, have ensured that these people's names are forever associated with what might have been a temporary lapse in judgment.

Even worse than the cases described above are those in which the alleged inciting incident did not occur at all. A recent example is the Covington Catholic High School debacle. This cybermobbing episode was sparked by a video depicting what seemed to be a disturbing scene: a crowd of MAGA-hatted[35] teenagers harassing a Native American veteran, Nathan Phillips, and engaging with a group of Black Israelites, at the Lincoln

---

[31] Andrew Sullivan, *When Racism is Fit to Print*, N.Y. MAG. (Aug. 3, 2018), http://nymag.com/intelligencer/2018/08/sarah-jeong-new-york-times-anti-white-racism.html (collecting and compiling the controversial Tweets) (altered to obscure profanity).

[32] *Id.*

[33] Jaclyn Peiser, *Times Stands by Editorial Board Member after Outcry Over Old Tweets*, N.Y. TIMES (Aug. 2, 2018), https://www.nytimes.com/2018/08/02/business/media/sarah-jeong-new-york-times.html. In August 2019, Jeong resigned her position on the editorial board, after serving less than a year. Brian Stelter, *Reliable Sources: Sarah Jeong Departs NYT Editorial Board*, CNN BUS. (Sept. 27, 2019), https://mailchi.mp/cnn/rs-sept-27-2019?e=e237f491cb.

[34] *See* Megan Mcardle, *The Power of Social Media Mobs and the Permanence of the Wreckage They Leave Behind*, GOV'T. TECH. (Aug. 23, 2017), https://www.govtech.com/social/The-Power-of-Social-Media-Mobs-and-the-Permanence-of-the-Wreckage-They-Leave-Behind.html.

[35] "MAGA" stands for "Make America Great Again" and was the campaign slogan of President Donald J. Trump. Karen Tumulty, *How Donald Trump Came Up with "Make America Great Again"*, WASH. POST (Jan. 18, 2017), https://www.washingtonpost.com/politics/how-donald-trump-came-up-with-make-america-great-again/2017/01/17/fb6acf5e-dbf7-11e6-ad42-f3375f271c9c_story.html.

Memorial.[36] Nicholas Sandmann, a 15-year old student, was prominent in this video and appeared to be smirking while obstructing Phillips's path.[37] The video quickly spread through social media and polarized the American public.[38] The news coverage and the accompanying cybermobbing, seemingly jumped to conclusions, based on a combination of the short video and interviews with Phillips who claimed the teenagers had surrounded and harassed him.[39]

The backlash on Twitter was immediate and brutal. High-profile celebrities condemned Sandmann and the other students with incendiary language:

- *"Baby snakes"*[40]
- *"Mocking, condescending, disrespecting, ***HOLE"*[41]
- *"Horrible smug ***wipe"*[42]

At least one celebrity called for the doxing of the children present in the video:

- *"Ps. The reply from the school was pathetic and impotent. Name these kids. I want NAMES. Shame them. If you think these ****ers wouldn't dox you in a heartbeat, think again."*[43]

---

[36] Wootson Jr et al., *"It was Getting Ugly": Native American Drummer Speaks on his Encounter with MAGA-hat-wearing Teens*, WASH. POST (Jan. 22, 2019, 3:47 PM), https://www.washingtonpost.com/nation/2019/01/20/it-was-getting-ugly-native-american-drummer-speaks-maga-hat-wearing-teens-who-surrounded-him/.

[37] *Id.*

[38] *Id*.

[39] *See id.*

[40] Jim Carrey (@JimCarrey), TWITTER (Jan. 22, 2019, 2:04 PM), https://twitter.com/JimCarrey/status/1087788108488167424.

[41] Debra Messing (@DebraMessing), TWITTER (Jan. 21, 2019, 12:57 PM), https://twitter.com/DebraMessing/status/1087454142187081729 (altered to obscure profanity).

[42] Rosie O'Donnell (@Rosie), TWITTER (Jan. 19, 2019, 1:52 PM), https://twitter.com/Rosie/status/1086743221802336258 (comparing a picture of Sandmann to a picture of white segregationists assaulting a group of black men) (altered to obscure profanity).

[43] Kathy Griffin (@Kathygriffin), TWITTER (Jan. 20, 2019, 5:05 AM), https://twitter.com/kathygriffin/status/1086927762634399744?lang=en (altered to obscure profanity).

However, further videos did not corroborate Phillips's claims and the cybermob's narrative.[44] First, the teenagers apparently were not harassing Phillips and instead were using school cheers to drown out hateful slurs thrown at them by other protestors.[45] Second, although Phillips had an alternate path to the Lincoln Memorial, Phillips approached Sandmann and the other students with the intention to confront the group.[46]

By the time the full story was uncovered, the damage had been done. Sandmann had been doxed and received numerous death threats and media scorn.[47] His school, Covington Catholic High School, was closed for several days due to bomb threats.[48] Sandmann has since sued numerous news outlets that repeated Phillips' misleading statements.[49] A charitable observer might note that some of the criticisms of Sandmann were based in reality, given that he wore a politically divisive hat in public and arguably thrust himself into the spotlight. But the same cannot be said of the next two cases involving mistaken identity.

After the Boston marathon was bombed on April 15, 2013, a group of individuals gathered on Reddit to find the perpetrator.[50] The group created a subreddit[51] titled "/r/findbostonbombers" and began speculating

---

[44] *See, e.g.*, Michael E. Miller, *Viral Standoff Between a Tribal Elder and a High Schooler is More Complicated Than it First Seemed*, WASH. POST (Jan. 22, 2019, 3:56 PM), https://www.washingtonpost.com/local/social-issues/picture-of-the-conflict-on-the-mall-comes-into-clearer-focus/2019/01/20/c078f092-1ceb-11e9-9145-3f74070bbdb9_story.html.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] Dan Griffin, *No Danger Found at Diocese of Covington; FBI Investigates Packages*, WLWT5 ABC NEWS (Jan. 23, 2019, 11:34 PM), https://www.wlwt.com/article/authorities-respond-to-reports-of-suspicious-package-at-diocese-of-covington/26015081; John London, *Prosecutor: Hundreds of Threats Made Against Covington Catholic After DC March Firestorm*, WLWT5 ABC NEWS (Jan. 23, 2019, 5:31 PM), https://www.wlwt.com/article/prosecutor-hundreds-of-threats-made-against-covington-catholic-after-dc-march-firestorm/26014571#.

[49] Cameron Knight, *Sandmann Files 5 More Defamation Lawsuits Against Media Outlets*, CINCINNATI ENQUIRER (Mar. 3, 2020, 11:51 AM), https://www.cincinnati.com/story/news/2020/03/03/sandmann-files-5-more-defamation-lawsuits-against-media-outlets/4938142002/. *See*, *e.g.*, Sandmann v. WP Co. LLC., 401 F. Supp. 3d 781 (E.D. Ky. 2019).

[50] Alexander Abad-Santos, *Reddit's "Find Boston Bombers" Founder Says "It Was a Disaster" but "Incredible"*, ATLANTIC (Apr. 22, 2013), https://www.theatlantic.com/national/archive/2013/04/reddit-find-boston-bombers-founder-interview/315987.

[51] "Subreddits are subsidiary threads or categories within the Reddit website. They allow users to focus on a specific interest or topic in posting content that gets voted up or down

about the bomber's identity using information found online and in the news.[52] They identified a college student named Sunil Tripathi. Tripathi had been missing since March 16, 2013[53] and resembled "Suspect #2." The F.B.I. had been working with his family to find him.[54] After the group spread its conclusion on Reddit, Tripathi's sister received 58 phone calls on April 19 from reporters looking for a scoop, and from others with less kind words.[55] The Facebook page "Help Us Find Sunil Tripathi," which had previously been set up by Sunil's family when he went missing in mid-March, had to be taken down after users posted a high volume of threatening messages.[56] However, it turned out that Tripathi was missing not because he was hiding, but because he had died before the bombings even took place.[57]

In another case of mistaken identity, Robert Cantrell was wrongfully accused of murdering a seven-year-old black girl named Jazmine Barnes. Barnes had been murdered in a drive-by shooting on the same day that Cantrell had arrested for a separate robbery.[58] Cantrell, who was in custody for the robbery-evasion, resembled the initial composite sketch of Barnes's murderer, an unknown white man with blue eyes.[59] Cantrell was then accused online of the Barnes murder and the incident was labeled a hate crime, drawing the attention of millions of Facebook and Twitter users.[60] Online activist, Shaun King tweeted Cantrell's mug shot to his one million Twitter

---

by relevance and user preference." *Subreddit*, TECHOPEDIA, https://www.techopedia.com/definition/31607/subreddit (last visited Aug. 2, 2019).

[52] Abad-Santos, *supra* note 50.

[53] Jay C. Kang, *Should Reddit Be Blamed for the Spreading of a Smear?*, N.Y. TIMES MAG. (July 25, 2013), https://www.nytimes.com/2013/07/28/magazine/should-reddit-be-blamed-for-the-spreading-of-a-smear.html.

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] Jess Bidgood, *Body of Missing Student at Brown is Discovered*, N.Y. TIMES (Apr. 25, 2013), https://www.nytimes.com/2013/04/26/us/sunil-tripathi-student-at-brown-is-found-dead.html.

[58] *Inmate Once Wrongfully Accused of Killing 7-Year Old Jazmine Barnes Killed Himself Behind Bars*, ABC 13 NEWS (July 20, 2019), https://abc13.com/man-wrongfully-accused-of-killing-jazmine-barnes-kills-himself/5428054/.

[59] Jessica Willey, *Family of Man Wrongfully Accused by Activist Shaun King in Jazmin Barnes' Shooting Speaks Out*, ABC 13 NEWS (Jan. 8, 2019), https://abc7chicago.com/family-of-wrongfully-accused-man-receiving-violent-threats/5034081/.

[60] *Id.*

followers, stating several sources claimed Cantrell was a "racist violent (expletive)."[61] Cantrell's family received death threats.[62] One user threatened Cantrell's niece, stating that "[s]omeone is going to rape, torture and murder the women and children in your family."[63] Investigators cleared Cantrell of any involvement,[64] and two other men were arrested and charged with Barnes's murder. However, the cybermob continued harassing Cantrell and his family.[65] Seven months later, Cantrell killed himself in jail, where he was still imprisoned on the robbery-evasion charge.[66]

b. Defining Cybermobbing and Evaluating its Social Utility

These case studies underscore an important question: Is cybermobbing, on balance, a socially-desirable phenomenon? To answer this question, cybermobbing must first be defined. From the examples above, it is obvious that cybermobbing is similar to cyber harassment and cyberstalking.[67] But while cyber harassment and cyberstalking are often effectuated by a single perpetrator, cybermobbing is a "team sport, with posters trying to outdo each other. Posters compete to be the most offensive, the most abusive."[68] In the case studies above, the victims likely would have suffered more limited real-world harm had the mob been limited to one or two individuals.

Cybermobbing is distinct from bullying, although the separation is thin.[69] Bullying is traditionally defined as: (1) verbal or physical aggression;

---

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Inmate Once Wrongfully Accused of Killing 7-Year Old Jazmine Barnes Killed Himself Behind Bars*, ABC 13 NEWS, *supra* note 58.

[67] CITRON, *supra* note 16, at 3. Citron defines cyber harassment as "the intentional infliction of substantial emotional distress accomplished by online speech that is persistent enough to amount to a 'course of conduct' rather than an isolated incident" and cyberstalking as "an online 'course of conduct' that either causes a person to fear for his or her safety or would cause a reasonable person to fear for his or her safety." *Id.* By contrast, she describes a cybermob as an online group that turns "[o]nline harassment [into] a team sport." *Id.* at 5.

[68] *Id.*

[69] *See* Klonick, s*upra* note 5, at 1034 (discussing the "cyber" distinction, and its impact on exacerbating bullying, shaming, and harassing behaviors).

(2) repeated over time; (3) which involves a power differential.[70] Cybermobbing seems to easily meet the first criterion, verbal aggression. Further, while the members of the cybermob might be, individually, weaker than the victim, the sheer size of the cybermob may implicate a power differential. So, the third criterion seems satisfied, as well. However, the second, repetition over time, is not. Many cybermobbings are single flare-ups, beginning and ending within a week.[71]

Cybermobbing is distinctive due to its relatively recent origins from social media. No formal definition seems to yet exist, but some have defined it as: (1) a group of persons acting in cyberspace, (2) joining together to hold accountable, (3) a victim or victims, (4) for a real or imagined misdeed or faux pas.[72] However, this definition leaves something to be desired.

Cybermobbing does not require "harassment" of the victim directly. That is, the victim need not receive harassing messages personally from the cybermob. And further, "harass" doesn't fully encompass the real-world harm effectuated by cybermobbing. Many victims have their careers ruined for something entirely unrelated to those careers. Therefore, this Note proposes the following definition as more appropriate: (1) a group of persons acting in cyberspace joining together to; (2) dox, threaten, humiliate, or call for physical or pecuniary harm against; (3) victim or victims; (4) for a real or imagined misdeed or faux pas. Given this definition, it is hard to imagine cybermobbing having any utility. However, the real answer is more complicated.

Public shaming and its internet cousin, online shaming via cybermobbing, play a role in social norm enforcement.[73] Online norm enforcement, in turn, is important because it is the "primary social control

---

[70] *Id* (citing EMILY BAZELON, STICKS AND STONES: DEFEATING THE CULTURE OF BULLYING AND REDISCOVERING THE POWER OF CHARACTER AND EMPATHY 28 (2013) (citing DAN OLWEUS, BULLYING AT SCHOOL: WHAT WE KNOW AND WHAT WE CAN DO 142–52 (1993))).

[71] *See id.* at 1046–50 (examples of online shaming and cyber harassment). However, note that Klonick points out that the permanent nature of the internet allows for the mob's posts to be associated with the victim in internet searches for long periods of time. She distinguishes bullying from social shaming in that the latter seeks to enforce a violation of a social norm. *Id.* at 1034.

[72] Winhkong Hua, *Cybermobs, Civil Conspiracy, and Tort Liability*, 44 FORDHAM URB. L. J. 1217, 1246 (2017) (citing to UrbanDictionary.com *Cybermob*, URB. DICTIONARY (Feb. 24, 2008), https://www.urbandictionary.com/define.php?term=cybermob).

[73] *See* Klonick, s*upra* note 5, at 1044.

mechanism of the internet."[74] Online shaming, in this sense, can serve as a replacement for governmental regulation of the internet given the lack of a current online regulatory scheme. Thus, criticizing people for their own words, as happened with Sacco, Jeong, and Gunn, may be socially desirable. Even when such shaming creates real-world harm, such as loss of employment, the social utility of normative role enforcement may outweigh the potentially outsized harm in some instances.

Notwithstanding the possible social utility of online shaming, incidents where cybermobbing involves the doxing of a private individual are always socially undesirable. Cybermobs are able to inflict real-world harm by exposing the victim's private information through doxing. This is problematic for two reasons. First, the dox-inciting incident is often imagined, not real. In instances where there is no misdeed or faux pas, there is no social benefit other than the affirmation that the faux paus *would* have been socially unacceptable—a marginal benefit at best. This is true with the above examples involving Sandmann, Cantrell, and Tripathi. Second, even if the inciting incident actually occurred, the lasting reputational, economic, and dignitary harm suffered by doxing victims normally far outsizes the inciting incident. The damage is permanent.[75] Search engines turn up harmful posts years after the fact,[76] and social media platforms give the cybermob a mechanism to easily reach millions of users.[77] Therefore, cybermobbing via doxing has a net-negative impact on society due to its tendency to inflict irreparable harm unrelated to purportedly-violated social online norms. As explained in Section IV, however, the proposed Doxing Notice and Takedown Act preserves many of the positive aspects of online shaming, while deterring the drawbacks of doxing.

III. VICTIMS CANNOT RECOVER AGAINST CYBERMOBS

Under current law, cybermobbing victims are generally unable to seek adequate relief. Even in the rare event that one is able to make the case for recovery, obtaining it from the mob is impractical and, as explained in Section IV, the CDA limits victims' recourse from ICSPs .[78]

---

[74] *Id.*

[75] CITRON, *supra* note 16, at 4 (noting that using the internet to harass or stalk extends the life of such behavior).

[76] *Id.*

[77] *Id.* at 5.

[78] *See infra* Section IV.

As explained below, under existing law, cybermob victims are blocked from obtaining adequate relief for two reasons. First, an individual mob members' actions generally are not actionable. Second, even if these actions were actionable , or if the victim could otherwise impose some sort of civil conspiracy cause of action,[79] practical difficulties involving internet defendants inhibit recovery.

a. An Individual Member's Cybermob Participation is Likely Not Actionable.

Common law torts and applicable statutes are inadequate remedies as private causes of action against individuals in the cybermob. This section analyzes why both common law torts (tortious interference, privacy, defamation, and intentional infliction of emotional distress) and statutory regimes (cyberbullying) fail as satisfactory remedies for cybermobbing via doxing.

i. Tortious Interference is an Insufficient Remedy.

Tortious interference with a contract seems, at first, like the best bet for recovery for a recently fired cybermobbing victim. The tort occurs when a person, without privilege, induces or causes a third person not to enter or continue a business relation with another.[80] It requires: (1) the existence of a valid contractual relationship; (2) the defendant's knowledge of the existence of the relationship; (3) the defendant's intentional interference with that relationship; (4) absence of justification; and (5) damages resulting from the defendant's wrongful interference with the relationship.[81]

At first, the tort seemingly provides a remedy for Gunn and Sacco, who were fired after public pressure was put on their employers.[82] However, it is unclear whether any one mob member's actions would rise to the level

---

[79] *See* Hua, *supra* note 72, at 1263–64. Hua argues that a civil conspiracy cause of action solves some problems inherent in cybermobbing; namely, the problems of individual non-actionability and personal jurisdiction. *Id.* However, this still leaves the problems of internet anonymity, judgement-proof defendants, and, as Hua points out, the possibility that no true "meeting of the minds" took place. *Id.* at 1263.

[80] 44B AM. JUR. 2D INTERFERENCE § 47 (2019).

[81] These claim elements may vary by jurisdiction. *Id.*(citing e.g., Effs v. Sony Pictures Home Entm't, Inc., 197 So.3d 1243, 1244 n.2 (Fla. 3d DCA 2016)).

[82] *See supra* Section II.

of tortious interference in these cases.[83] Collectively, the statements by the mob had the effect of interfering with the contracts in question. However, the victim could likely not point to any one member of the mob, even the loudest member, to prove there would not have been a breach but for his or her activities, which is what is required under the tort.[84] Further, the employer could point to the inciting incident itself as the reason for firing, rather than the public backlash. And lastly, the reputational harm resulting from a cybermobbing might not instantiate itself in the form of a breached contract. So, tortious interference misses the mark.

ii. Remedies for Privacy Torts are also Insufficient.

The four privacy torts are also near misses: (1) unreasonable intrusion upon the seclusion of another; (2) publicity that places another in a false light before the public; (3) Public disclosure of embarrassing private facts about another; and (4) appropriation of another's name, image or likeness.[85] Intrusion upon seclusion and public disclosure of embarrassing facts both fail as remedies because the nature of cybermobbing is to generally excoriate the victim for a perceived public faux pas. To establish liability, the plaintiff must demonstrate there was an intrusion upon the plaintiff's physical solitude or seclusion, as by invading his or her home or conducting an illegal search.[86] The intrusion must be offensive to a reasonable person.[87] Sandmann was videotaped in a public place, the Lincoln Memorial, so he had no expectation of privacy.[88] Sacco, Jeong, and Dunn were criticized for publicly-posted Tweets, so there is again no argument for unreasonable intrusion. Lastly, Cantrell's arrest information and mugshot were materials of

---

[83] To establish tortious interference with a contract, the plaintiff must show that the defendant actually induced the other party of the contract into breaching it. *See, e.g.,* Maricultura Del Norte, S. de R.L. de C.V. v. Umami Sustainable Seafood, Inc., 769 Fed.Appx. 44, 55 (2d Cir. 2019) (affirming dismissal of tortious interference because plaintiff did not prove "that there would not have been a breach but for the activities of defendants.").

[84] *Id.*

[85] *See generally* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). The last type, appropriation, is obviously not an appropriate remedy and is not discussed further.

[86] 77 C.J.S. *Rights of Privacy and Publicity* § 24 (2020).

[87] *Id.*

[88] *See supra* Section II. Although Sandmann could argue that the disclosure of his name by being doxed was a breach of privacy, he would be unable to pursue the cybermob for the reasons stated *infra* Section III(B).

public record.[89] The only case that is even close is Sunil Tripathi's, whose family maintained a Facebook page dedicated to finding him.[90]

iii. False Light Publicity and Defamation Torts are Impracticable Solutions.

False light publicity also likely fails as a realistic remedy.[91] Many victims—like Sacco, Jeong, and Dunn—were not put in a false light; they were criticized for their own words. And victims who *were* put in a false light, like Sandmann, Tripathi, and Cantrell, must still establish that the defendants "had knowledge or acted in reckless disregard as to the falsity of the publicized matter and false light in which the [victim] would be placed."[92]

Defamation is similar to false light publicity in that it also falls short as a catch-all solution to cybermobbing. The reach of defamation is quite limited because of First Amendment concerns.[93] The tort generally requires: (1) a false and defamatory statement concerning another; (2) an unprivileged publication to a third party; (3) fault amounting to at least negligence on the part of the publisher; and (4) either actionability of the statement irrespective of special harm or the existence of special harm cause by the publication.[94]

---

[89] *For Immediate Release*, MONTGOMERY CTY. (Dec. 31, 2018), http://www.mctxsheriff.org/news_detail_T6_R407.php (last visited Apr. 24, 2020).

[90] *See* Kang, *supra* note 53 (discussing threatening messages posted to the family's Facebook page).

[91] *See generally* 6 AM. JUR. PROOF OF FACTS 3D 585 (originally published in 1989).

[92] RESTATEMENT (SECOND) OF TORTS § 652E(b) (AM. LAW. INST. 1965).

[93] New York Times v. Sullivan, 376 U.S. 254, 279-80 (1964) (holding the First Amendment bars public officials from recovering for defamatory remarks relating to their "official conduct" unless they can prove the statements were made with "actual malice"); Curtis Pub. Co. v. Butts, 388 U.S. 130 (1967) (extending "actual malice" requirement to public "figures," not just public "officials."); Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974) (holding private figures must also establish "actual malice" when seeking "presumed" or "punitive" damages); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985) (narrowing Gertz v. Robert Welch, Inc. by only requiring private figures to prove actual malice to establish presumed damages when defamatory remarks relate to matters of public interest).

[94] These elements are based on Kentucky law. *See* Sandmann v. WP Co. LLC., 401 F. Supp. 3d 781, 787 (E.D. Ky. July 26, 2019) (applying Kentucky law). While the exact elements differ state to state, each state has some requirement that the statement be false

Some authors suggest defamation as a measure against cybermobbing,[95] but this stance overstates the reach of defamation liability. The first element presents an insurmountable sticking point for most victims of cybermobbing because statements made by the cybermob are often true.[96] Even when such statements cast the victim in a false light, they generally constitute assertions of opinion, which, by definition, cannot be false. As illustrated by the dismissal of Sandmann's defamation suit, courts generally agree that such attacks on victims are "nonactionable opinion."[97] Recovery is further complicated when the plaintiff is a public figure.[98] These impediments make defamation an unsatisfying option for cybermobbing victims.

iv. Recovery Under Intentional Infliction of Emotional Distress is also Difficult.

As an alternative to defamation, some authors point to intentional infliction of emotional distress (IIED).[99] However, recovering under IIED

---

and defamatory. *See, e.g.*, 128 AM. JUR. TRIALS 1, ch.II.A §§ 3–8 (originally published in 2013).

[95] *See* Klonick, *supra* note 5, at 1059–60 (pointing to defamation law as "a relatively effective protection against unhinged shaming," but also noting problems with litigation expenses, judgment-proof defendants, and anonymous defendants). *See also*, Cory Batza, *Trending Now: The Role of Defamation Law in Remedying Harm from Social Media Backlash*, 44 PEPP. L. REV.429, 452–74 (2017). Batza points out many of the difficulties cybermobbing victims face in recovering for defamation; such as the CDA immunity for ISPs, anonymous defendants, and nonactionable opinions. *Id.* at 452–54. Instead of advocating for alternative causes of action for cybermobbing victims, though, Batza argues that courts should reach certain findings in their defamation analyses. *Id.* at 459–74. Namely, Batza argues that the average social media user shouldn't be considered a public figure because of his or her use of the Internet, even for a limited purpose, and that mob shaming should not be considered a matter of public concern. *Id.*

[96] *See, e.g.*, *infra* Section II.a.

[97] *See Sandmann*, 401 F. Supp. 3d at 791–94 (dismissing defamation claims as not actionable because the statements did not specifically reference Sandmann and/or did not state or imply "actual, objectively verifiable facts", and because the social media scorn was beyond the four corners of the written communication at issue). Sandmann presumably did not sue individual Twitter users because the Tweets directed at him would similarly be considered nonactionable.

[98] *See, e.g.*, 6 AM. JUR. PROOF OF FACTS 3D 585, *supra* note 91, at § 11 (in jurisdictions that make the private/public distinction, a plaintiff who is a public figure must make a showing of "actual malice" by the defendant).

[99] *See* Klonick, *supra* note 5, at 1059–60; Gallardo, *supra* note 2, at 731.

can be incredibly difficult.[100] Plaintiffs must prove: (1) extreme and outrageous conduct with either the intention of, or reckless disregard for, causing emotional distress; (2) the suffering of severe or extreme emotional distress; and (3) actual or proximate causation.[101] IIED is not a workable solution because it is strongly disfavored in the law.[102] Only the most egregious conduct is sufficient to satisfy the first element.[103] Posting mean things on the internet likely does not qualify. So, IIED, like other common law torts, is an inadequate remedy for cybermobbing.

v. Current Statutory Regimes Provide Insufficient Remedies.

Current statutory protections, such as cyberbullying statutes, are also insufficient. While some of the conduct described above certainly fits with a conventional understanding of the term "bullying," such statutes do not protect cybermobbing victims. While states have methods of prohibiting bullying and cyberbullying, they only protect students and children, not adults.[104] Additionally, many of these statutes are only "model acts," which do not necessarily carry the full force of law.[105] Further complicating things is the fact that Congress has not acted directly on cyberbullying and the laws that do exist do not create private rights of action. Cyberbullying statutes do not fully address the problem of cybermobbing.

b. Even if a Cause of Action Fits, Practical Difficulties Bar Recovery.

Assuming the victim had a meritorious claim, additional practical issues would bar recovery. Oftentimes, the mob is composed of anonymous or pseudonymous members, so the victim does not know who to sue. But even if the victim can correctly identify defendants, two more issues appear.

---

[100] 136 AM. JUR. 3D *Recognition of IIED* § 2 (2013) (describing conduct warranting liability under this tort as "a very small slice of human behavior").

[101] *Id.* at § 4.

[102] Andrews v. Staples the Office Superstore East, Inc., 2013 WL 3324227, at *15 (W.D. Va. July 1, 2013).

[103] *See, e.g.*, Medcalf v. Walsh, 938 F. Supp. 2d 478, 488 (S.D. N.Y. Apr. 9, 2013) ("Only the most egregious conduct has been found sufficiently extreme and outrageous to establish this tort").

[104] *See, e.g.*, Minn. Stat. § 121A.031 (defining bullying as harmful conduct that involves "an actual or perceived imbalance of power between the *student* engaging in prohibited conduct . . . .") (emphasis added); Cal. Ed. Code § 48900 (similarly using the language "pupil" to define bullying).

[105] *Laws, Policies, & Regulations*, STOP BULLYING.GOV, https://www.stopbullying.gov/laws/index.html (last reviewed Jan. 7, 2018).

First, members of the mob may be judgment-proof. Second, the sheer number of people involved in most cybermobs makes it impracticable to identify, serve, and enforce a judgment on all or any of them. The amount of resources required to do so would be prohibitive. Therefore, the victim is all but barred from suing individual mob members. As explained below, the victim cannot simply turn to the online platform, the "ICSP," for relief, either.

IV. THE COMMUNICATIONS DECENCY ACT DOES NOT DETER CYBERMOBBING AND SHOULD BE SUPPLEMENTED BY THE DOXING NOTICE AND TAKEDOWN ACT.

ICSPs are immune from liability for cybermobbings under the CDA.[106] Section 230 of the CDA clarifies that ICSPs do not become "publishers" of material when they exercise "Good Samaritan" blocking and screening of offensive material.[107] Section 230 has been interpreted broadly, preventing ICSP liability for essentially all user postings except for child pornography, intellectual property violations, and other select types of content.[108] After summarizing the history of the CDA in subsection A of Section IV, subsection B argues that Congress should amend the CDA and pass the Doxing Notice and Takedown Act ("DNTA"), the sample legislation proposed by this Note and included in Appendix A. Subsection C walks through the sample legislation and explains why it is consistent with the First Amendment.

a. History of the Communications Decency Act

The CDA was passed as an amendment to the Telecommunications Act of 1996.[109] Specifically, the "Good Samaritan" provision of the CDA

---

[106] 47 U.S.C. § 230 (2018).

[107] *Id.*§ 230(c).

[108] Hassell v. Bird, 420 P.3d 776, 793 (Cal. 2018); KATHLEEN ANN RUANE, CONG. RESEARCH SERV., LSB10082, HOW BROAD A SHIELD? A BRIEF OVERVIEW OF SECTION 230 OF THE COMMUNICATIONS DECENCY ACT 2 (2018), https://fas.org/sgp/crs/misc/LSB10082.pdf; Matt Laslo, *The Fight Over Section 230—and the Internet as We Know It,* Wired (Aug. 13, 2019, 3:18 PM), *https:*//www.wired.com/story/fight-over-section-230-internet-as-we-know-it/.

[109] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified as amended in scattered sections of 47 U.S.C.).

was a reaction to *Stratton Oakmont, Inc. v. Prodigy Services Co*,[110] where the defendant, Prodigy, was penalized for screening materials posted to its site to make it more family-friendly.[111] The court held that, by screening the posts, Prodigy had made itself a "publisher" of the posts and thus, was liable for any defamatory remarks it failed to exclude.[112] Under this reasoning, Prodigy could have only avoided publisher liability if it allowed users to post freely without screening. Fearing the twisted incentive created by the *Stratton Oakmont* court, Congress passed the "Good Samaritan" provision of the CDA.[113] The section reads:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
>
> (1) Treatment of publisher or speaker
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) Civil liability
> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the

---

[110] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1995); H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.) (stating one of the purposes of § 230 was to "overrule Stratton Oakmont v. Prodigy"). *See also* Olivera Medenica & Kaiser Wahab, *Does Liability Enhance Credibility? Lessons from the DMCA Applied to Online Defamation*, 25 CARDOZO ARTS & ENT. L.J. 237, 247 (2007); Gallardo, *supra* note 2, at 733–35.

[111] *Stratton Oakmont*, 1995 WL 323710 at *2.

[112] *Id.* at *4.

[113] H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.) (stating one of the purposes of 230 was to "overrule Stratton Oakmont v. Prodigy."). *See* also Medenica & Wahab, *supra* note 110, at 249–50; Gallardo, *supra* note 2, at 734–35.

> technical means to restrict access to material described in paragraph (1).[114]

In addition to overruling *Stratton Oakmont*, the CDA's § 230 was intended to generally protect the growth and expansion of the internet, preserve a vibrant free market unfettered by regulation, encourage technological development, and "ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer."[115]

The Fourth Circuit, in *Zeran v. Am. Online*, was the first appellate court to apply § 230.[116] Beyond laying out the elements an ICSP must prove to avoid liability using the § 230 carveout,[117] the *Zeran* court controversially went one step further. The *Zeran* court held that § 230 immunity applied to all claims not explicitly excluded in the CDA statute.[118] Since then, courts have used the CDA to bar ICSP liability for defamation, employment torts, negligent misrepresentation, cyberstalking, and breach of contract.[119] Thus, despite the legislative purpose provision in § 230(b) seemingly endorsing the punishment of online harassment, courts have broadly interpreted the Good Samaritan immunity provision to prevent ICSP liability for such harassment.[120]

b. Congress Should Augment the Communications Decency Act by Passing the Doxing Notice and Takedown Act.

Section 230 of the CDA is far from universally loved. Many argue that it creates similar incentives to the *Stratton Oakmont* court's holding, such that ICSPs are encouraged to leave content unfiltered in order to avoid

---

[114] 47 U.S.C. § 230(c) (2018).

[115] *Id.* § 230(b).

[116] Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).

[117] *Id.* at 328–35.

[118] *Id.* at 330–34; *see also* Cecilia Ziniti, *The Optimal Liability System for Online Service Providers: How Zeran v. America Got it Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L. J. 583, 585 n.14 (2008) (collecting cases) .

[119] Ziniti, *supra* note 118, at 585. *But see* Doe v. Internet Brands, Inc., 824 F.3d 846, 854 (9th Cir. 2016) (holding that § 230 does not protect an ISP against a failure-to-warn claim).

[120] *See* Ziniti*, supra* note 118, at 585.

publisher-liability and unnecessary cost.[121] Some legal commentators assert that the CDA section should nonetheless be left untouched.[122]

Other spectators disagree.[123] Proposed solutions include: a flat-out repeal of the CDA,[124] amending the CDA and imposing notice and takedown regime for defamatory statements,[125] and free-market solutions.[126] While many of these proposals have merit, this Note proposes that the best solution would be legislation that imposes a notice and takedown regime for posts that dox private individuals. This proposed statute would be consistent with the original Congressional intent behind the CDA and would preserve many of the benefits of online shaming, while resulting in the optimal amount of information being disseminated online.

i. The DNTA is Consistent With the Legislative Intent Behind the CDA.

Courts have interpreted the CDA to generally immunize ICSPs from liability for any harm caused on their platforms.[127] This statutory interpretation departs from the original legislative intent behind the CDA, which specifically addressed ICSP-publisher liability for attempts to block violent or obscene sexual material.[128] Congress should amend the CDA and pass the DNTA to return to the original legislative intent behind the CDA.

Currently, the CDA is inadequate to combat cybermobbing. Further, addressing cybermobbing is likely beyond the scope of the CDA, as the CDA was passed to combat defamation. Defamation is distinct from cybermobbing for several reasons. First, publisher liability for defamation far

---

121 Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003).

122 *See generally* Ziniti, *supra* note 118.

123 *Id.*

124 *See* Matthew G. Jeweler*, The Communications Decency Act of 1996: Why § 230 Is Outdated and Publisher Liability for Defamation Should Be Reinstated Against Internet Service Providers,* 8 U. PITT. J. TECH. L. & POL'Y 1, 1 (2007).

125 *See* Medenica & Wahab*, supra* note 110, at 239.

126 Gallardo, *supra* note 2, at 741–43.

127 *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

128 Communications Decency Act of 1996, Pub. L. No. 104–104, 110 Stat. 138 (1996) (codified as amended in scattered sections of 47 U.S.C.); *Stratton Oakmont*, 1995 WL 323710, at *1 (superseded by statute, Communications Decency Act, 47 U.S.C. § 230, as recognized in Shiamili v. Real Est. Grp. of N.Y., Inc., 952 N.E.2d 1011 (N.Y. 2011)).

predates the advent of the internet.[129] Second, defamation relates to a unique sort of harm, whereas cybermobbing is linked to a more general, extensive harm. Finally, a defamer is not reliant on an online publisher or platform to defame a plaintiff. In contrast, a cybermobbing incident cannot occur without a social media platform. Further, cybermobs are uniquely enabled by the "low-cost, anonymous, instant, and easy access to the internet" made possible by social media sites.[130] In this sense, cybermobbings could be analogized to other torts; the ease of cybermobbing could reflect a "defect" by the ICSP under product liability[131] or negligent entrustment of a chattel if property is misappropriated while using the platform.[132] Because of these differences from defamation, the CDA is not adequate to frustrate cybermobbing.

The CDA is one of the most consequential laws governing the internet, but most of the modern internet and its modern problems—including cybermobbing— did not exist when the CDA was passed in 1996.[133] Thus, Congress could not have anticipated provider immunity for cybermobbing within the CDA, because the phenomenon had not yet occurred. Although proponents of the CDA could argue that § 230(b) was intended to establish immunity against unforeseen types of harm in order to foster the growth of the internet,[134] they would need to ignore, or at least deemphasize, other

---

[129] *See* 6 AM. JUR. PROOF OF FACTS 3D 585, *supra* note 91 (discussing defamation cases predating the internet).

[130] Klonick, *supra* note 5, at 1031 (noting that this easy access "has eviscerated whatever 'natural' limits there were to public shaming and has served to amplify its effects.").

[131] Users are far more likely to send hateful and incendiary messages when using an online platform. *See* CITRON, *supra* note 16. One could argue that the failure of an ICSP to take this into account when constructing and maintaining its platform could be considered a "defect."

[132] RESTATEMENT (SECOND) OF TORTS § 308 (1965) (defining the tort of negligent entrustment). *But cf. Doe*, 347 F.3d at 661 (rejecting this theory when ISP hosted website which sold videos of underage male athletes).

[133] "When the most consequential law governing speech on the internet was created in 1996, Google.com didn't exist and Mark Zuckerberg was 11 years old." Daisuke Wakabayashi, *Legal Shield for Websites Rattles Under Onslaught of Hate Speech*, N.Y. TIMES (Aug. 6, 2019), https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html.

[134] The policy section found in 47 U.S.C. § 230(b) (2018) provides that:

> It is the policy of the United States—
>
> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

language in § 230, which notes the policy goals of deterring of "harassment by means of computer."[135] In short, the DNTA is not a radical proposition; it is consistent with what the legislature originally intended and would bring the CDA more squarely into the 21st century.

ii. Public Policy Supports a Change From Total Immunity.

There are significant public policy arguments that support a change to the current CDA regime. The CDA allows cybermobs to use social media platforms to cause damage that would otherwise be considered tortious if done through a different medium or if effectuated by one individual acting alone.[136] Even worse, it leaves ICSPs with no incentive to prevent cybermobbings. As explained by then-Circuit Judge Frank Easterbrook, if § 230(c)(1) "blocks civil liability when web hosts and other Internet service providers (ISPs) refrain from filtering or censoring the information on their sites,"[137] then:

> § 230(c) as a whole makes ISPs indifferent to the content of information they host or transmit . . . . As precautions are costly, not only in direct outlay but also in lost revenue from the filtered customers, ISPs may be expected to take the do-nothing option and enjoy immunity under § 230(c)(1). . . .

> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
> (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

[135] *See id.* § 230(b)(5).

[136] *See supra* Section III (discussing the general lack of relief available to cybermobbing victims). For instance, if one individual achieved the result of getting a victim fired, they may be liable for tortious interference with a contract. Change the medium, the number of perpetrators, and the public nature of the wrong, and suddenly relief for the victim disappears.

[137] Doe v. GTE Corp., 347 F.3d 655, 659 (7th Cir. 2003).

> Why should a law designed to eliminate ISPs' liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?[138]

Judge Easterbrook resolved the tension between the statute's title ("Protection for 'Good Samaritan' Blocking and Screening of Offensive Material") and its text (which protects ICSPs when they fail to block offensive material) by yielding to its text.[139] But, as explained above, the legislative intent behind § 230 supports a finding that CDA immunity should not be all-encompassing.

Concerns with amending the CDA relate to the suppression of online speech. These concerns are held by some of the biggest players in the tech industry, many of whom provided written testimony at a late 2019 House Commerce Committee meeting on § 230 of the CDA.[140] Steve Huffman, the CEO of Reddit, testified that "even small changes to [the CDA] will have outsized consequences for our business, our communities, and what little competition remains in our industry."[141] Huffman maintained that Reddit's self-moderation policy is an adequate measure for content control. Eliminating § 230, he explained, would destroy Reddit's ability to make good-faith content moderation, and even a slight narrowing of § 230 would create an unworkable regulatory burden on small social media sites and would "chill discussion and hurt the vulnerable."[142]

---

[138] *Id.* at 659–60.

[139] *Id* (citing Brotherhood of R.R. Trainmen v. Baltimore & Ohio R.R. Co., 331 U.S. 519, 528–29 (1947)).

[140] *Fostering a Healthier Internet to Protect Consumers: Hearing Before the H. Comm. on Energy and Commerce*, 116th Cong. (2019). For a summary of the hearing and some attendant commentary, *see* Eric Goldman, *Roundup of the House Commerce Committee Hearing on Section 230*, TECH. & MARKETING L. BLOG (Oct. 17, 2019), https://blog.ericgoldman.org/archives/2019/10/roundup-of-the-house-commerce-committee-hearing-on-section-230.htm.

[141] Steve Huffman, Co-Founder and CEO of Reddit, Inc., Testimony Submitted for the Record at U.S. House of Representatives Committee on Energy and Commerce Hearing on "Fostering a Healthier Internet to Protect Consumers" 1 (Oct. 16, 2019), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Huffman_rev.pdf.

[142] *Id* at 3 (comma removed).

Katherine Oyama, a Google representative, gave a similar statement.[143] She stated that, without § 230, any sites that moderate content could be held liable for defamatory statements, which would result in companies either ceasing to filter content, leading to more harmful content, or over-filtering content, leading to suppression of political speech.[144]

Concerns about the CDA's protection of speech are not uncommon.[145] As Elliot Harmon, a director at the Electronic Frontier Foundation, stated:

> If lawmakers weakened Section 230, they wouldn't just be threatening those spaces—they would risk kicking some people completely off the internet. Without Section 230, platforms would effectively have to determine the risk of a user before that user would ever be allowed to speak.[146]

These arguments have merit—unfettered internet speech is certainly a priority. However, updating the CDA is, on balance, a better policy than leaving it as is. As a preliminary matter, these statements anticipate a complete abandonment of the CDA, a position not advocated by this Note. If the DNTA became law, the CDA would continue to protect good-faith provider screening of content, but limit total ICSP immunity.

Total ICSP immunity under the CDA is bad policy for two additional reasons. First, the above tech executives' statements only consider the suppression of speech caused by over-screening content; they do not fairly consider the speech that is discouraged by under-screening. For example, providers' failure to screen content inevitably results in harassment. Users facing such harassment may be intimidated into not participating, which reduces the quantity and quality of online speech. As Danielle Keats Citron, a professor of law at Boston University, noted in her testimony:

---

[143] *See generally* Katherine Oyama, Global Head of Intellectual Property Policy, Google, Inc., Written Testimony for U.S. House of Representatives Committee on Energy and Commerce Hearing on "Fostering a Healthier Internet to Protect Consumers" (Oct. 16, 2019), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Oyama.pdf.

[144] *Id.* at 4–5.

[145] Elliot Harmon, *Changing Section 230 Would Strengthen the Biggest Tech Companies*, N.Y. TIMES (Oct. 16, 2019), https://www.nytimes.com/2019/10/16/opinion/section-230-freedom-speech.html.

[146] *Id.*

> More often, targeted individuals are women, women of color, lesbian and trans women, and other sexual minorities. They do not feel safe on or offline. They experience anxiety and severe emotional distress. Some victims move and change their names. In the face of online assaults, victims have difficulty finding employment or keeping their jobs because the abuse appears in searches of their names. Online abuse not only makes it difficult to make a living, but it silences victims. Targeted individuals often shut down social media profiles, blogs, and accounts.[147]

Second, total provider immunity, as § 230 currently provides for, enables cybermobbings, which have a net-negative social impact when they involve doxing private individuals. Cybermobs often obfuscate the truthfulness of an individual's perceived social faux paus, which limits social utility stemming from harassment of an individual. The cybermob's pursuit of doxing based on a particular incident has significant consequences for victims, such that victims are often fired or otherwise suffer irreparable reputational, financial, or emotional harm unrelated to any social norm they violated. Amending the CDA and passing the DNTA would help address these issues.

c. What is the DNTA and How is it Consistent With the First Amendment?

Congress should amend the CDA and pass the DNTA to address the numerous issues referenced in this Note.[148] The proposed legislation borrows from the notice and takedown structure of the Digital Millennium Copyright Act ("DMCA") to create a notice and takedown regime for online posts that dox private individuals.[149] The DNTA also borrows some

---

[147] Danielle Keats Citron, Professor of Law, Boston University School of Law, Prepared Written Testimony and Statement for the Record for U.S. House of Representatives Committee on Energy and Commerce Hearing on "Fostering a Healthier Internet to Protect Consumers" 7 (Oct. 16, 2019) (internal citations omitted), available at https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony_Citron.pdf.

[148] For the DNTA to be effective, the CDA must be amended as shown in Appendix A, where the text of the DNTA is also available. *See infra* Appendix A.

[149] *See generally infra* Appendix A; 17 U.S.C. § 512 (2018) (detailing the notice-and-takedown regime under the DMCA).

principles from defamation law, but relies on doxing-based liability, rather than publisher liability, for defamation.

If a person discovers his or her personal information online, the DNTA allows that person to contact the ICSP to request the information be taken down.[150] The ICSP must have a publicly-available channel in which to receive such requests.[151] Upon receiving a request, the ICSP must take down the offending post within twelve hours, provided that the request meets the statutory guidelines.[152] At this point, the person who posted the information may provide counter-notification alleging specific facts and circumstances showing that the victim is not a private individual, but instead is a public figure.[153] If the poster provides such a showing, the ICSP must restore the posts unless the victim files for an injunction.[154] The DNTA punishes the misrepresentation of both the nature of the posts and the status of the victim as a private or public individual.[155]

Failure to meet these guidelines results in the ICSP being liable to any doxed victim for statutory damages.[156] From there, the ICSP may seek contribution from those who actively participated in the doxing.[157] This contribution clause deters would-be cybermobbers and, by shifting the risk of judgment-proof defendants onto ICSPs, incentivizes ICSPs to prevent cybermobs from occurring.

The DNTA also borrows from defamation law, in that it is similarly focused on protecting private individuals rather than public figures.[158] This focus on protecting private individuals more easily aligns with the First Amendment,[159] and is an important first step towards addressing cybermobs via doxing. It is also important that the DNTA protects individuals, rather

---

[150] *See infra* Appendix A, DNTA § (a)(1)(C).
[151] *See infra* Appendix A, DNTA § (b).
[152] *See infra* Appendix A, DNTA § (a)(2)(A).
[153] *See infra* Appendix A, DNTA § (a)(3)(A).
[154] *See infra* Appendix A, DNTA § (a)(3).
[155] *See infra* Appendix A, DNTA § (c).
[156] *See infra* Appendix A, DNTA § (f).
[157] *See infra* Appendix A, DNTA § (g).
[158] While the distinction between a private and public figure can be unclear in certain situations, courts have generally considered candidates for public office and people who have achieved pervasive fame or notoriety as "public figures." *See, e.g.*, Curtis Pub. Co. v. Butts, 388 U.S. 130, 154 (1967).
[159] *See infra* Section IV(c)(2).

than legal entities such as corporations, partnerships, or limited liability companies, both because (1) legal entities would not suffer the same particular harm that private individuals experience from doxing and (2) ICSPs might become incentivized to preemptively remove criticism of these entities to avoid liability. Although federal law provides some protection from doxing for certain public employees and others involved in the justice system,[160] separate legislation would need to be considered to protect public figures and public employees. This additional legislation would require a closer examination of First Amendment principles, free speech norms, and underlying policy incentives. However, this analysis is beyond the scope of this Note.

The DNTA prioritizes liability for doxing, rather than defamation, harassment, threats, or other features of cybermobbing, for three reasons. First, is the practicality consideration; doxing is easy to recognize. While harassment and threats may resemble legal criticism in certain instances, doxing and exposing a private individual's personal information never resembles appropriate speech. Second, doxing presents the few First Amendment implications. While First Amendment exceptions exist for threats and harassment,[161] ICSPs may react adversely to potential liability for threatening or harassing posts and preemptively remove actually harmless posts. This chilling effect certainly would have First Amendment concerns.[162] Because posts including personal information are easily recognized, this limits the overinclusive chilling effect of taking down harmless posts. Finally, cybermobs have greater social utility when they cannot dox their victims.[163] The exposure of personal information is what allows cybermobs to inflict real world harm and thus have net-negative social utility. By eliminating doxing, the DNTA allows cybermobs to continue enforcing norms by condemning socially-undesirable behavior while, at the same time, preventing them from imposing long-term reputational, financial, and emotional harm on individuals.

---

[160] *See* 18 U.S.C. § 119 (2018) (criminalizing the posting of private information regarding specific individuals performing certain defined duties with intent).

[161] *See infra* Section IV(c)(2).

[162] *See* Note, *Section 230 as First Amendment Rule*, 131 HARV. L. REV. 2027, 2032–47 (2018) (arguing that the First Amendment requires a rule similar to §230) [hereinafter Note, *Section 230 as First Amendment Rule*].

[163] *See, e.g.*, Klonick, *supra* note 5, at 1055–57 (providing example of "manspreading" as a positive use of online shaming, which occurred without a specific doxing or cyber harassment of an individual).

Because the DNTA proposes to amend the CDA and to impose liability for certain types of speech, constitutional questions arise. To pass muster, the DNTA must overcome two hurdles. First, in order to limit ICSP immunity for doxing, the CDA cannot be a First Amendment rule. Second, the DNTA itself must pass separate constitutional scrutiny. The DNTA survives both .

i. The CDA is Not Required by the First Amendment and Therefore the DNTA May Allow for Limited Doxing Immunity.

Although many judges and academics assume that the First Amendment does not require § 230 of the CDA,[164] some scholars argue otherwise.[165] Specifically, these scholars assert that the First Amendment requires that ICSPs should be shielded from secondary liability for both speech that is protected by the First Amendment and for speech that is not constitutionally-protected, such as defamatory statements.[166] These commentators argue that "the private censorship produced by defamation liability for internet intermediaries cannot be justified by a government interest in defamation law."[167] They further argue that since courts have used the First Amendment to pare back defamation liability,[168] courts could similarly pare back secondary liability for defamation in the online context.[169] This, they argue, leads to an optimal amount of information being disseminated in society.[170] Any contrary rule has the potential for collateral censorship which cannot be justified by any valid governmental interest.[171] However, this argument that the First Amendment requires this secondary liability for ICSPs goes too far, and therefore should fail.

However vital the role of unfettered political speech is, it does not require that ICSPs have complete immunity from secondary liability as a matter of constitutional dictate. Further, this expanded immunity would not result in optimal information creation and distribution. As this Note discusses , cybermobbing has significant and harmful economic externalities.

---

[164] Note, *Section 230 as First Amendment Rule*, *supra* note 162, at 2030 (citing, for example, *Batzel v. Smith*, 333 F.3d 1018, 1020 (9th Cir. 2003)).

[165] Note, *Section 230 as First Amendment Rule*, *supra* note 162, at 2035.

[166] *Id.*

[167] *Id.* at 2028.

[168] *See id.* at 2029.

[169] *Id.* at 2046.

[170] *Id.*

[171] *Id.* at 2035–42.

Because the criminalization of doxing private individuals would reduce these externalities, the DNTA would actually increase the social utility of public shaming.

Finally, § 230 protection as a First Amendment requirement faces an uphill battle. As mentioned, the majority of courts and scholars argue that the First Amendment does not require § 230 .[172] Rather, § 230 simply "reflects a 'policy choice,' not a First Amendment imperative."[173] Internet speech would be preserved by a far more reasonable rule, rather than one establishing complete immunity for ICSPs. Because the First Amendment does not require § 230, and therefore would not require the complete immunity for ICSPS, the DNTA may reduce immunity for doxing content. Specifically, the DNTA would serve to protect speech while also deterring cybermobbing and ensuring victims harmed by a cybermobbing receive compensation.

ii. The DNTA Survives First Amendment Scrutiny.

The First Amendment provides that "Congress shall make no law . . . abridging the freedom of speech."[174] Protection of free speech is substantial, extending even to "ideas that the overwhelming majority of people might find distasteful or discomforting."[175] However, this protection is subject to numerous exceptions.[176] The DNTA's imposition of liability for statements that dox private individuals is consistent with policies underlying two of these First Amendment exceptions.

First, a close common law analogy to doxing is the tort of publication of private information.[177] Although a publisher of this information would generally be tortiously liable, the First Amendment provides limited

---

[172] Note, *Section 230 as First Amendment Rule*, *supra* note 162, at 2030 (citing, for example, *Batzel v. Smith*, 333 F.3d 1018, 1020 (9th Cir. 2003)).

[173] Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 421 (S.D. N.Y. Mar. 14, 2001) (citing Zeran v. Am. Online, Inc. 129 F.3d 327, 330–31 (4th Cir. 1997).

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

[175] Virginia v. Black, 538 U.S. 343, 358 (2003) (citing Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting)).

[176] Chaplinsky v. New Hampshire, 315 U.S. 568, 571–72 (1942) ("[T]he right of free speech is not absolute at all times and under all circumstances. There 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.").

[177] *See supra* Section III.

immunity for published information that relates to threats to public safety[178] or other matters of public concern.[179] The DNTA aligns with this exception in two ways. First, the proposed DNTA only protects private individuals, not public figures or individuals who "otherwise voluntarily entered the public eye because of a particular matter of public concern."[180] Second, the DNTA limits actionable harm to the exposure of a private individual's home address, place of work, school, real name, or similar personal information.[181] For the majority of cases, it is unlikely that the exposure of this information would be considered a matter of public concern. In the event that this private information would be of public concern, then it is likely that no actionable harm has occurred.

The DNTA further conforms to the constitutional boundaries defined by case law implicating First Amendment rights. In *Chaplinsky v. New Hampshire*, the Supreme Court upheld a statute that prohibited using offensive, derisive, or annoying language to deride, offend, or annoy someone lawfully in a public place.[182] The defendant challenged the constitutionality of the statute under the First Amendment after he yelled at a police officer, "You are a God damned racketeer . . . a damned Fascist," in a public place.[183] In affirming the conviction, the Court pointed to an exception to the First Amendment for lewd, obscene, profane, libelous, insulting, or fighting words—"those which by their very utterance inflict injury or tend to incite an immediate breach of the peace."[184] Because the statute was intended to prevent breaches of the peace, it posed no constitutional issue.[185]

Chaplinsky is not a relic of a more genteel past. In 1969, the Court in *Watts v. United States* explained that states may prohibit "true threats" and still be consistent with the First Amendment.[186] In *Black v. Virginia*, a 2003 case, the Supreme Court relied on *Chaplinsky* to uphold a similar statute prohibiting the burning of crosses "with the intent of intimidating any

---

[178] Bartnicki v. Vopper, 532 U.S. 514, 534 (2001).

[179] *See generally* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 490 (1975).

[180] *See* DNTA's proposed definition of "private individual," *infra* Appendix A, DNTA § (d)(4).

[181] *Infra* Appendix A, DNTA § (d)(1)(A).

[182] *Chaplinsky*, 315 U.S. at 569.

[183] *Id.*

[184] *Id.* at 572.

[185] *Id.*

[186] Watts v. United States, 394 U.S. 705, 708 (1969).

person or group of persons."[187] In short, fighting words, threats, and statements constituting a breach of the peace are not protected by the First Amendment.

While doxing itself might not constitute "fighting words," the activity is certainly used to intimidate and threaten individuals, whether explicitly or implicitly. Having your home address, place of work, school, or name published online, could very reasonably instill fear of bodily harm.[188] Thus, the DNTA likely would not violate the First Amendment because of the carveout for speech which implies threat of bodily harm to individuals, and the DNTA would pass constitutional muster.

V. CONCLUSION

Cybermobs have a net-negative impact on society when they are able to dox their victims by exposing and publishing private personal information online. They often obfuscate the truth or falsity of underlying incidents and create wildly-outsized consequences for alleged wrongdoers. A victim of cybermobbing is practically barred from seeking justice from the mob using existing causes of action, and the CDA should not be an additional hurdle to recovery. Thus, Congress should amend the CDA and pass the DNTA to impose liability onto ICSPs for cybermobs for doxing private individuals. This would deter online malfeasance and incentivize ICSPs to foster useful and productive online spaces. While the DNTA does not address all of the problems related to online harassment and cybermobbing, its passage would be an initial step in the providing greater protection for users of the modern internet.

---

[187] *Black*, 538 U.S. at 347–48.

[188] *See generally* CITRON, *supra* note 16.

APPENDIX A

Amendment to the Communications Decency Act:

"The following paragraph shall be added at the end of subsection (e) as subparagraph (6):

> 'Nothing in this section shall be construed to limit the application of the Doxing Notice and Takedown Act.'"

The Doxing Notice and Takedown Act:

(a) In general

(1) A service provider shall not be liable for monetary, injunctive, or other equitable relief under this Act by reason of storage, at the direction of a user, of messages or statements that reside on a system or network controlled, operated by, or for the service of the provider, if the service provider:

(A) does not have actual knowledge that such messages or statements on the system or network cause actionable harm;
(B) upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the messages or statements; and
(C) upon notification, responds expeditiously to remove or disable access to the messages or statements that are claimed to cause actionable harm.

(2) A service provider shall be liable for monetary, injunctive, or other equitable relief under this Act to a private individual if:

(A) within 12 hours after receiving notification under paragraph (c), the service provider fails to remove or disable access to messages or statements causing actionable harm in which the private individual is identified; or
(B) the service provider fails to designate an agent under paragraph (b) and a private individual is subsequently identified by messages or statements causing actionable harm.

(3) The service provider shall not be liable for monetary relief if it restores the messages or statements allegedly causing actionable harm after a participating individual has filed a counter-notification providing an initial showing that:

(A) the person identified in messages or statements is not a private individual; or

(B) the messages or statements do not cause actionable harm, unless the person identified files for injunctive relief in a court of competent jurisdiction.

(4) If the service provider removes or disables access to messages or statements causing actionable harm in which the private individual is identified within 12 hours after receiving notification and the message or statements are not restored, the private individual may seek monetary relief from participating individuals. The court shall award monetary relief upon finding that the claimant is a private individual and that the messages or statements caused actionable harm.

(5) The service provider shall adopt, reasonably implement, and inform subscribers and users of the service provider's system or network policy that provides for the termination in appropriate circumstances of repeat participating individual subscribers and users from the service provider's system or network.

(b) Designated agent

The limitations on liability established in this section apply to a service provider only if the service provider has designated an agent to receive notifications relating to claims of actionable harm. To designate an agent pursuant to this subsection, the service provider must make the agent's certain contact information available through its service, including on its website in a location accessible to the public.

(c) Elements of notification

(1) **Notification**

To be effective under this subsection, a notification must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(A) a physical or electronic signature of the complaining party or their agent;

(B) identification of the specific messages or statements causing actionable harm or, if there exists too many messages or statements to reasonably be identified by the individual, a representative list of such messages or statements;

(C) information reasonably sufficient to permit the service provider to locate the messages or statements;
(D) information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted;
(E) a statement that the complaining party has a good faith belief that the complaining party is a private individual and that the messages or statements cause actionable harm; and
(F) a statement that the information in the notification is accurate and if applicable, that the filing agent is authorized to act on behalf of the complaining party.

(2) **Counter-notification**

To be effective under this subsection, a counter-notification must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(A) a physical or electronic signature of the participating individual or their agent filing the counter-notification;
(B) identification of the specific messages or statements the participating individual is contesting;
(C) information reasonably sufficient to permit the service provider to locate the messages or statements;
(D) information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the participating individual may be contacted;
(E) a statement containing facts and circumstances which provide an initial showing that the person identified in the messages or statements made by the participating individual is not a private individual or that the messages or statements do not cause actionable harm; and
(F) A statement that the information in the notification is accurate and, if applicable, that the filing agent is authorized to act on behalf of the participating individual.

(3) **Failure to substantially comply**

(A) Subject to clause (B), a notification that fails to comply substantially with the provisions of subparagraph (1) shall not be

considered under paragraph (a) in determining whether a service provider has actual knowledge of actionable harm.

(B) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (1) but substantially complies with clauses (B), (C), and (D) of subparagraph (1), clause (A) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Definitions

(1) "Actionable harm" means:

(A) requesting or revealing, a private individual's, or a private individual's, friend's or family member's, home address, place of work, school name or address, real name, or other personal information, when such information is not a matter of public concern and was not revealed by the private individual on the service provider's system or network; and

(B) with the intent to harass or threaten a private individual, cause a private individual physical, financial, emotional, or other harm, or place a private individual in reasonable fear of such physical, financial, emotional, or other harm.

(2) "Monetary relief" means damages, costs, attorneys' fees, and any other form of monetary payment.

(3) "Participating individual" means an individual who causes a statement or message causing actionable harm to be placed on the service provider's system or network.

(4) "Private individual" means a person other than:

(A) an individual who holds public office or is a candidate for public office;

(B) a corporation, partnership, limited liability company, or other legal entity;

(C) an individual who has achieved pervasive fame or notoriety; or

(D) an individual who has otherwise voluntarily entered the public eye because of a particular matter of public concern.

(5) "Service provider" means an entity that offers the transmission or routing, or provides connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

(e) Misrepresentations

Any person who knowingly materially misrepresents under this section:

(1) that messages or statements cause actionable harm,
(2) that messages or statements were removed by mistake or misidentification, or
(3) that a person identified in messages or statements is or is not a private individual,

shall be liable for any damages, including costs and attorneys' fees, incurred by an alleged participating individual, by an individual identified by messages or statements causing actionable harm, or by a service provider, who is injured by such misrepresentation, as a result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be harmful, or in replacing the removed material or ceasing to disable access to it.

(f) Damages

Upon finding a service provider liable under subsection (2) of paragraph (a) of this Act or a participating individual liable under subsection (4) of paragraph (a) of this Act, the court shall award the individual identified in messages or statements monetary damages adequate to compensate the individual, but in no event less than $2,000 per message or statement causing actionable harm.

(g) Right to seek contribution

A service provider found liable under subsection (2) of paragraph (a) of this Act may seek contribution for damages from participating individuals who contributed to the messages causing actionable harm for which the service provider was found liable. Participating individuals are jointly and severally liable for such contribution.