

## THE GOOD, THE BAD, AND THE UGLY BEHAVIOR

*Michal Lavi*<sup>†</sup>

*Shaming is usually referred to as the publication of perceived anti-social or illegal behavior of an individual in order to condemn or humiliate him. It has some virtues: it makes it harder for people to get away with wrongful behavior, and it promotes justice. It also promotes freedom of expression and enables efficient deterrence. By spreading information on the behavior of individuals, shaming encourages one to maintain his reputation and facilitates beneficial transactions. Finally, it helps the public to avoid inefficient services.*

*Yet shaming raises many problems. Anyone can shame another based on individual, as opposed to universal, values, thus offending certain segments of society just because they are different. Shaming can also insult human dignity disproportionately. When the initiators of shaming are private citizens, as opposed to courts, it is committed without fact-checking or due process and can promote the dissemination of falsehoods. Shaming can also spin out of control and develop into a “lynch mob,” violence, and harassment. Thus, an action that started with an aspiration to promote social order can lead to social turmoil.*

*Shaming is nothing new—people have been doing it for centuries. But the digital era makes shaming easier. Every person can write a post, publicize inappropriate behavior, and shame others. A post on the internet can travel around the world and be shared by millions of users within seconds. Digital technologies make it difficult to keep shaming under control. Thus, it can spread like wildfire, be*

---

<sup>†</sup> Ph.D. (Law); Postdoctoral Fellow, University of Haifa—Faculty of Law, Center of Cyberlaw & Policy; Research Fellow at The Federmann Cyber Security Research Center—Cyber Law Program, Hebrew University; Cheshin Fellow, Hebrew University. I thank Guy Pessach, Re'em Segev, Katya Assaf, Ariel Nevo, Jonathan Lewy, the participants of the Hebrew University's young scholars' workshop and the participants of the Annual Private Law Association Conference for comments and the Cheshin Scholarship. Last but not least, I thank Jennifer Pierce, Ilana Kornfeld, and their colleagues on the *Cardozo Law Review* staff for comments, suggestions, and outstanding editorial work.

taken out of context, and develop into defamation, harassment, cyberbullying, and even mass violence against an individual. It can harm individuals who did not violate norms or sanction individuals disproportionately.

In the digital age, forgetting has become the exception and remembering the rule. Online shaming is not ephemeral and is searchable through a simple Google query. It leaves a trail that follows the individual everywhere.

Should the law provide a relief for online shaming? If so, when and how? This Article addresses these questions and aims to provide answers. It focuses on the shaming of ordinary people who are not public figures and are not corporations. It outlines the phenomenon, and addresses shaming's virtues and flaws. Then it sets forth a taxonomy of three types of shaming: (1) "good shaming"—shaming that is initiated by the court and carried out according to a judicial decision or recommendation; (2) "bad shaming"—shaming an individual by spreading false defamatory rumors, or shaming that got out of control and evolved into defamation or harassment; and (3) "shaming the ugly behavior"—the shaming of a person by private individuals for violating the law, or norms.

This Article focuses on non-ephemeral online shaming. It examines whether search engines should remove links to search results that contain shaming, and if so, when. The Article focuses on the characteristics of digital dissemination that amplify harm to dignitary interests. It explains that the characteristics of the internet and its influences on online expressions can justify new remedies for dissemination of shaming, beyond the traditional remedies for harm that reach the threshold of criminal or tort law.

The Article overviews the benefits and shortcoming of the "right to be forgotten." It demonstrates that the benefits and shortcomings are not equally valid in all circumstances. Following this analysis, the Article argues that a dichotomous perspective that chooses between oblivion and permanent memory is inappropriate. This Article makes the case for a differential right to be forgotten that acknowledges nuances of shaming, which outlines nuanced guidelines for delisting links to search results of shaming expressions, depending on the type of shaming.

## TABLE OF CONTENTS

INTRODUCTION .....	2600
I. SHAMING ORDINARY PEOPLE.....	2608
A. <i>Re-conceptualizing Shaming of Ordinary People: A Pragmatic Approach to Dignitary Harm in the Digital Age</i> .....	2608
1. Shaming in the Digital Age: Virtues and Flaws.....	2611

II. THE TAXONOMY OF SHAMING .....	2614
A. <i>Good Shaming</i> .....	2616
B. <i>Bad Shaming</i> .....	2618
C. <i>Shaming the Ugly Behavior</i> .....	2620
III. LEGAL TOOLS AND PRIVATE ORDERING.....	2621
IV. SHAMING FOREVER? .....	2627
A. <i>In Praise of the Forgotten</i> .....	2627
B. <i>Memory in the Digital Age</i> .....	2628
C. <i>Rediscovering Forgetting: A Comparative Perspective</i> .....	2629
1. E.U. ....	2630
2. U.S.....	2635
D. <i>Rethinking Remedies for Dignitary Harm in the Digital Age</i> .....	2638
E. <i>Normative Considerations on the Right to Delist (Right to Be Forgotten)</i> .....	2641
1. <i>In Praise of a Right to Delist</i> .....	2642
2. <i>A Right to Delist: Addressing the Objections</i> .....	2644
V. GUIDELINES FOR APPLYING THE RIGHT TO DELIST .....	2649
A. <i>Delisting Links to Good Shaming</i> .....	2649
B. <i>Delisting Links to Bad Shaming</i> .....	2651
C. <i>Delisting Links to Shaming of Ugly Behavior</i> .....	2652
D. <i>The Benefits of Bright-Line Rules for Delisting Shaming Expressions</i> .	2655
E. <i>The Proposed Rules and Law</i> .....	2658
1. Section 230 of the CDA.....	2658
2. The Proposed Rules and Substantive Law.....	2661
F. <i>The Scope of the Right to Be Forgotten</i> .....	2664
1. <i>Should Delisting Be Local or Global?</i> .....	2664
2. <i>The Challenge of Bad Shaming, Fake Stories, and the Like</i> ....	2666
G. <i>Addressing Objections and Challenges to the Proposed Framework</i> ....	2674
H. <i>A Concluding Remark on Good Shaming</i> .....	2679
CONCLUSION.....	2682

## INTRODUCTION

*A Jewish man refused to divorce his wife for four years, barring her from marrying another, and thus rendering her chained.<sup>1</sup> In an unusual move, the Israeli rabbinical court recommended the public to publish his name, photo, and personal details.<sup>2</sup> The rabbinical court repeated this practice in another case.<sup>3</sup>*

*One day in 2015, a person discovered a defamatory post on Facebook accusing him of racism. Over 6,000 individuals shared the post. Consequently, it went viral and garnered media attention. As a result, he committed suicide.<sup>4</sup>*

---

<sup>1</sup> Under Jewish law, divorce occurs when a husband writes a gett and the wife accepts it. Women who are not given a gett by their husbands are called chained women because they cannot remarry according to Orthodox Jewish law. See Talia Einhorn, *Jewish Divorce in the International Arena*, in *PRIVATE LAW IN THE INTERNATIONAL ARENA* (Jürgen Basedow et al. eds., 2000).

<sup>2</sup> See *Israeli Rabbinical Court Shames, Excommunicates Man Who Won't Divorce Wife*, JEWISH TELEGRAPHIC AGENCY (Feb. 19, 2016, 12:57 PM), <http://www.jta.org/2016/02/19/news-opinion/israel-middle-east/israeli-rabbinical-court-shames-excommunicates-man-who-wont-divorce-wife> [https://perma.cc/6MBW-CZUR]. The man, Oded Guez, was dismissed from his job and excommunicated for not granting the divorce. *Id.* He escaped to Belgium with a fake passport and continued refusing to unchain his wife. Yaniv Kubovich & Yair Ettinger, *Israeli Who Refuses to Grant Wife Divorce Arrested in Belgium for Using Fake Passport*, HAARETZ (July 28, 2016, 9:28 PM), <http://www.haaretz.com/israel-news/.premium-1.734056> [https://perma.cc/UE56-WGHE]. Later, he filed a petition to the Israeli High Court of Justice (the Israeli Supreme Court). The court concluded that the rabbinical court has the authority to shame a man who leaves his wife chained. See HCJ 5185/13 *Anonymous v. The Great Rabbinical Court in Jerusalem* (2017) (Isr.) [hereinafter *Anonymous v. The High Rabbinical Court*]. After Guez continued to chain his wife to the marriage, the Rabbinical Court used a legal procedure to nullify the marriage. See David Sedley, *In Rare Move, Rabbinical Court Annuls Marriage of Woman Refused Divorce*, TIMES ISR. (June 18, 2018, 9:55 PM), <https://www.timesofisrael.com/in-rare-move-rabbinical-court-annuls-marriage-of-woman-refused-divorce> [https://perma.cc/9PZ7-6RP3].

<sup>3</sup> Jeremy Sharon, *Edelstein Advised He Cannot Ban Divorce Refuser from Knesset*, JERUSALEM POST (May 24, 2018, 1:30 AM), <https://www.jpost.com/Israel-News/Edelstein-advised-he-cannot-ban-divorce-refuser-from-Knesset-558222> [https://perma.cc/TCP2-LYP5]. After spreading posts on the divorce refuser's behavior and being briefly jailed, the man, Yaron Attias, agreed to divorce his wife. See Aaron Rabinowitz, *After Two Years, Israeli Who Refused to Grant His Wife a Divorce Finally Relents*, HAARETZ (June 3, 2018, 5:43 PM), <https://www.haaretz.com/israel-news/.premium-after-2-years-israeli-who-refused-to-grant-his-wife-a-divorce-relents-1.6139820> [https://perma.cc/6Q2H-5522].

<sup>4</sup> This is the story of Ariel Ronis, a manager at the Interior Ministry's Population, Immigration and Border Crossing Authority. See *Interior Ministry Official Commits Suicide*

*An Israeli passenger on a flight to Varna verbally attacked a flight attendant during an argument over the purchase of tax-free chocolate. A video documenting the argument was posted on Facebook and went viral.*<sup>5</sup>

Shaming is not new; it has existed in different cultures for centuries.<sup>6</sup> In the past, shaming was especially popular for punishing people who were found guilty of minor crimes.<sup>7</sup> These sanctions had a disciplinary effect because societies were composed of close-knit communities in which people knew each other well. This led to humiliation and deterrence of the wrongdoer. This punishment was efficient because of the familiarity of the community with the offender.<sup>8</sup> The industrial revolution changed the community. Rapid urbanization allowed people to escape from the sting of shame. Consequently, shaming became less effective. In addition, people started to perceive shaming as too brutal a punishment, and prisons provided an alternative means of castigation.<sup>9</sup>

Shaming has returned. The internet and technological developments created a new “global village.” In the digital age, the scope of shaming is extensive.<sup>10</sup> Modern technology allows anyone to take out

---

*After Accusation of Racism Goes Viral*, JERUSALEM POST (May 24, 2015, 2:50 AM), <http://www.jpost.com/Israel-News/Interior-Ministry-official-commits-suicide-after-accusation-of-racism-goes-viral-403924> [<https://perma.cc/8PX9-8LKG>].

<sup>5</sup> See Amit Cotler, *The Ugliest Kind of Israeli: Passengers Hurl Abuse at Flight Attendant*, YNETNEWS (Feb. 22, 2015, 11:15 AM), <http://www.ynetnews.com/articles/0,7340,L-4629380,00.html> [<https://perma.cc/KF2V-SPH6>] (known as the Chocolate Flight).

<sup>6</sup> See DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* 91 (2007) (referring to shaming sanctions such as the ancient Romans branding a letter signifying the crime onto the wrongdoer’s forehead); Lauren M. Goldman, Note, *Trending Now: The Use of Social Media Websites in Public Shaming Punishments*, 52 AM. CRIM. L. REV. 415, 418–19 (2015).

<sup>7</sup> See Kristy Hess & Lisa Waller, *The Digital Pillory: Media Shaming of ‘Ordinary’ People for Minor Crimes*, 28 CONTINUUM: J. MEDIA & CULTURAL STUD. 101, 103 (2014).

<sup>8</sup> See Goldman, *supra* note 6, at 419–20 (explaining that without familiarity of the community, public shaming would probably not have been effective).

<sup>9</sup> *Id.* at 421; see also JON RONSON, *SO YOU’VE BEEN PUBLICLY SHAMED* 48 (2015) (referring to the brutality of this sanction. In some cases, a physical mark was made on the shamed individual); SOLOVE, *supra* note 6, at 91–92 (referring to urbanization and the rise of prisons).

<sup>10</sup> See SOLOVE, *supra* note 6, at 78; Kristine L. Gallardo, Note, *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).

a cell phone, snap a photo, upload it, and tag it. People record others by using internet-connected devices, share the information, and shame them. The internet of things (IoT) allows even greater surveillance and social control than ever before, as sensors in physical objects can passively record and transmit information to cloud storage.<sup>11</sup> Shaming can spread like wildfire, by word-of-mouth,<sup>12</sup> copying and imitating posts of other people,<sup>13</sup> or information and reputation cascades that form when individuals follow the statements or actions of their predecessors and do not express their independent opinions.<sup>14</sup> When many people forward or share a post, it might spread beyond their own narrow social network in a short time, going viral.<sup>15</sup>

---

<sup>11</sup> See MIREILLE HILDEBRANDT, SMART TECHNOLOGIES AND THE END(S) OF LAW 41–42 (2015) (expanding on the IoT, the end of dichotomy between online and offline networks, and the rise of “the onlife world”); Andrew Tutt, *The Reversibility Principle*, 66 HASTINGS L.J. 1113, 1154 (2015).

<sup>12</sup> See KARINE NAHON & JEFF HEMSLEY, GOING VIRAL 36 (2013) (defining “word-of-mouth” as flows of information among actors who know each other, engage in mutual activity, or have mutual interests).

<sup>13</sup> A prominent example of this type of dissemination are “memes.” See LIMOR SHIFMAN, MEMES IN DIGITAL CULTURE 2, 9–15 (2014) (explaining that Richard Dawkins coined the term “meme” to describe “small units of culture that spread from person to person by copying or imitation”); see also RICHARD DAWKINS, THE SELFISH GENE 189–201 (1976); Ronald S. Burt, *Social Contagion and Innovation: Cohesion Versus Structural Equivalence*, 92 AM. J. SOC. 1287, 1290 (1987) (referring to imitation and stickiness that increase the likelihood of disseminating information). More recently, the term “Internet meme” has been commonly applied to describe the propagation of items such as jokes, rumors, and videos from person to person via the internet. Thus the posts are multiplied and iterated in these posts, and shared norms and values are constructed through cultural artifacts. See AN XIAO MINA: MEMES TO MOVEMENTS: HOW THE WORLD’S MOST VIRAL MEDIA IS CHANGING SOCIAL PROTEST AND POWER 6, 20 (2019) (defining an internet meme as a piece of online media that is shared and remixed over time with the community. “a meme in other words is a unit of culture”), SHIFMAN, *supra*, at 2, 9–15.

<sup>14</sup> Informational cascades are formed when individuals follow the statements or actions of predecessors and do not express their opposing opinions because they believe their predecessors are right. As a result, the social network does not obtain important information. Reputational cascades are formed because of social pressures. In these cases, people think they know what is right, or what is likely to be right, but they go along with the crowd in order to maintain their status. See Cass R. Sunstein & Reid Hastie, *Four Failures of Deliberating Groups* 12–17 (Univ. of Chi., Public Law Working Paper No. 215, 2008).

<sup>15</sup> See NAHON & HEMSLEY, *supra* note 12, at 16.

Information that spreads on the internet can reach traditional media outlets that may contextualize it.<sup>16</sup> Furthermore, new technologies, including artificial intelligence (AI) and machine learning, allow contextualization and identification of a shamed individual, thus identifying a person who would otherwise remain anonymous or unknown to the person who first published the post.<sup>17</sup> Needless to say, tagging can also be used for shaming.<sup>18</sup> As a result, the audience may figure out who is in a picture. Courts are discovering the virtues of shaming and encourage using the internet for shaming individuals who broke the law, thus identifying violators.<sup>19</sup> Online shaming is not ephemeral. It stays on the internet and remains accessible and searchable through a simple Google query indefinitely.<sup>20</sup> Furthermore,

---

<sup>16</sup> See Hess & Waller, *supra* note 7, at 107–09. For example, traditional media identified the passengers who attacked others on the Chocolate Flight by their names. See Marissa Newman, *The Good Israeli and the Ugly Israeli*, TIMES ISR. (Feb. 23, 2015, 2:44 PM), <https://www.timesofisrael.com/the-good-israeli-and-the-ugly-israeli> [<https://perma.cc/C9CJ-YLJZ>] (mentioning the name of the husband Koby Ben-Eliyahu); see also JACOB SILVERMAN, TERMS OF SERVICE: SOCIAL MEDIA AND THE PRICE OF CONSTANT CONNECTION 65 (2015) (explaining that journalists are also exposed to shaming on the internet and can report on individuals who violate norms on traditional media).

<sup>17</sup> BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE 137–40 (2015) (referring to face recognition and contextualization of individuals by new technologies); ELI PARISER, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK 194–200 (2011); see also Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 421–22 (2017) (explaining that the use of AI machine learning is becoming more prevalent. As a result, everyone in public is likely to be identified through facial recognition).

<sup>18</sup> Sometimes shaming is published on special websites that are devoted to shaming and this may allow contextualization. See SOLOVE, *supra* note 6, at 86–90 (referring to special websites that are dedicated to shaming bad drivers, lousy tippers in restaurants, men who cheat on their spouses, and other activities).

<sup>19</sup> In her Article, Laruen M. Goldman explains that judges utilizing social media for shaming has potential in promoting efficiency; yet careful guidelines for using this tool should set forth in order to prevent inconsistency. See Goldman, *supra* note 6, at 446. Yet courts are already utilizing social media to support legal sanctions. For example, in 2006, Judge James Kimbler from Ohio posted videos of sentencing hearings on YouTube to shame the criminals and to educate the public. See Anne S.Y. Cheung, *Revisiting Privacy and Dignity: Online Shaming in the Global E-Village*, 3 LAWS 301, 304 (2014); see also *Anonymous v. The High Rabbinical Court*, *supra* note 2 (in Israel).

<sup>20</sup> See DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 11 (2014); Daniel J. Solove, *Speech, Privacy, and Reputation on the Internet*, in THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 15–19 (Saul Levmore & Martha C. Nussbaum eds., 2010).

as the information circulates, it tends to become more damaging because people tend to believe statements they are exposed to often.<sup>21</sup> In addition, the more times a post is shared, the higher it appears in the list generated by a Google search, and the more users will ascribe it relevance.<sup>22</sup> This attracts a greater exposure to the post and leaves a trail that follows the individual everywhere.<sup>23</sup> Furthermore, due to the “negativity bias,” individuals tend to ascribe more weight to negative content in comparison to other types of content.<sup>24</sup> This may result in extensive harm to the individual, infringe on his autonomy, privacy, and sovereignty,<sup>25</sup> and sanction him disproportionately. Digital shaming raises a variety of questions and challenges that policymakers must address, yet it remains under-explored.

This Article focuses on the shaming of “ordinary people” who are not public figures or celebrities<sup>26</sup> and are not corporations.<sup>27</sup> In

---

<sup>21</sup> See NICHOLAS DIFONZO & PRASHANT BORDIA, RUMOR PSYCHOLOGY: SOCIAL AND ORGANIZATIONAL APPROACHES 225 (2007); CASS R. SUNSTEIN, CONSPIRACY THEORIES AND OTHER DANGEROUS IDEAS 25–27 (2014); see also Gordon Pennycook et al., *Prior Exposure Increases Perceived Accuracy of Fake News*, 147 J. EXPERIMENTAL PSYCHOL. 1865 (2018).

<sup>22</sup> See Bing Pan et al., *In Google We Trust: Users’ Decisions on Rank, Position, and Relevance*, 12 J. COMPUTER-MEDIATED COMM. 801 (2007).

<sup>23</sup> See BOYD, *supra* note 20, at 11–13; SILVERMAN, *supra* note 20, at 168; SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING: (AND WHY WE SHOULD WORRY) 20–21 (2011).

<sup>24</sup> Due to the negativity bias, bad events, information, or feedback influence us more than good events. Roy F. Baumeister et al., *Bad Is Stronger than Good*, 5 REV. GEN. PSYCHOL. 323 (2001); see also Elizabeth A. Kensinger, *Negative Emotion Enhances Memory Accuracy: Behavioral and Neuroimaging Evidence*, 16 CURRENT DIRECTIONS PSYCHOL. SCI. 213 (2007).

<sup>25</sup> See SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 54 (2019) (introducing new types of harm of surveillance capitalism, including how tying an individual to the past infringes on “his right to the future tense and the right to sanctuary”).

<sup>26</sup> The Article adopts a narrow definition of “ordinary people” and does not include general public figures or even limited public figures who have voluntarily injected themselves into a particular public controversy, yet it will include involuntary public figures. See Kate Klonick, *Facebook v. Sullivan*, KNIGHT FIRST AMEND. INST. (Oct. 2018), [https://knightcolumbia.org/content/facebook-v-sullivan?fbclid=IwAR22L0qaobB8H76wn9jVJdcGZvcHktYNNRReVhjdp0CN\\_YKowQrqAgBDoHng](https://knightcolumbia.org/content/facebook-v-sullivan?fbclid=IwAR22L0qaobB8H76wn9jVJdcGZvcHktYNNRReVhjdp0CN_YKowQrqAgBDoHng) [<https://perma.cc/ASC7-PZ9F>] (referring to involuntary public figures in the digital age. In such cases, the privacy and reputational interests should give way to the public interest); Thomas Kadri & Kate Klonick, *Facebook v. Sullivan: Building Constitutional Law for Online Speech*, S. CALIF. L. REV. (forthcoming), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3332530](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3332530) (manuscript at 20) (referring to contemporary approaches of Facebook regarding public figures and newsworthy information); Michael L.



particular, it deals with shaming done by third parties.<sup>28</sup> Should shaming result in an everlasting “scarlet letter”? Should there be a “right to be forgotten” for individuals who have been shamed? What is the appropriate balance between free speech and autonomy, reputation, and even privacy<sup>29</sup> of the shamed individual? This Article deals with these

---

Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 404 (2015) (explaining that there are general public figures and limited public figures).

Policymakers should differentiate between shaming ordinary people and shaming public figures or celebrities. When it comes to celebrities and public figures, the public interest is more extensive, and the justifications for shaming are stronger. In the same manner, U.S. defamation law applies the standard of “actual malice” in defamation claims of public figures and uses the standard for negligence in claims of private people. See *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 279–80 (1964); Rustad & Kulevska, *supra*, at 413; see also Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L.J. 981, 1013 n.129 (2018) (“American courts sometimes conclude that persons who have sought to play a role ‘in public life’ waive their right to privacy. ‘A person—who by his accomplishments, fame, or mode of life, or by adopting a profession or calling which gives the public a legitimate interest in his doings, affairs, or character—is said to become a public personage, and thereby relinquishes a part of his right of privacy.’”).

<sup>27</sup> The considerations regarding shaming are different when it comes to corporations. For example, courts have ruled that corporations have no constitutional rights to privacy. See *FCC v. AT&T*, 562 U.S. 397, 407–08 (2011); Elizabeth Pollman, *A Corporate Right to Privacy*, 99 MINN. L. REV. 27, 88 (2014) (concluding that most corporations should not have a constitutional right to privacy). Similarly, in the European Union, the General Data Protection Regulation (GDPR) Article 4(1) refers to “natural person,” and this definition does not include corporations.

<sup>28</sup> This Article focuses on shaming that was disseminated by third parties, in contrast to a person’s own posts (such as racial jokes) that were disseminated to a wider audience than expected and led to shaming of the person who posted them. See Rustad & Kulevska, *supra* note 26 (discussing a right to delist from search engines and differentiating between an individual that requests deletion of a post that he published, an individual that requests deletion of a post published by himself in cases of republication and widespread dissemination, and an individual that requests deletion of a post that was published by third parties).

<sup>29</sup> In most cases, individuals are shamed for their behavior in the public sphere, and the right to privacy is weaker. See Michael Zimmer, “*But the Data Is Already Public*”: *On the Ethics of Research in Facebook*, 12 ETHICS & INFO. TECH. 313 (2010). Yet the right to privacy also exists in such cases under the rationale of “the right to be let alone.” See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Many scholars criticize the assumption that there is no privacy in public and advocate for a more comprehensive theory of privacy that focuses on enabling participation in social spaces, enabling connections and relationships to form, and enabling identity-making. See Emily B. Laidlaw, *Online Shaming and the Right to Privacy*, 6 LAWS 1 (2017); see, e.g., Woodrow Hartzog, *Body Cameras and the Path to Redeem Privacy Law*, 96 N.C. L. REV. 1257, 1290–92 (2018) (“The question of what is public,

questions and aims to provide answers. It offers a comprehensive framework for applying a right to be forgotten to online shaming posts that can be used by judges and policymakers. Keeping these goals in mind, this Article is divided into five parts.

Part I conceptualizes digital shaming. Due to the special properties of digital dissemination, shaming will be defined broadly as publishing and disseminating speech that causes dignitary harm to a person and humiliates him. This definition is not limited to the traditional definition of shaming. It encompasses, under the umbrella of shaming, different types of expressions. Some of them are forbidden according to the law, while others are legitimate. Yet all the types of speech under the umbrella of shaming result in dignitary harm. Following this conceptualization, the Article explores the virtues and flaws of shaming.

Part II offers a descriptive taxonomy of shaming and identifies three main categories: (1) “good shaming”—when the authority to shame is drawn from the law (following a court order or a judicial recommendation); (2) “bad shaming”—when falsehoods and

---

however, is often just a plot on the spectrum of things that range from completely obscure to totally obvious or known.”); WOODROW HARTZOG, *PRIVACY’S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* 96 (2018) (arguing that there is no dichotomy between private and public; thus, privacy concerns degrees of obscuring); Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459, 513 (2019) (arguing that there is no clear definition of public information, and the notion of public information is value-laden: “To say something is ‘public’ is to make a value-laden conclusion about what information should be protected and what kinds of surveillance and data practices should be permissible. It is an exercise of power.”). ARI EZRA WALDMAN, *PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE* 99 (2018) (explaining that, in the United States, the law does not protect privacy regarding information that was already discovered to other people, and proposing an approach of “privacy as trust” that acknowledges nuances of privacy).

Today, it is easier to access public information, and commercial stakeholders can collect information and form digital dossiers. See HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 89–98 (2010); Shlomit Yanisky-Ravid, *To Read or Not to Read: Privacy Within Social Networks, the Entitlement of Employees to a Virtual “Private Zone,” and the Balloon Theory*, 64 AM. U. L. REV. 53, 83 (2014) (arguing that, in the digital era, a private zone in the public sphere is highly important). Moreover, empirical studies discovered that the ease of accessibility of information in the public sphere does not drive judgments of appropriateness of its dissemination, and reasonable expectations of privacy can exist for public records. Therefore, assessments of privacy should be more nuanced. See Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J.L. & TECH. 111 (2017).

defamation are published,<sup>30</sup> or when harmful content is disseminated without a legitimate purpose and in cases of harassment;<sup>31</sup> and (3) “shaming the ugly behavior”—when violation of the law or norms are published.<sup>32</sup> This Part argues that the arguments in favor and against shaming do not equally apply for all types of shaming. Furthermore, certain types of shaming are inherently wrong. Re-conceptualizing shaming and mapping central types of shaming allow better understanding of this phenomenon.

Part III explores the legal and extra-legal approaches for confronting negative outcomes of shaming and addresses their limitations.

Part IV explores situations in which the law regulates the removal of certain records from databases. It also overviews the laws in the European Union and the United States on delisting links from search engine results. Following this, it explains that the digital age changed the characteristics of dissemination. It argues that the scope of dissemination, the ability to find information, and the access to information via search engines at a later stage justify a new approach towards protected dignitary interests outside the traditional categories of protected interests in civil and criminal law. It proposes that the law should recognize dignitary harm even when the dissemination is not a tort or a crime. Delisting links to shaming information is an important step in restoring the balance between memory and oblivion in the digital era. Finally, this Part examines normative considerations on the right to be forgotten.

Part V argues that the law should acknowledge different shades of forgetting and not rely on a forgetting-remembering dichotomy. It proposes a nuanced approach towards oblivion and outlines differential guidelines for delisting shaming information.

---

<sup>30</sup> This could happen even when the original statement is true, but, in the course of dissemination, users supplement it with falsehoods or the information is taken out of context.

<sup>31</sup> Examples of this include spreading non-consensual intimate pictures in order to inflict emotional harm or charge money from the victim for its removal, or shaming a person for his appearance, race, or gender. Such posts have no legitimate purpose of enforcing social norms; they only aim to harm others.

<sup>32</sup> For example, shaming uncivil behavior that diverts from social norms.

## I. SHAMING ORDINARY PEOPLE

A. *Re-conceptualizing Shaming of Ordinary People: A Pragmatic Approach to Dignitary Harm in the Digital Age*

Shaming punishes an individual who diverted from social norms or disobeyed the law. It informs the public about the conduct of individuals and allows criticism and expressions of disapproval of a person's actions.<sup>33</sup> Traditionally, shaming focuses on dissemination of true information in order to improve social supervision and sanction norm violators.<sup>34</sup>

The digital age transformed dissemination of information relative to the analog era.<sup>35</sup> In the digital age, the line between shaming, speech torts, and even criminal offences is blurring. Therefore, it is difficult to stick with the traditional concept of shaming. In the past, shaming occurred in small communities where everyone knew each other, and the context of the norm violation was clear. By contrast, today, a person can shame another without even knowing him. In addition, shaming can spread beyond the small community and be interpreted wrongly by strangers who will not be aware of the original context and circumstances. Traditional media check the facts before publication. In contrast, on the internet, everyone can share information with the public that condemns others without sticking to the facts.<sup>36</sup>

A person can publish an expression in order to shame another for violating norms, yet the shaming expressions come to be a speech tort or a criminal offence. This can happen when a person misinterprets the situation, or when a person intends to shame but does not stick to the facts and adds an interpretation or creates narratives that extend beyond

---

<sup>33</sup> Jacob Rowbottom, *To Punish, Inform, and Criticise: The Goals of Naming and Shaming*, in *MEDIA AND PUBLIC SHAMING: DRAWING THE BOUNDARIES OF DISCLOSURE 1* (Julian Petley ed., 2013).

<sup>34</sup> See Dan M. Kahan, *What's Really Wrong with Shaming Sanctions*, 84 *TEX. L. REV.* 2075 (2006); Goldman, *supra* note 6 (referring to shaming as a punishment for violations).

<sup>35</sup> Digital technologies make it easier for everyone to disseminate information. They increase the scope of dissemination and allow users to find information in later stages. See *infra* Section IV.D.

<sup>36</sup> See Jack M. Balkin, *The First Amendment in the Second Gilded Age*, 66 *BUFF. L. REV.* 979, 984–86 (2018).

the qualified privileges in defamation law.<sup>37</sup> Moreover, a person can publish a traditional shaming expression that would be taken out of context and evolve into defamation in the process of dissemination.<sup>38</sup> This can happen when the disseminators add defamatory comments, or when they unite forces and harass the shamed individual. Since digital ecosystems remove barriers to speak and spread and share information,<sup>39</sup> the dignitary harm of shaming is tremendous.<sup>40</sup>

The digital era dictates changes in dissemination. It requires re-conceptualizing dignitary harm and recognizing new categories of protected interests beyond the traditional categories in criminal and tort law.<sup>41</sup>

---

<sup>37</sup> Consider the fair comment defense. See DAN B. DOBBS ET AL., TORTS AND COMPENSATION: PERSONAL ACCOUNTABILITY AND SOCIAL RESPONSIBILITY FOR INJURY 969–71 (2013); DAN B. DOBBS, THE LAW OF TORTS § 413 (2000). For example, a person can write a negative review on a website in order to shame a vendor who sold him a defective product, calling the vendor a “mega crook.” The review itself might be a fair comment, but the addition of “mega crook” is defamatory. Adding the title “mega crook” to a fair comment changes its context and turns it to defamation.

<sup>38</sup> For a related context, see Alice E. Marwick, *Why Do People Share Fake News? A Sociotechnical Model of Media Effects*, 2 GEO. L. TECH. REV. 474, 478 (2018) (“[T]he networked nature of the internet and the ability to replicate and remix images, text, and video makes it impossible to determine where a particular idea, image, or meme originated, let alone pinpoint the intent of the author.”).

<sup>39</sup> The digital architecture removes barriers to speak. It allows everyone to spread information anonymously or by using pseudonyms, and makes it easier to share information with a click of a button. See NICHOLAS CARR, THE GLASS CAGE: AUTOMATION AND US 177–82 (2014). In addition, the platforms’ algorithms promote positive feedback from friends and family and encourage users to share and post harmful content. See CASS R. SUNSTEIN, #REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA 123 (2017); JARON LANIER, TEN ARGUMENTS FOR DELETING YOUR SOCIAL MEDIA ACCOUNTS RIGHT NOW 16–21 (2018) (explaining that algorithms on social networks show users content that exerts emotions and positive feedback from family and friends leading to social pressures to post and share harmful content); Julie E. Cohen, *The Emergent Limbic Media System*, in LIFE AND THE LAW IN THE ERA OF DATA-DRIVEN AGENCY (Mireille Hildebrandt & Kieron O’Hara eds., forthcoming 2019) (“Algorithmically-mediated processes designed to create tight stimulus-response feedback loops have exposed and deepened social divides . . . . The result is an information environment that magnifies the vulnerability of ordinary citizens to reputational and financial harm, manipulation, and political disempowerment.”).

<sup>40</sup> See Michal Lavi, *Taking Out of Context*, 31 HARV. J.L. & TECH. 145 (2017) (explaining that true statements can turn into defamation in the process of dissemination).

<sup>41</sup> See *infra* Section IV.D.

The traditional conception of shaming does not fit dissemination in the digital age. Therefore, it is necessary to define shaming broadly, beyond condemnation of norm violations. This Article will not limit the definition to informing the public about the conduct of individuals, condemning, and sanctioning shaming. Instead, it will refer to shaming as an umbrella term that includes every active dissemination of negative information on a person that can humiliate him in public and infringe on his dignity. The umbrella of shaming includes a wide range of different expressions. Some of them are forbidden by criminal law or tort law, while others are legitimate and even desirable. Yet all these expressions share a common denominator. They all lead to dignitary harm in the eyes of the public.<sup>42</sup> This definition allows a normative analysis of dignitary harm in the digital age. Although there is little legal scholarship on online shaming, it does not provide a coherent definition of shaming;<sup>43</sup> yet it seems that this definition was adopted in everyday life and is reflected in the definition for shaming on Wikipedia.<sup>44</sup>

The following Subsection focuses on the shaming of “ordinary people” who are not public figures, celebrities, or corporations, and overviews the virtues and flaws of shaming.

---

<sup>42</sup> It should be noted that this Article focuses on dissemination of expressions that results in dignitary harm in the eyes of society. It will not refer to other implications of dissemination such as the collection of data on individuals and the analysis of data by big data and AI. Although these activities can influence speech and opportunities of the data’s subject and eventually infringe on his dignity, these activities are not transparent to all internet users and do not directly degrade a person in the eyes of society. Therefore, in itself, data processing for personalization purposes will not be defined under the umbrella of shaming. For an expansion on the implications of data processing on speech and opportunities, see Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149 (2018).

<sup>43</sup> See, e.g., Kate Klonick, *A New Taxonomy for Online Harms*, 95 B.U. L. REV. ANNEX 53 (2015) (grouping cyberbullying and cyberharassment in a separate category and not including the terms in the definition of shaming). *But see* Laidlaw, *supra* note 29 (proposing a broader approach to shaming).

<sup>44</sup> See *Online Shaming*, WIKIPEDIA, [https://en.wikipedia.org/wiki/Online\\_shaming](https://en.wikipedia.org/wiki/Online_shaming) [<https://perma.cc/7H8L-LSS9>] (last visited May 9, 2019) (“Online shaming is a form of Internet vigilantism in which targets are publicly humiliated using technology like social and new media.”).

### 1. Shaming in the Digital Age: Virtues and Flaws

Online shaming has many benefits. *First*, it allows everyone to share the burden of law enforcement.<sup>45</sup> Online shaming led to the arrest of a person who committed an obscene act in public;<sup>46</sup> it led to the arrest of a cell-phone thief; and it made it easier to enforce the law in many other cases.<sup>47</sup> At times, shaming can be a cost-effective alternative to criminal punishment or other sanctions.<sup>48</sup>

*Second*, online shaming makes it harder for people to escape transgressions. It allows condemning wrongful behavior and makes it harder for people to get away with rude and wrongful behavior.<sup>49</sup>

*Third*, online shaming has a spillover effect. Even if it fails to deter a particular individual who violated the legal norm, it promotes widespread deterrence to the entire public by reinforcing the community's norms and preserving public order.<sup>50</sup>

---

<sup>45</sup> SOLOVE, *supra* note 6, at 83.

<sup>46</sup> *Id.* at 80.

<sup>47</sup> See CLAY SHIRKY, *HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS* 1–6 (2008) (referring to an example in which online shaming led to the police involvement in and to the arrest of a sixteen-year-old girl who stole a cell phone).

<sup>48</sup> See Goldman, *supra* note 6, at 429; Dan M. Kahan, *What Do Alternative Sanctions Mean?*, 63 U. CHI. L. REV. 591, 611 (1996) (arguing that shaming can be a punishment by itself and an efficient alternative to the prison system.). It should be noted that a decade later Kahan retreated from his previous approach. See Kahan, *supra* note 34.

<sup>49</sup> See David R. Karp, *The Judicial and Judicious Use of Shame Penalties*, 44 CRIME & DELINQ. 277, 278–79 (1998); Goldman, *supra* note 6, at 430; SOLOVE, *supra* note 6, at 80–94 (for example, bad driving, littering in public domain, and giving bad service).

<sup>50</sup> See Goldman, *supra* note 6, at 431. A counter argument is that more shaming can backfire and lead to less deterrence. See Alon Harel & Alon Klement, *The Economics of Shame: Why More Shaming May Deter Less* (Hebrew Univ., Federmann Ctr. for the Study of Rationality, Discussion Paper No. 401, 2005), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=789244](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=789244) [<https://perma.cc/BZN6-JRA5>]; Alon Harel & Alon Klement, *The Economics of Stigma: Why More Detection of Crime May Result in Less Stigmatization*, 36 J. LEGAL STUD. 355 (2007) (explaining that more shaming undermines the deterrence of this tool because the costs of searching for law-abiding partners increase with the rate of detection. Thus, the more shaming there is, the less people will refrain from business or social contacts with someone they believe has committed an offense or violated norms, and shaming will cause less stigmatization). Yet one can argue that on the internet, the search costs of law and norm abiding people are lower, and it is more difficult to reach the point in which deterrence is ineffective anymore.

*Fourth*, online shaming can promote efficiency and improve the information available to the market by helping consumers to assess a vendor's reputation. This discourages inefficient transactions and services.<sup>51</sup>

*Fifth*, online shaming gives people a chance to fight back and voice their disapproval of violating laws and norms.<sup>52</sup> It promotes free speech and strengthens the autonomy of the person who was offended by allowing him to condemn it. It promotes a vibrant marketplace of ideas by enhancing access to information on people. It also promotes democracy and a participatory culture by allowing everyone a fair chance to develop and share ideas as they express their opinions on individuals.<sup>53</sup>

Online shaming has many virtues; however, there is a flip side that can lead to extensive harm. *First*, shaming is one-sided. In contrast to incarceration that condemns wrongful behavior according to the values reflected in the legal jurisdiction, anyone can shame according to their individual values and offend certain segments of society just because they are different.<sup>54</sup> People who hold certain values may shame others for violating norms that are not universal.<sup>55</sup> Shaming may spread even when there is no social consensus that a norm had been violated by an individual, since the disseminators are trapped in a system of feedback reinforcement.<sup>56</sup>

*Second*, shaming is powerful, visible, and can damage human dignity disproportionately,<sup>57</sup> especially when it is disseminated to a vast

---

<sup>51</sup> SOLOVE, *supra* note 6, at 93–94.

<sup>52</sup> *Id.* at 92.

<sup>53</sup> See Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 3 (2004) (explaining how dissemination of information on the internet promotes free speech and the rationales at its base).

<sup>54</sup> See Kahan, *supra* note 34, at 2076.

<sup>55</sup> SOLOVE, *supra* note 6, at 83–84 (referring to an example of shaming a person for using the internet in a computer store for a long time. Bystanders took his picture and shamed him online. He was shamed even though the store employees did not seem to care, and he did not violate a universal norm).

<sup>56</sup> See RONSON, *supra* note 9, at 280–82.

<sup>57</sup> Kate Klonick, *Re-Shaming the Debate: Social Norms, Shame, and Regulation in an Internet Age*, 75 MD. L. REV. 1029, 1055 (2016) (“[I]n this new era, shaming is an indeterminate, inaccurate, and uncalibrated form of punishment”). Even before the age of



audience.<sup>58</sup> This may also disproportionately result in over-deterrence and a chilling effect on the shamed individual who may lose social and professional opportunities.<sup>59</sup> This effect may spill over and affect the public in general. Due to the fear of being shamed, people may avoid acting freely in public.

*Third*, when online shaming is initiated by private people, it is done without due process and conducted without hearing the arguments of the shamed individual and without a right of appeal that exist in traditional courts' proceedings. In contrast to traditional media outlets, internet users rarely check facts before they share information. They may interpret a picture or a video in a wrong way and share inaccurate stories without knowing the overall context.<sup>60</sup> Consequently, individuals can be shamed even if they have not done anything wrong.<sup>61</sup>

*Fourth*, expressions can be taken out of context, and defamatory comments can be added maliciously to an existing text. Once this type of shaming spins out of control, mob justice ("lynch mob"), harassment, and violence soon follow.<sup>62</sup> Thus, an action that starts with an aspiration to promote social order can lead to the opposite effect.

---

online social networks, literature expressed concerns regarding the disproportional harm to dignity that may be a result of shaming. MARTHA C. NUSSBAUM, *HIDING FROM HUMANITY: DISGUST, SHAME, AND THE LAW* 230–33 (2004); James Q. Whitman, *What's Wrong with Inflicting Shame Sanctions?*, 107 *YALE L.J.* 1055, 1062–68 (1998); Toni M. Massaro, *The Meanings of Shame: Implications for Legal Reform*, 3 *PSYCHOL., PUB. POL'Y, & L.* 645, 700 (1997).

<sup>58</sup> See Klonick, *supra* note 57, at 1053–54.

<sup>59</sup> *Id.* at 1046–49 (giving a few examples).

<sup>60</sup> *Id.* at 1054 (discussing the accuracy problem); SOLOVE, *supra* note 6, at 80–83 (referring to a person who was shamed for stealing a cell phone, but it is possible that he was not the thief; instead, he might have received it as a gift without knowing that it was stolen). Shaming can be committed without awareness to the full picture of the behavior and interaction.

<sup>61</sup> See *supra* note 4 (shaming a person for being racist, while he was not racist at all); see also SOLOVE, *supra* note 6, at 87 (for example, the website "Bitter Waitress" contains the names of bad tippers in restaurants. In one case, Malcolm Gladwell, author of the best-sellers *The Tipping Point* and *Blink*, saw his name shamed on the website for not tipping above 10% of the service even though he left a 15–20% tip).

<sup>62</sup> Klonick, *supra* note 57, at 1040; James Q. Whitman, *What Is Wrong with Inflicting Shame Sanctions?*, 107 *YALE L.J.* 1055, 1089 (1998); see also SILVERMAN, *supra* note 23, at 168–74; SOLOVE, *supra* note 6, at 100; *Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists*, 290 F.3d 1058, 1080 (9th Cir. 2002). The website "Nuremberg Files" posted online the personal information of doctors who performed abortions. Every time a doctor was killed, a strikethrough was placed over their name. Planned Parenthood and a group

*Fifth*, shaming can cause negative psychological effects, such as inducing a sense of ostracization that encourages an individual to act against the norms.<sup>63</sup> Shaming may cause a negative psychological effect in society as a whole, especially if it results in mass attacks on individuals.<sup>64</sup>

*Sixth*, as shaming becomes more prevalent, it might lose its deterrent effect.<sup>65</sup> Moreover, supportive environments for violators would soon be created in places where this tool is often used.<sup>66</sup>

Shaming is not monolithic and the validity of the common arguments advocating and opposing this practice do not apply equally to different types of shaming.

## II. THE TAXONOMY OF SHAMING

This Part introduces a new taxonomy of shaming. A nod to Sergio Leon's film,<sup>67</sup> it divides the phenomenon into three abstract categories.<sup>68</sup>

---

of doctors sued, contending that the website caused them to live in fear; a jury awarded the doctors more than one hundred million dollars in damages. The case was appealed, with the website owner's claim that the verdict violated their right to free speech. The court of appeals concluded that the website involved threats of violence with an intent to intimidate rather than to articulate a position in a debate and affirmed the previous decision. *See id.*; SOLOVE, *supra* note 6.

<sup>63</sup> Klonick, *supra* note 57, at 1039 (citing Massaro, *supra* note 57, at 694) (arguing that shaming can exclude a person from society and encourage him to rebel). For more on this argument, see RONSON, *supra* note 9, at 101.

<sup>64</sup> *See* RONSON, *supra* note 9, at 91–109.

<sup>65</sup> *See* Harel & Klement, *supra* note 50, at 373 (“[B]ecause increasing the rate of detection increases the proportion of unwilling stigmatizers who fail to cooperate with the shaming-penalties scheme, the normative message conveyed may be diluted.”).

<sup>66</sup> Klonick, *supra* note 57, at 1039 (“[F]eeling shamed by a community might create feelings of ostracization and ultimately encourage the offender to continue to act against the norms, or they might simply act violently out of anger. Conversely, over time and frequency of use, shaming might simply become ubiquitous and lose its power as a tool of enforcing norms.”).

<sup>67</sup> *THE GOOD, THE BAD AND THE UGLY* (United Artists 1966) is a western film directed by Sergio Leon.

<sup>68</sup> The idea of outlining a taxonomy for offensive speech online is not new. Literature suggested differentiating between shaming and other types of speech and behavior. *See* Klonick, *supra* note 43; Klonick, *supra* note 57, at 1044 (suggesting a taxonomy for differentiating between shaming, cyberbullying, and cyberharassment); *see also* Gallardo, *supra* note 10, at 730. I would like to introduce a different taxonomy, which includes defamation, cyberbullying, and cyberharassment to the definition of shaming because the line between these types of behavior

First, “good shaming,” shaming that is initiated by court and carried out after a judicial decision that an individual violated the law. Second, “bad shaming,” which consists of publishing defamation, taking (true) information out of context and misrepresenting it, or publishing information without a legitimate purpose, such as nonconsensual intimate photos. This category of shaming also includes dissemination of information on norm violation that develops into defamation,<sup>69</sup> harassment or direct violent attacks against individuals in the process of dissemination. Third, “shaming the ugly behavior,” which is shaming an individual that violated social norms. The taxonomy allows a better understanding of shaming and its implications on dignitary harm.

It should be noted that the categories of the taxonomy are abstract and do not purport to take an overall stand as to every particular expression in them. Good shaming can be disproportionate and even develop into bad shaming. In addition, as explained below, shaming the ugly behavior does not necessarily result in shaming truly ugly behavior, according to consensual norms.<sup>70</sup> Furthermore, there is no absolute dichotomy among these categories and, at times, there can be a spillover between them.<sup>71</sup>

---

is lean and there is a spillover. Thus, classic shaming that aims to enforce norms can easily develop into harassment.

It should be noted that in contrast to Klonick’s narrow approach, Laidlaw proposes a wider perspective of shaming. The taxonomy is also different than a wider perspective of shaming that was proposed. This perspective focuses on negative aspects of shaming and uses four broad and overlapping categories of shaming: vigilantism, bullying, bigotry, and gossiping. See Laidlaw, *supra* note 43. In contrast, the proposed taxonomy in this Article addresses the source of shaming (“bottom up” or “top down”) and the question of whether shaming violates the law.

<sup>69</sup> This may happen when the disseminators add comments to the speech, turning it into defamation. See Lavi, *supra* note 40, at 194. See, e.g., *Icon Health & Fitness v. ConsumerAffairs.com*, No. 1:16-cv-00168-DBP, 2017 WL 2728413 (D. Utah June 23, 2017); *Samsel v. Desoto Cty. Sch. Dist.*, No. 3:14-cv-00113-MPM-SAA, 2017 WL 1043640 (N.D. Miss. Mar. 17, 2017) (demonstrating that individuals who repeat others and add defamatory comments to their text can lose section 230 of the Communication Decency Act’s immunity, because by adding comments and titles they create and develop content). After losing their immunity, defendants may be held responsible in defamation suits for mixing their generated content with the publishers’ content, adding defamatory comments and titles, even if the original speech enjoys defamation law defenses.

<sup>70</sup> See *supra* note 55 and accompanying text.

<sup>71</sup> For example, in order to hold a person responsible for defamation, the plaintiff does not have to prove that the defendant intended to defame him. One person can shame another in a

### A. *Good Shaming*

As mentioned above, good shaming is predicated on a judicial decision or recommendation to condemn a person for an illegal act or other violation of law on social media. This type of shaming can either add to traditional legal sanctions or replace them. For example, one can shame an individual who does not comply with judicial decisions or court orders. It might also be used as a form of punishment for contempt of court,<sup>72</sup> or intentional violation of the law.<sup>73</sup> By default, courts publish their verdicts, naming the involved parties. This information is normally available online. As a result, the person who lost a case or was convicted of a crime is shamed. Yet the goal of publication is to fulfill the public's right to information—shaming is only a by-product. In contrast, good shaming encourages the public to *actively* spread the decision and condemn the violator intentionally.

It should be noted that defining this shaming as “good” does not conclude that every direction of a court to shame results in fairness and efficiency. However, the presumption is that good shaming is generally fair and just, since courts direct or order the public to shame only in rare cases and after thorough judicial balances.<sup>74</sup>

This type of shaming has many virtues. It promotes compliance with the law, retribution, and efficient deterrence of the activity. It may also discourage members of society from similar violations. The

---

review website in order to enforce norms but not limit his review to opinion, or hyperbole speech, and defame the plaintiff as a byproduct. *See, e.g.,* Dietz Dev., LLC v. Perez, No. 2012-16249 (Va. Cir. Ct. Oct. 31, 2012); Justin Jouvenal, *Fairfax Jury Declares a Draw in Closely Watched Case over 'Yelp' Reviews*, WASH. POST (Feb. 1, 2014), [http://www.washingtonpost.com/local/in-closely-watched-yelp-case-jury-finds-dual-victory/2014/01/31/2d174580-8ae5-11e3-a5bd-844629433ba3\\_story.html](http://www.washingtonpost.com/local/in-closely-watched-yelp-case-jury-finds-dual-victory/2014/01/31/2d174580-8ae5-11e3-a5bd-844629433ba3_story.html) [<https://perma.cc/T49B-AZWG>] (the main question was whether reviews on Yelp and Angie's List were false. A jury found that both the plaintiff and defendant defamed each other). Moreover, a person can write a post in order to shame another person who violated norms, interpret his behavior incorrectly and defame him or add defamatory remarks to the facts in the post. Furthermore, shaming may start as good shaming or shaming the ugly behavior but turn into bad shaming in the process of dissemination.

<sup>72</sup> For example, shaming a person who refuses to divorce his wife. *See Israeli Rabbinical Court Shames, Excommunicates Man Who Won't Divorce Wife*, *supra* note 2.

<sup>73</sup> For example, posting videos of sentencing hearings on YouTube to shame the criminals and educate the public. *See* Cheung, *supra* note 19.

<sup>74</sup> It should be noted that this Article concludes by addressing the need for guidelines or an ethical code for top down shaming. *See infra* Section V.H.

argument against shaming weakens when it is done according to a judicial writ, since the individual is shamed for breaking the law, and a court instructs the public from top down. As a result, one might claim that it better reflects the values of society as a whole and not just a specific person. Furthermore, the court reaches its decision after adhering to the rules of due process and proper fact checking. Finally, the court shames a person solely for his actions. One may presume that no inappropriate considerations were taken (such as a person's appearance of gender). As a result, it is less likely that the court will play a hand in de-humanizing the condemned party. It is also likely that the court will use this tool sparingly and proportionally only when the behavior of an individual was outrageous. Furthermore, even if this sanction is extreme, the price might be worthwhile because this type of shaming improves overall deterrence against anti-social behavior.

However, good shaming may devolve into bad shaming when taken out of context and it may turn into defamation,<sup>75</sup> cyberbullying,<sup>76</sup> or harassment.<sup>77</sup> Even though good shaming might be considered a proportional sanction at present, from a prospective point of view, it might not be so because the condemnation can be found online for years after the person violated the law.

---

<sup>75</sup> See Lavi, *supra* note 40.

<sup>76</sup> See Klonick, *supra* note 57, at 1034 (citing EMILY BAZELON, STICKS AND STONES: DEFEATING THE CULTURE OF BULLYING AND REDISCOVERING THE POWER OF CHARACTER AND EMPATHY 28 (2013)) (bullying is generally understood among academics and educators as having to meet three criteria: (1) verbal or physical *aggression*; (2) *repeated* over time; and (3) involve a *power differential*. When talking about cyberbullying, the aggression is mostly verbal, using "threats, blackmail . . . gossip and rumors"). Many legal scholars refer to cyberbullying as an aggression against children and youth in particular. See Jamie Wolf, Note, *The Playground Bully Has Gone Digital: The Dangers of Cyberbullying, the First Amendment Implications, and the Necessary Responses*, 10 CARDOZO PUB. L. POL'Y & ETHICS J. 575 (2012); Elizabeth M. Jaffe, *From the School Yard to Cyberspace: A Review of Bullying Liability*, 40 RUTGERS COMPUTER & TECH. L.J. 17 (2014); Ari Ezra Waldman, *Are Anti-Bullying Laws Effective?*, 103 CORNELL L. REV. ONLINE 135 (2018).

<sup>77</sup> See Klonick, *supra* note 57, at 1034 (cyberharassment "involves threats of violence, privacy invasions, reputation-harming lies, calls for strangers to physically harm victims, and technological attacks").

## B. *Bad Shaming*

Bad shaming is defined as dissemination that reaches the threshold of tort or criminal offenses—for example, publishing defamatory speech that condemns an individual for something he did not commit,<sup>78</sup> or publishing a speech that does not benefit from defamation law defenses. It may include posts that are not focused on the conduct of a person but rather on his race, or negative posts without a legitimate purpose, whose aim is to inflict emotional harm—for example, disseminating intimate photos of an individual without consent.<sup>79</sup> Bad shaming may begin with a legitimate form of expression that condemns an individual for violating a social norm (shaming the ugly behavior), or in response to a

---

<sup>78</sup> See, e.g., Liz Klimas, *Viral Facebook Post Accuses Man of Being a Child Molester—Except He’s Not*, THEBLAZE (May 26, 2013), <http://www.theblaze.com/news/2013/05/26/viral-facebook-post-accuses-man-of-being-a-child-molester-except-hes-not> [<https://perma.cc/8Z2E-YARB>] (exploring a case in which an ex-girlfriend of a man named Chad Lesko published a false rumor on Facebook that claimed that he is a rapist. The post went viral and he was excluded from a public park). It should be noted that technology exacerbates the problem of bad shaming and allows the spread of reliable lies by using general adversarial neural networks. See Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, CALIF. L. REV. (forthcoming 2019) (raising the problem of deep fakes that are created by general adversarial neural networks, seemingly authentic and reliable despite not reflecting the truth).

<sup>79</sup> See Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019); Zak Franklin, *Justice for Revenge Porn Victims: Legal Theories to Overcome Claims of Civil Immunity by Operators of Revenge Porn Websites*, 102 CALIF L. REV. 1303 (2014); see also Rustad & Kulevska, *supra* note 26, at 354 (nonconsensual dissemination of embarrassing photos serves no legitimate purpose other than to embarrass or extort payment from individuals); Emily Poole, Note, *Hey Girls, Did You Know? Slut-Shaming on the Internet Needs to Stop*, 48 U. S.F. L. REV. 221, 231, 236 (2013) (referring to the act of attacking a female for being sexual and giving the example of the story of Amanda Todd, a twelve-year-old girl who discovered that an intimate photo of her captured while she was topless by a stranger was disseminated on the internet). Disseminating intimate photos is a crime in thirty-four states in the United States. In addition, on July 14, 2016, Congresswoman Jackie Speier (D-CA) introduced the Intimate Privacy Protection Act, a bipartisan federal bill addressing nonconsensual pornography. See Mary Anne Franks, *“Revenge Porn” Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251, 1256 (2017); MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN 71 (2016). Similar legislation was enacted in England. See Criminal Justice and Courts Act 2015, c. 2, § 33 (Eng.), <http://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted> [<https://perma.cc/2WZ2-ERAM>]; James Vincent, *Sharing Revenge Porn in the UK Now Carries a Two Year Jail Sentence*, VERGE (Apr. 13, 2015, 7:23 AM), <http://www.theverge.com/2015/4/13/8398691/revenge-porn-laws-uk-jail-time> [<https://perma.cc/SL8A-DKFT>].

court order or decision that recommends the public to shame (good shaming). Yet the content may be taken out of context and turn into defamation as part of the dissemination process.<sup>80</sup> In fact, the process can spin out of control and induce violence, cyberbullying, or cyberharassment that is directed at the shamed individual.<sup>81</sup> This type of shaming can infringe on cybersecurity<sup>82</sup> and is normally either a civil tort or a criminal offense.<sup>83</sup>

Bad shaming has very few virtues, if any. It does not promote norm enforcement. In many cases, it starts as a form of defamation or dissemination of offensive content whose sole aim is to inflict harm and violate the norms outlined by law. In other cases, legitimate shaming spins out of control and develops into defamation, harassment, and violence. These expressions may cause the victim to withdraw from online life and as a result, his right to free speech might be infringed.<sup>84</sup>

Shaming that includes defamation and disinformation does not promote efficiency but rather infringes on it, as people get the wrong impression about the shamed individual and may avoid efficient

---

<sup>80</sup> This may happen when the disseminators add information that misrepresents the case or is defamatory in nature. See Lavi, *supra* note 40, at 196–201 (referring to selective repetition of content in the process of dissemination, and adoption of statements by adding titles and comments that can be defamatory).

<sup>81</sup> For example, disseminating an individual's phone number and home address while threatening him. See Jacqueline D. Lipton, *Repairing Online Reputation: A New Multi-Modal Regulatory Approach* 1, 6–11 (June 12, 2010) (unpublished manuscript), [https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=1144&context=ua\\_law\\_publications](https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=1144&context=ua_law_publications) [<https://perma.cc/D5T3-ZFNM>]; see also Klonick, *supra* note 57, at 1034; JAQUELINE LIPTON, *RETHINKING CYBERLAW: A NEW VISION FOR INTERNET LAW* 141–49 (2015) (expanding on victimization).

<sup>82</sup> See Jeff Kosseff, *Cybersecurity of the Person*, *FIRST AMEND. L. REV.* (forthcoming 2019).

<sup>83</sup> See DANIELLE KEATS CITRON, *HATE CRIMES IN CYBERSPACE* 212–18 (2014) (the court can conclude that direct attacks are intentional infliction of emotional distress or criminal harassment).

<sup>84</sup> *Id.* at 195–99; SILVERMAN, *supra* note 23, at 80 (explaining the implications of defamation, cyberbullying, and cyberharassment on the victim's free speech); see also ZEYNEP TUFEKCI, *TWITTER AND TEAR GAS: THE POWER AND FRAGILITY OF NETWORKED PROTEST* 179 (2017) (explaining that calling a person's political view "stupid" is free speech; yet, when mass mobs attack a person because of her political view, this may create fear and block free speech). It should be noted that the right to speak should be on both sides. See Jeremy K. Kessler & David E. Pozen, *The Search for an Egalitarian First Amendment*, 118 *COLUM. L. REV.* 1953, 1994 (2018) ("Arguments involving speech on both sides focus on the degree to which one party's expressive activity compromises the ability of other private parties to exercise their own First Amendment rights.").

transactions with him. Dissemination of intimate photos without consent is also inefficient because it can deprive the victim of opportunity in markets and hinder efficient transactions. Moreover, it can silence the victim, infringe on her free speech, and hinder the vibrant market of ideas and the trust in society generally.<sup>85</sup>

When shaming gets out of control and develops into violent attacks, it may also harm social order and lead to social deterioration. Shaming that goes out of control may exclude individuals from society, thus making it more likely that they will violate more norms. In addition, shaming is often a disproportionate sanction even for violating a consensual norm. It is all the more so when a person does not violate a consensual norm or when the shaming starts as a legitimate form of expression and gets out of control. Furthermore, search engines that display the shaming posts years after they are disseminated make bad shaming even less proportional.

### C. *Shaming the Ugly Behavior*

Shaming the ugly behavior is an action initiated by private individuals (as opposed to a judicial writ, or a judicial recommendation) that aims to shame individuals for violating norms. In many cases, this type of shaming fulfills the general benefits gained from good shaming. First, it has the potential to increase norm enforcement and may deter a person from violating certain norms. Second, it may deter other members of society from infringing norms. Third, it gives people a chance to fight back against or to voice their disapproval of, inappropriate behavior and as a result it promotes their free speech.<sup>86</sup> On the other hand, it can lead to self-exclusion and hinder the person's democratic participation. Yet, as long as it was not taken out of context and turned into bad shaming, the infringement of the shamed individual's free speech is limited.

Private shaming bears some risks. In contrast to good shaming, this type of shaming is not directed from the top down. Consequently, a

---

<sup>85</sup> See CITRON, *supra* note 83, at 5; Citron, *supra* note 79, at 1924–28, Danielle Keats Citron, *Why Sexual Privacy Matters for Trust*, WASH. U. L. REV. (forthcoming 2019).

<sup>86</sup> See SOLOVE, *supra* note 6, at 92.



person can be shamed even if there is no consensus that his behavior violates a norm.<sup>87</sup> At the court of public opinion, a person can be shamed disproportionately to the norm violation. Private shaming is committed without due process and is not necessarily accurate. A person may share videos without knowing the context or the full picture. This may lead to misinterpretation and condemnation of a non-reprehensible behavior.<sup>88</sup> In addition, shaming the ugly behavior can evolve into bad shaming in the process of dissemination.

Legal and extralegal tools can mitigate part of the harm resulted from shaming. The following Part reviews these tools and explains that they are insufficient.

### III. LEGAL TOOLS AND PRIVATE ORDERING

Shaming on a social network is not limited to the specific platform to which it was uploaded, since it may spread and cross onto other platforms. Moreover, search engines may locate it with ease. Consequently, shaming can cause extensive harm to an individual: he might be fired from work, bear economic losses, or suffer from social exclusion and emotional distress.<sup>89</sup> This Part outlines the legal and extra-legal approaches for confronting these negative outcomes and addresses their limitations.

In a wide range of bad shaming cases, the victim can file a direct civil suit or file a complaint with the police, which can lead to prosecution.<sup>90</sup> For example, if the shaming post is untrue or is taken out

---

<sup>87</sup> See, e.g., *supra* note 55 and accompanying text (shaming a person for spending a long time inside a computer store for wireless access to internet).

<sup>88</sup> For examples, see *supra* note 60.

<sup>89</sup> Shaming can inflict tremendous harm, especially when it spins out of control and turns into cyberbullying or cyberharassment. See SOLOVE, *supra* note 6, at 76–102.

<sup>90</sup> See ALICE E. MARWICK & ROSS MILLER, FORDHAM LAW SCH., ONLINE HARASSMENT, DEFAMATION, AND HATEFUL SPEECH: A PRIMER OF THE LEGAL LANDSCAPE (2014). In many cases, this person uses his real name (for example, on social networks). See *Terms of Service*, FACEBOOK, <https://www.facebook.com/terms> [<https://perma.cc/EFG7-S7TN>] (last visited Apr. 24, 2019) (“Use the same name that you use in everyday life.”). In addition, even if the speaker is not using his real name, courts can unmask his identity. See MARWICK & MILLER, *supra*, at 12 (“[F]ederal and state courts use different court-created tests to determine if the court will order the unmasking of the anonymous speaker”).

of context, the subject of the post can file a libel suit against the person who defamed him.<sup>91</sup>

When shaming turns into cyberharassment or cyberbullying that results in emotional distress, the shamed individual can file a civil suit for intentional infliction of emotional distress.<sup>92</sup> A plaintiff may also recover damages for negligently inflicted emotional distress, although some states allow these claims only if there is a physical impact.<sup>93</sup> Some states even passed criminal infliction of emotional distress (CIED) laws.<sup>94</sup> They are designed to combat harassment and bullying. They usually apply when the defendant knowingly engages in an action that would cause a reasonable person to suffer significant mental anguish or distress. In addition, the law often recognizes disseminating intimate photos without consent as a criminal offense that may be prosecuted.<sup>95</sup> Furthermore, the federal cyberstalking law makes it a felony to use any “interactive computer service or electronic communication system” to “intimidate” a person in ways “reasonably expected to cause substantial emotional distress.”<sup>96</sup>

Traditional law has threshold problems involving the identification of the publisher, jurisdiction over foreign defendants, resource constraints of victims, and privacy risks of civil suits.<sup>97</sup> The penal code might not be the most efficient way to deal with the problem, since the legal system has many requirements before a court can render its decision and it can be helpful only in particular limited contexts.<sup>98</sup>

---

<sup>91</sup> See Klonick, *supra* note 57, at 1059.

<sup>92</sup> See Avlana K. Eisenberg, *Criminal Infliction of Emotional Distress*, 113 MICH. L. REV. 607, 623–24 (2015) (the plaintiff will have to demonstrate that the behavior was “extreme and outrageous”); Lipton, *Repairing Online Reputation*, *supra* note 81, at 28–38; JONES, *supra* note 79, at 70 (“Although there is no federal law against cyber bullying, some states drafted laws that address real and lasting harm without involving government censorship. Currently thirty seven states have online harassment laws.”).

<sup>93</sup> See Eisenberg, *supra* note 92, at 624.

<sup>94</sup> *Id.* at 627.

<sup>95</sup> See Franks, *supra* note 79, at 1256 (explaining that thirty-eight states have criminalized this behavior and a federal bill has been introduced in Congress called the Federal Intimate Privacy Protection Act of 2016).

<sup>96</sup> 18 U.S.C. § 2261A(2) (2018); Chesney & Citron, *supra* note 78.

<sup>97</sup> Citron, *supra* note 79, at 1929–31.

<sup>98</sup> See, e.g., Eisenberg, *supra* note 92, at 627–30 (reviewing the terms for prosecution under CIED. For example, if the prosecution does not prove intent, the CIED law does not apply).

Making matters worse, state and local law enforcement often fail to pursue complaints adequately because they lack training in the relevant laws and investigative techniques.<sup>99</sup> The authorities do not always enforce the law, or may place these violations lower on their priority lists.<sup>100</sup> Relief is also difficult in the civil process. Filing a civil action involves costly litigation and years can pass before a case is settled. In the meantime, the shaming continues, or even accelerates.<sup>101</sup>

Many individuals are usually responsible for sharing a legitimate post that turns into bad shaming. Not a single person is solely responsible for the damage, making litigation even more difficult, to the point of rendering it impossible because of the large number of potential defendants.<sup>102</sup> Keeping this in mind, one should remember that a court ruling might not necessarily restore the reputation of the shamed individual since the shaming expressions usually remain searchable via search engines. The law has an important role in expressing values but it might have only little effect on the rate of bad shaming.<sup>103</sup>

A second option for mitigating harm caused by shaming is self-help. The shamed individual can counter a defamatory speech, correct inaccurate speech, or explain his behavior. Scholars suggested that search engines should allow individuals to add a comment that would appear next to the search results that negatively refer to them, and for a short period Google experimented in this area.<sup>104</sup> The comment could

---

<sup>99</sup> Chesney & Citron, *supra* note 78.

<sup>100</sup> See SILVERMAN, *supra* note 23, at 75–82 (the police are usually disinterested in investigating spreading information online, unless there are threats of violence); see also Lipton, *Repairing Online Reputation*, *supra* note 81, at 16.

<sup>101</sup> See Klonick, *supra* note 57, at 1060; Lipton, *Repairing Online Reputation*, *supra* note 81, at 16 (“Criminal law does not typically require a victim to bear the costs of litigation. However, reliance on criminal law forces prosecutors and the police to be well versed in the law and in online conduct to make an effective case against the abuser.”).

<sup>102</sup> See Michal Lavi, *Forward, Share and Retweet: Meeting the Challenges of Spreading False Rumors on Social Networks*, in *THE CHALLENGES OF THE DIGITAL ERA: PRIVACY, INFORMATION, AND MORE* (Shlomit Yanisky-Ravid ed., forthcoming) (on file with author).

<sup>103</sup> See Waldman, *supra* note 76 (focusing on cyberbullying and explaining that anti-bullying laws enacted in all fifty states have important expressive values, but they have little effect on the rate of cyberbullying). See, e.g., Citron, *supra* note 79, at 1938–44 (addressing the limitation of current law in cases of infringement of sexual privacy).

<sup>104</sup> Frank Pasquale, *Rankings, Reductionism, and Responsibility*, 54 CLEV. ST. L. REV. 115, 135–36 (2006); Rustad & Kulevska, *supra* note 26, at 385 (“In 2007, Google experimented in this area by introducing a feature that allowed individuals who were mentioned in articles

be an explanation of the source, an apology, or an argument for disregarding the content.<sup>105</sup> However, this solution is limited because it is normally more efficient to ignore an expression than add a comment to it. If an expression stands without rebuttal, an audience may pay less attention to it.<sup>106</sup>

A third option for mitigating harm caused by shaming is reputation management and search engine optimization. The shamed individual can try to obscure the information by bombarding the internet with information. To do so, he can create personal profiles in social media and update them regularly.<sup>107</sup> Consequently, the page-rank of the shaming information will be downgraded, and it will become harder to access by search engines.<sup>108</sup>

Yet, in some instances of bad shaming, the mob “bombs” the internet with negative expressions to ensure the prominence of their content, making it difficult to manage one’s reputation successfully.<sup>109</sup> Furthermore, successful reputation management takes time; meanwhile,

---

indexed by Google News to add a comment that would appear next to the article. The comment could be an explanation of the information contained in the article, an apology, or an argument to why readers should disregard the content. However, Google later abandoned this feature.”)

<sup>105</sup> See Rustad & Kulevska, *supra* note 26, at 385. A different solution that relies on the same principle of rebuttal is a flagging system administrated by the Federal Trade Commission to flag true but misleading content. See Cook, *infra* note 195, at 19.

<sup>106</sup> See SUNSTEIN, *supra* note 21, at 25–26 (the very act of rebuttal focuses the audience on the expression in a way that increases its salience); see also Pennycook et al., *supra* note 21 (explaining that the more we are exposed to a statement, the more we tend to believe it, even if the additional exposure aims to disprove it).

<sup>107</sup> See Jon Ronson, ‘Overnight, Everything I Loved was Gone’: The Internet Shaming of Lindsey Stone, *GUARDIAN* (Feb. 21, 2015, 2:00 PM) <https://www.theguardian.com/technology/2015/feb/21/internet-shaming-lindsey-stone-jon-ronson> [https://perma.cc/ZRL5-SHT7]; RONSON, *supra* note 9, at 263 (giving an example: the story of a woman, Lindsey Stone, who published a picture of herself in a cemetery that can be interpreted as disrespectful. The picture was widely shared and people shamed her for it. Reputation management services helped her to fill the internet with neutral information in order to downgrade shaming content in search engine results). See also SILVERMAN, *supra* note 23, at 212. For a discussion of reputation management in general, see Lipton, *supra* note 81, at 41.

<sup>108</sup> See FINN BRUNTON & HELEN NISSENBAUM, *OBFUSCATION: A USER’S GUIDE FOR PRIVACY AND PROTEST* 87 (2015) (explaining practices for obfuscating information). See generally Hartzog, *The Public Information Fallacy*, *supra* note 29 (referring to the concept of obscurity as an essential component of modern notions of privacy); HARTZOG, *PRIVACY’S BLUEPRINT*, *supra* note 29, at 108.

<sup>109</sup> See CITRON, *supra* note 84, at 134.

the shaming persists and inflicts more harm.<sup>110</sup> In addition, the average user does not understand the operation of search engine algorithms and might need professional services to manage his reputation, which can be expensive.<sup>111</sup> Due to the costs of these services, only people with financial resources could use them,<sup>112</sup> whereas minorities and other disadvantaged groups in society would not be able to afford these services, and the shaming expressions will continue to haunt them.<sup>113</sup>

The easiest way to make negative information less accessible online is to bury it under highly-ranked positive or neutral information. Thus, reputation management provides a remedy only to those who are comfortable with increased online presence. This method essentially ignores privacy as a right and infringes on the desire for seclusion.<sup>114</sup> In addition, filling the internet with irrelevant information pollutes the flow of information, harms the information economy, and leads to inefficiency.<sup>115</sup> It may also interrupt social relation and erode trust in social networks and society as a whole.<sup>116</sup>

---

<sup>110</sup> See RONSON, *supra* note 9, at 263–74 (it takes time to achieve efficient results of reputation management).

<sup>111</sup> See JONES, *supra* note 79, at 74 (for example, companies such as Reputation.com); *see also* Klonick, *supra* note 57, at 1062–64 (online reputation management is effective because it can change what is being discussed and calibrate the punishment of online shaming); Cohen, *supra* note 39 (manuscript at 4) (“A new industry euphemistically titled ‘search engine optimization’ has emerged to serve the needs of both individuals and businesses seeking to burnish their public images.”).

<sup>112</sup> See RONSON, *supra* note 9, at 263–74.

<sup>113</sup> See Thomas H. Koenig & Michael L. Rustad, *Digital Scarlet Letters: Social Media Stigmatization of the Poor and What Can Be Done*, 93 NEB. L. REV. 592 (2015) (minorities and disadvantaged groups in society suffer from shaming more than the average population. Thus, shaming increases social gaps); Citron, *supra* note 79 (given “the way that stigma works and its collateral impact on the job market,” the harm compounds for women and minorities); JONES, *supra* note 79, at 74 (this is a “privacy for price” approach). On the distributive implications of the algorithm game, *see generally* Jane Bambauer & Tal Zarsky, *The Algorithm Game*, 94 NOTRE DAME L. REV. 1, 5 (2018) (“The algorithm game also has important yet unintuitive distributional consequences. Some populations will be less willing or able to engage in gaming, and therefore both gaming and counter-moves can have disparate effects on different subgroups.”).

<sup>114</sup> See JONES, *supra* note 79, at 75.

<sup>115</sup> Neil Richards & Woodrow Hartzog, *Privacy’s Trust Gap: A Review*, 126 YALE L.J. 1180, 1186 (2017).

<sup>116</sup> *Id.* at 1207.

The fourth solution is legal and focuses on allowing the removal of shaming content from the internet. Unlike a direct legal action against the publisher of the speech, this solution is directed towards the content providers. One example is a “notice-and-takedown” regime, namely, an obligation to remove offensive content once a potential plaintiff brings its existence to the attention of a platform owner. Under this solution, the emotional harm to the shamed individual may continue, but his reputational damage will be reduced. This solution is available in some jurisdictions,<sup>117</sup> but does not apply in the United States.<sup>118</sup> In addition, this regime is applicable only to bad shaming.<sup>119</sup>

Another legal solution strives to mitigate the problem by allowing a “right to delist” from search results. In Europe, the European Court of Justice (ECJ) ruled that search engines can be responsible for search results linking to false or irrelevant personal data, which appears on webpages published by third parties, if they decline to delist them after they received a request to delist.<sup>120</sup> Applying this regime will make it more difficult to access shaming information.

In the United States, there is no obligation to delist anyone, and as a result, search engines are immune to liability even if they do not remove offensive content upon request.<sup>121</sup> Adopting a right to be forgotten forms a remedy for dignitary harm even if a tort or a criminal offense had not been committed in the process of shaming. The scope of the right to be delisted from search engines involves a complex balance of considerations that will be discussed in the following Part.

---

<sup>117</sup> See Directive 2000/31, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1 [hereinafter Directive on Electronic Commerce]; see also Michal Lavi, *Content Providers' Secondary Liability: A Social Network Perspective*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 855, 870–71 (2016).

<sup>118</sup> See *infra* Section IV.C.2.

<sup>119</sup> On this solution and bad shaming, see *infra* Section V.B.

<sup>120</sup> See Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos* (May 13, 2014), [http://curia.europa.eu/juris/document/document\\_print.jsf?doclang=EN&docid=152065](http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065) [<https://perma.cc/2R8F-W9TF>] [hereinafter *Google Spain*].

<sup>121</sup> See *infra* Section IV.C.2.

## IV. SHAMING FOREVER?

This Part asks the following questions: Should shame stick to an individual forever and shackle him to his past? Or should the law recognize a reversibility principle and allow individuals to disassociate themselves from it?<sup>122</sup> Can the benefits of shaming be preserved in the *longue durée*, or are they lost over time? Should there be a right to delist links to shaming and, if so, when? Should the law differentiate between different types of shaming?

A. *In Praise of the Forgotten*

Since the beginning of time, forgetting has been the norm and remembering the exception.<sup>123</sup> Much has been written in praise of oblivion. Forgetting allows us to leave the past behind. It preserves the autonomy of the individual and it motivates individuals to develop and learn.<sup>124</sup> It promotes freedom of expression. It also promotes participatory democracy, because individuals know that they will not have to account for decisions and expressions they have made in the distant past. Consequently, they are more likely to express themselves freely and be engaged in the democratic process.<sup>125</sup> Oblivion also enables individuals to forgive others, move on with their lives, and be at peace.<sup>126</sup>

In some cases, society prefers oblivion to eternal memory and allows forgetting and forgiving as years pass. Legal forgiveness has its place in the United States. For example, bankruptcies are forgotten after a time,<sup>127</sup> and in some cases even criminals have their convictions

---

<sup>122</sup> See Tutt, *supra* note 11, at 1118.

<sup>123</sup> See VIKTOR MAYER-SCHÖNBERGER, *DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE* 1–15 (2009).

<sup>124</sup> See Tutt, *supra* note 11, at 1126.

<sup>125</sup> See *id.* at 1129.

<sup>126</sup> See JONES, *supra* note 79, at 14–16 (the ability to forgive and be at peace depends on escaping bad memories).

<sup>127</sup> See Fair Credit Reporting Act, 15 U.S.C. § 1681c(a)(1) (2018) (“[N]o consumer reporting agency may make any consumer report containing . . . [bankruptcies that] antedate the report by more than 10 years.”); Frank Pasquale, *Reforming the Law of Reputation*, 47 LOY. U. CHI. L.J. 515, 530 (2015) (“The FCRA requires that bankruptcies be removed from consumers’ credit

expunged from their records after sufficient time has passed, depending on the severity of the crime.<sup>128</sup> In addition, states generally provide minors a right to file a petition to expunge a juvenile court conviction.<sup>129</sup>

Society eliminates the stigma of past behavior in many instances, from arrests and convictions to debt forgiveness. This norm recognizes that humans may change for the better over time and learn from their experience.<sup>130</sup>

Forgetting has many benefits; however, due to modern digital technologies and global networks, forgetting has become the exception, and remembering the new rule.

### B. *Memory in the Digital Age*

People have struggled to preserve knowledge and hold on to their memories for centuries. To this end, they developed numerous devices and mechanisms. For example: books, recording devices, and cameras. Yet forgetting remained easier and cheaper than remembering.<sup>131</sup> However, the digital era revolutionized memory and its costs.<sup>132</sup> Everyone can record information, take a picture with a smartphone, publish an opinion or an article on the internet, and share their

---

reports one decade after they occur.”); *see also* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 281 (2016); JONES, *supra* note 79, at 140; Ravi Antani, *The Resistance of Memory: Could the European Union’s Right to Be Forgotten Exist in the United States?*, 30 BERKELEY TECH. L.J. 1173 1198 (2015).

<sup>128</sup> *See* JONES, *supra* note 79, at 141; Antani, *supra* note 127, at 1196–97 (legal forgiveness exists in U.S. law and is aimed to help rehabilitate those with a criminal past. However, there are exceptions. The public has a right to access information on serious crimes, including those involving sexual offenses and significant violent behavior. Thus, there are laws that require sex offenders to register in federal databases and report their crimes to neighbors). *See, e.g.*, 18 U.S.C. § 2250 (2018).

<sup>129</sup> *See* Rustad & Kulevska, *supra* note 26, at 379–80; Pasquale, *supra* note 127, at 535; Antani, *supra* note 127, at 1196.

<sup>130</sup> *See* MAYER-SCHÖNBERGER, *supra* note 123; Tutt, *supra* note 11, at 1132 (“The very notion of bankruptcy reveals our acceptance of the fact that beyond a certain point, the sheer magnitude of a person’s debt may be demoralizing.”).

<sup>131</sup> *See* MAYER-SCHÖNBERGER, *supra* note 123, at 49.

<sup>132</sup> *Id.* at 51; ERIK BRYNJOLFSSON & ANDREW MCAFEE, THE SECOND MACHINE AGE: WORK, PROGRESS, AND PROSPERITY IN A TIME OF BRILLIANT TECHNOLOGIES 9 (2014) (we are entering the second machine age, an age of astonishing progress with digital technologies).



information with everyone.<sup>133</sup> Search engines changed the rules of the information lifecycle by allowing anyone to find information easily, years after it had been first disseminated.<sup>134</sup> Digital memory and data mining increase the information available to vendors, who make use of them in their marketing strategies.<sup>135</sup> They also improve the information gathering practices of the government as it forms its policy.<sup>136</sup> Digital memory has many important benefits, but it can expose individuals and society to harmful consequences in many areas.<sup>137</sup>

Digital memory can impair the benefits of online shaming because it remains online long after it had served its purpose. This leads users to be exposed to shaming without being aware of the context and the circumstances of the case. Meanwhile, the shamed individual might have reformed his behavior, and the shaming information no longer represents him.<sup>138</sup> At this stage, shaming is less useful for norm enforcement. Furthermore, this “after life” of shaming can over-deter the shamed individual and society in general.

Technological developments have changed the balance between free speech and the right to dignity, reputation, and privacy. How should the law react to these changes? Should it recognize dignitary harm that is not a result of a tort or a criminal offense? Should it allow the right to be forgotten even in cases of shaming?

### C. *Rediscovering Forgetting: A Comparative Perspective*

This Section explores the legal approaches to forgetting. It begins with the law in the European Union and the ruling of the ECJ in the

---

<sup>133</sup> See SILVERMAN, *supra* note 23, at 45 (sharing information has become a part of our personality, and if we do not record, publish, and share information, it is as if it did not exist).

<sup>134</sup> ZUBOFF, *supra* note 25, at 58–59 (“[I]nformation that would normally age and be forgotten now remains forever young, highlighted in the foreground of each person’s digital identity”).

<sup>135</sup> See JOSEPH TUROW, *THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY AND DEFINE YOUR POWER* 169 (2017); ZUBOFF, *supra* note 25, at 94–97.

<sup>136</sup> See MAYER-SCHÖNBERGER, *supra* note 123, at 60.

<sup>137</sup> *Id.* at 96.

<sup>138</sup> See JONES, *supra* note 79, at 124; SILVERMAN, *supra* note 23, at 82 (explaining that the dissemination of a viral post stops after a while. Yet, it leaves an afterlife trail that can be located via search engines and hashtags).

*Google Spain* case that granted a version of a right to be forgotten.<sup>139</sup> It then discusses the opposite approach in the United States.

### 1. E.U.

The E-Commerce Directive dictates the framework for intermediaries' liability in the European Union.<sup>140</sup> The Directive does not impose a general duty of care on intermediaries to monitor content on their websites. The intermediaries are insulated from liability, provided that they remain passive facilitators and react upon knowledge of illegal content. This framework can apply to bad shaming and allow its removal from the platforms. In general, the Data Protection Directive (DP Directive) provides the framework for forgetting in the European Union,<sup>141</sup> and it is directed at supervisors and processors of personal data in the European Union.<sup>142</sup> One of the principles of the DP Directive is that the collected data must be "adequate, relevant, and not excessive in relation to the purpose for which they are collected and/or further processed."<sup>143</sup> Article 12(b) guarantees that a data subject may rectify, erase, or block processing of data if they are incomplete or inaccurate.<sup>144</sup>

When the DP Directive was enacted, the internet was in its infancy, and search engines were rudimentary. Consequently, it was difficult for people to find relevant information online. Google revolutionized

---

<sup>139</sup> See *Google Spain*, *supra* note 120. This ruling obligated search engines to delist links to inaccurate, irrelevant, or excessive data from search results following a request of the data subject.

<sup>140</sup> Directive on Electronic Commerce, *supra* note 117. For expansion on the safe haven and its limitations, see Lavi, *supra* note 40, at 171–72. The European Council issued recommendations for dispute resolution procedure regarding the content removed. See Recommendation 2018/334, of the European Commission of 1 March 2018 on Measures to Effectively Tackle Illegal Content Online, 2018 O.J. (L 63) 50, 58 ("Member States are encouraged to facilitate, where appropriate, out-of-court settlements to resolve disputes related to the removal of or disabling of access to illegal content.").

<sup>141</sup> Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter DP Directive].

<sup>142</sup> For the definitions of processors and controllers, see *id.* art. 2(d)(e).

<sup>143</sup> See *id.* art. 6(1)(c).

<sup>144</sup> See *id.* art. 12(b). These principles were entrenched a decade later in Art. 8 of the Charter of Fundamental Rights of the European Union, titled "Protection of personal data."

search engines' abilities to help users find relevant information.<sup>145</sup> Due to technological developments, remembering is the new default. This default is in tension with the DP Directive, which limits the identification of data subjects for no longer than is necessary for the purpose for which the data was collected.<sup>146</sup>

The tension between the technological ability to collect and store information and the DP Directive was at the core of the decision in *Google Spain v. AEPD*.<sup>147</sup> Spanish citizen Mario Costeja González filed a complaint with the Spanish data protection agency (AEPD) against Google Spain, Google, and the Spanish newspaper *La Vanguardia*. He alleged that a Google search of his name returned links to a 1998 *La Vanguardia* article that included an announcement of a real estate auction of González's house, which was subject to attachment proceedings due to his failure to pay social security debts. González claimed that the publication of these old posts violated his privacy rights under the DP Directive because "the attachment proceedings . . . had been fully resolved for a number of years and that reference to them were now entirely irrelevant."<sup>148</sup>

The AEPD ruled in favor of González against Google Spain and Google, but rejected the claim against the newspaper because it had lawfully published the content.<sup>149</sup> Google appealed through the Spanish court system, which referred the case to the European Union's high court. The Court of Justice of the European Union (CJEU) decided that Google's search activity met the definition of "data controller" under Article 2(d) of the DP Directive. It explained that the search engine's collection, storage analysis, and ranking of content were acts that "determined the purpose and means" of personal data in the system. The court also found that, as a data controller, Google was "processing"

---

<sup>145</sup> See Rustad & Kulevska, *supra* note 26, at 353.

<sup>146</sup> Edward Lee, *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, 49 U.C. DAVIS L. REV. 1017, 1030 (2016); see also DP Directive, *supra* note 141, at art. 6(1)(e). Cf. Miquel Peguera, *The Shaky Ground of the Right to Be Delisted*, 18 VAND. J. ENT. & TECH. L. 507, 522 (2016).

<sup>147</sup> See *Google Spain*, *supra* note 120.

<sup>148</sup> See Lee, *supra* note 146, at 1030.

<sup>149</sup> *Id.* The AEPD ruling justified the newspaper in posting the auction notice because "it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible." *Id.*

personal data under Article 2(b). As a controller, a search engine “must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of [the DP Directive].”<sup>150</sup>

Following this analysis and conclusion, the CJEU held that the right to data protection includes the right of “rectification, erasure or blocking of data” under Article 12(b) of the DP Directive, as well as Article 14(a) that provides the right to object to data processing. The court determined that Google must remove the links to González’s name from search results, even though the website lawfully published the information.<sup>151</sup> The court also acknowledged a right to be forgotten, but the decision did not explain what this right entailed. It is not clear what exactly violated the DP Directive. Was it the fact that the posts contained personal information that was published sixteen years prior? Or did Google violate the DP Directive because the information became irrelevant?<sup>152</sup> If the reason is the latter, at what point should Google determine that information is no longer relevant?

The CJEU clarified that personal information does not have to be prejudicial in order to establish a right of erasure and that, “as a rule,” the privacy interests of the individual outweigh both the search engine’s economic interest and the public’s interest in finding the information. However, the CJEU noted that the right to be forgotten is subject to a case-by-case balancing test that weighs the public’s interest in obtaining information with the individual’s right to privacy.<sup>153</sup>

This ruling left unclear whether the right to be forgotten is instrumental, and thus aims to protect data privacy, or whether it protects dignitary privacy.<sup>154</sup> The court offered little guidance on

---

<sup>150</sup> *Google Spain*, *supra* note 120, at ¶ 38.

<sup>151</sup> For criticism of this decision, see Post, *supra* note 26, at 1068 (arguing that this remedy “is comprehensible neither within the instrumental logic of the Directive, which does not contain concepts of harm of the public interest, nor within the normative logic of the right to be forgotten, which [would not be triggered by the processing of personal data and thus] would not separate Google from its underlying websites”).

<sup>152</sup> See Lee, *supra* note 146, at 1033–34; see also JONES, *supra* note 79, at 42.

<sup>153</sup> See Lee *supra* note 146, at 1022.

<sup>154</sup> See *Google Spain*, *supra* note 120, at ¶¶ 98–99; Post, *supra* note 26 (explaining that the ruling focuses on the instrumental rationale of controlling the information but partially relies on rationales of protecting dignitary privacy).

implementing the right to be forgotten. Therefore, the Article 29 Working Party—an institution composed of representatives of the national data protection authorities (DPAs), the European Data Protection Supervisor, and the European Commission—tried to fill in the gaps by issuing guidelines on how right to be forgotten requests should be decided, which contained thirteen criteria for search engines to consider.<sup>155</sup> The “Article 29 Working Party guidelines, again, do not have the direct force of law,” but they are strongly indicative of how the law will be interpreted by its enforcers.<sup>156</sup> In addition to Article 29 Working Party guidelines, Google established an advisory council on the right to be forgotten and identified four main criteria for its decision-making process.<sup>157</sup>

The CJEU decision asserted only a right to delist the link from a search result, as opposed to a right to remove the information from search engines’ indexes altogether. It strove only to make it difficult to discover old personal information by obstructing it.<sup>158</sup>

Yet, even though *Google Spain* only required the information to be obscured, the guidelines issued by the Article 29 Working Party state that the right to be forgotten requires search engines to remove links on all their domains, including those outside the European Union. Thus,

---

<sup>155</sup> Lee, *supra* note 146, at 1045 & n.152 (citing ARTICLE 29 DATA PROT. WORKING PARTY, GUIDELINES ON THE IMPLEMENTATION OF THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT ON “GOOGLE SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ” C-131-12 13–20 (2014), [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf) [https://perma.cc/7A7J-VUJW] [hereinafter Art. 29 Data Prot. Working Party, Guidelines]).

<sup>156</sup> Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 194 (2019) (referring to their guidelines in the context of the right to explanation of algorithmic decision-making).

<sup>157</sup> Michael J. Kelly & David Satola, *The Right to Be Forgotten*, 2017 U. ILL. L. REV. 1, 17 (identifying the criteria as “(1) the data subject’s role in public life”; “(2) the nature of information which is subject of the delisting request”; “(3) the source of the information requested to be delisted; and (4) the timing (relevance) of when the information was posted”).

<sup>158</sup> See JONES, *supra* note 79, at 94; Peguera, *supra* note 146, at 549; see also Balkin, *supra* note 42, at 1202 (explaining that requiring newspapers to take down stories would appear to be a serious intrusion into the freedom of the press. Instead, the CJEU has targeted search engines, on the ground that under the terms of the directive search engine, companies are data controllers and protect personal information). It should be noted that the right is not absolute and does not allow, in itself, erasure from public registry. See *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017 E.C.R. (case C-398/15).

these guidelines might have global implications that extend beyond removal from the search results in the European Union.<sup>159</sup> The global application of the right to be forgotten is disputed, with an appeal by Google against the French data protection agency's (CNIL) order for global delisting pending.<sup>160</sup>

It should be noted that the General Data Protection Regulation (GDPR), which replaced the DP Directive, includes a specific provision titled "Right to erasure ('right to be forgotten')." This provision does not deal specifically with search engines. However, it guarantees the right to erasure by imposing on the data controller obligations to erase data. This provision may apply to internet websites, leading to erasure and not just obstruction.<sup>161</sup> Yet it is more likely to be interpreted the former way in light of *Google Spain*.<sup>162</sup>

---

<sup>159</sup> See Lee, *supra* note 146, at 1041–42 (citing Art. 29 Data Prot. Working Party, Guidelines, *supra* note 155, at 3, 9). For criticism, see Balkin, *supra* note 42, at 1204–06 (explaining that applying the right to be forgotten globally threatens the public good of the internet).

<sup>160</sup> See Natasha Lomas, *Google's Right to Be Forgotten Appeal Heading to Europe's Top Court*, TECHCRUNCH, <https://techcrunch.com/2017/07/19/googles-right-to-be-forgotten-appeal-heading-to-europes-top-court> [https://perma.cc/72UG-VB6D] (last visited Mar. 30, 2019). The appellate court decided to refer certain questions to the CJEU for preliminary ruling before coming to a judgment on the case. *Id.* It should be noted that preliminary opinion of ECJ found that the right to be forgotten should be enforced locally and not globally. See Owen Bowcott, *'Right to Be Forgotten' by Google Should Apply Only in EU, Says Court Opinion*, GUARDIAN (Jan. 10, 2019, 6:36 PM), <https://www.theguardian.com/technology/2019/jan/10/right-to-be-forgotten-by-google-should-apply-only-in-eu-says-court> [https://perma.cc/77Y4-8FPQ].

<sup>161</sup> See Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 17 [hereinafter GDPR]; Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMM. TECH. L. 65, 90 (2019) ("Roughly summarized, a data subject has a right to erasure when he or she successfully exercises the right to object, when the personal data were unlawfully processed, should be erased because of a legal obligation, or are no longer necessary in relation to the processing purposes."); Peguera, *supra* note 146, at 557–58; see also JONES, *supra* note 79, at 10 (explaining that Article 17 to the GDPR, titled "Right to erasure ('right to be forgotten')," can impose obligations on controllers to delete information from the internet altogether); Cook, *supra* note 195, at 7–8; Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 68–69 (2017).

<sup>162</sup> Post, *supra* note 26, at 986–87 (explaining that the GDPR "marks the triumph of a distinctive EU variant of the right to be forgotten that derives directly from data privacy" and is therefore "likely to be interpreted in light of *Google Spain*"); see also Edwards & Veale, *supra*

This new policy applies equally to all types of shaming presented in the taxonomy mentioned in Part II.

## 2. U.S.

The First Amendment to the U.S. Constitution affords extensive protection to freedom of speech. The margins of protection are even wider on the internet.<sup>163</sup> In the United States, there is neither a general right to be forgotten nor a right to delist from search results. In fact, the law does not provide shamed individuals any redress<sup>164</sup> outside of a few legislative exceptions.<sup>165</sup> For example, there is no redress if the media

---

note 161, at 72 (“[T]he GDPR makes it plain that a controller is only obliged to do this as far as is reasonable . . . .”); Alexander Tsesis, *Data Subjects’ Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 U. COLO. L. REV. 593, 602 (2019) (explaining that there is a right to erasure of data that was collected and stored by websites. Thus, erasure from the websites is not likely to apply regarding data that was publicly published on websites by third parties).

<sup>163</sup> See Oreste Pollicino & Marco Bassini, *Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis*, in RESEARCH HANDBOOK ON EU INTERNET LAW 508 (Andrej Savin & Jan Trzaskowski eds., 2014) (the U.S. freedom of expression enjoys extensive protection relative to the protection in the European Union. Freedom of expression is even wider on the internet); see also Rustad & Kulevska, *supra* note 26, at 376–77 (explaining that while free speech receives broad protection, the United States has no comprehensive privacy framework, but rather a sectorial approach to legislating privacy rights).

<sup>164</sup> See *Garcia v. Google, Inc.*, 786 F.3d 733, 745–46 (9th Cir. 2015); *Nelson v. Comm’r of Soc. Sec.*, No. 14 Civ. 1109 (ENV), 2017 WL 1314118 (E.D.N.Y. 2017); *Yeager v. Innovus Pharm., Inc.*, No. 18-cv-397, 2019 WL 447743 (N.D. Ill. Feb. 5, 2019).

<sup>165</sup> There is legislation that acknowledges a right to erasure in some contexts, such as the “notice-and-takedown” regime in section 512 of the Digital Copyright Millennium Act (DMCA). There are also some developments at the state level. For example, the state of California gave children the right to delete posts that they made on social media such as Facebook. However, this narrow right of erasure merely covers the deletion of posts that children made themselves, not content about them. S.B. 568, 2013–14 Leg., Reg. Sess. (Cal. 2013); Rustad & Kulevska, *supra* note 26, at 380; JONES, *supra* note 79, at 67–68; Kelly & Satola, *supra* note 157, at 44–45; see also HARTZOG, *supra* note 29, at 79. In a related context, California also recently enacted legislation granting a right to erasure in the consumer protection context. CAL. CIV. CODE § 1798.105 (West 2018); Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)* 4 (Santa Clara Univ., Legal Studies Research Paper, 2018), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3211013](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013) [<https://perma.cc/5Y8G-JAZ5>] (“Erasure. Upon a consumer’s request, a business shall delete any personal information about the consumer that the business collected from the consumer.”) (citing CAL. CIV. CODE § 1798.105).

publishes local stories on the internet about an arrest and the charges are later dropped.<sup>166</sup> Moreover, even if an expungement statute requires the destruction of all police and court records, there is no guarantee that removing one's name from an official database will render one's reputation untarnished by news of an arrest that previously spread on the internet.<sup>167</sup>

Even in cases of bad shaming, when the information published on an individual contains defamatory expressions, the law does not offer redress. Federal legislation limits lawsuits against online intermediaries, or platform owners.<sup>168</sup> Section 230(c) of the Communications Decency Act (CDA) states: "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."<sup>169</sup> In other words, Congress declared that online intermediaries cannot be treated as publishers for material authored by third parties.<sup>170</sup> The courts have interpreted section 230 broadly and repeatedly shielded web enterprises

---

<sup>166</sup> See *Martin v. Hearst Corp.*, 777 F.3d 546, 553 (2d Cir. 2015) (surmising that reasonable readers would know that charges are dropped against some percentage of those arrested, and publishers need not provide an update that the charges were nulled).

<sup>167</sup> Expungement statutes do not impart obligations to third parties. See *JONES*, *supra* note 79, at 64; Pasquale, *supra* note 127, at 535.

<sup>168</sup> The immunity for third-party content also applies to state crimes, but not to federal criminal offenses. See Eric Goldman, *The Implications of Excluding State Crimes from 47 U.S.C. § 230's Immunity 2* (Santa Clara Univ., Legal Studies Research Paper No. 23-13, 2013), [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2287622](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2287622) [<https://perma.cc/U5XB-6BDZ>]. Immunity also does not apply to copyright infringement that is subject to the Digital Millennium Copyright Act's notice-and-takedown regime. Pub. L. No. 105-304, § 202, 112 Stat. 2860, 2877 (1998) (codified in scattered sections of 17 U.S.C.).

<sup>169</sup> 47 U.S.C. § 230(c)(1) (2018); Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 262 (2006). By passing section 230, Congress sought to overrule *Stratton Oakmont v. Prodigy*, in which an unidentified user defamed an investment firm on Prodigy's "Money Talk" bulletin board. *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at \*1-2 (N.Y. Sup. Ct. May 26, 1995). The New York trial court decided that Prodigy acted as a publisher when it screened its site to make it family-friendly and held that Prodigy was responsible for third parties' messages on its board. *Id.* at \*10-11. Recognizing the injustice of this case, legislators drafted section 230 to exempt content providers from traditional publishers' liability. See Vanessa S. Browne-Barbour, *Losing Their License to Libel: Revisiting § 230 Immunity*, 30 BERKELEY TECH. L.J. 1505, 1525 (2015).

<sup>170</sup> Congress sought to promote self-regulation and free speech, and foster the rise of vibrant internet enterprises. See Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 651-52 (2014).



from primary and secondary liability in a wide variety of claims.<sup>171</sup> Intermediaries retain immunity even if they avoid taking action after learning about potentially illegal content on their site.<sup>172</sup>

This result has been criticized in legal scholarship. Scholarly work has suggested narrowing section 230 immunity.<sup>173</sup> In addition, some scholars and policymakers have called for changes that allow “forgetting and forgiving” within the boundaries of the First Amendment.<sup>174</sup> However, other scholars have outlined specific policy changes that create the right to delist from search results by analogizing these policies to currently existing laws, such as credit reporting laws and expungement statutes, or, in severe cases of bad shaming, to nonconsensual dissemination of intimate photos or cyberbullying.<sup>175</sup> These scholars emphasize the importance of outlining a right to be

---

<sup>171</sup> See *Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (“By its plain language, § 230 creates a federal immunity to *any* cause of action that would make service providers liable for information originating with a third-party user of the service.”) (emphasis added); see also *Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 27–28 (2d Cir. 2015) (per curiam); *Dowbenko v. Google Inc.*, 582 F. App’x 801, 804–05 (11th Cir. 2014) (per curiam); *GoDaddy.com, LLC v. Toups*, 429 S.W.3d 752 (Tex. App. 2014).

<sup>172</sup> See *Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc.*, 591 F.3d 250, 254 & n.4 (4th Cir. 2009); see also, e.g., *Klayman v. Zuckerberg*, 753 F.3d 1354, 1355 (D.C. Cir. 2014); *Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056, 1064–66 (N.D. Cal. 2016), *aff’d*, 700 F. App’x 588, 590 (9th Cir. 2017), *cert. denied*, 138 S. Ct. 1027 (2018), *reh’g denied*, 138 S. Ct. 2021 (2018); *Doe v. Am. Online, Inc.*, 783 So. 2d 1010, 1017 (Fla. 2001).

<sup>173</sup> See Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401 (2017); Browne-Barbour, *supra* note 169, at 1554; Zak Franklin, *supra* note 79, at 1334–35.

<sup>174</sup> See JONES, *supra* note 79, at 164 (“Even in the US there are ways to make the digital age a forgiving era. But the ways must be within the boundaries of what makes Americans most free”); see also Tutt, *supra* note 11, at 1158; Kelly & Satola, *supra* note 157, at 51 (explaining that Americans themselves support the establishment of some form of a “right to be forgotten”: 61% of Americans favor some form of a “right to be forgotten,” 39% want a broad European-style right, and 47% believe that irrelevant search results can harm reputation and that the law should allow some degree of a right to be forgotten); SCI., TECH., & SOC’Y, FORMULATING AND IMPLEMENTING A RIGHT TO BE FORGOTTEN IN THE UNITED STATES: AMERICAN APPROACHES TO A LAW OF INTERNATIONAL ORIGIN 17 (2015), [https://getinspired.mit.edu/sites/default/files/documents/ST118\\_Report.pdf](https://getinspired.mit.edu/sites/default/files/documents/ST118_Report.pdf) [<https://perma.cc/W275-BQQX>] (“[T]he United States can work to establish international soft law guidelines (that is, non-binding laws that help to guide the binding laws of states) to experiment with the right and eventually develop a unique version of the right to be forgotten specific to each country’s cultural context.”) (suggesting a modified approach to the right to be forgotten in the United States).

<sup>175</sup> See Antani, *supra* note 128, at 1210; Pasquale, *supra* note 127, at 537.

forgotten in order to harmonize U.S. law with European data protection and privacy laws,<sup>176</sup> and to allow transatlantic portability of information.<sup>177</sup>

As of today, there is no right to be forgotten in the United States, and thus, shamed individuals cannot find redress, even for bad shaming.

#### D. *Rethinking Remedies for Dignitary Harm in the Digital Age*

Dissemination of information in the digital age has different characteristics than dissemination in the analog era because technology has changed the balance between freedom and control. For example, smartphones and similar devices allow for the dissemination of information to a wide audience easily and instantly, almost without cost, through constant connection to the internet. Technology also influences

---

<sup>176</sup> See, e.g., Rustad & Kulevska, *supra* note 26, at 406–08 (proposing a right to be forgotten for private persons upon proof that the information serves no purpose other than to embarrass or extort payment from the data subject and that there is no compelling public interest in the information).

<sup>177</sup> See *id.* at 386 (predicting that without a right to be forgotten, renegotiation for an agreement for data portability would be necessary for allowing transatlantic portability of information); Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. (forthcoming 2019) (manuscript at 6) (“[P]rinciples found in the GDPR, such as data portability and the ‘right to be forgotten,’ are already influencing laws outside Europe.”). Harmonizing United States and European laws will allow data portability from the E.U. to the U.S. In the past, a safe harbor that allowed the transfer of personal data if the U.S. ensured an adequate level of protection to the personal data transferred. In *Schrems v. Data Protection Commissioner*, the ECJ declared that this safe harbor was invalid. Case C-362/14, *Schrems v. Data Prot. Comm’r* (Oct. 6, 2015), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143358> [<https://perma.cc/28ZA-4ZUE>]. Following this decision, the United States and the European Union reached a new arrangement called the Privacy Shield. This arrangement imposes stronger obligations on U.S. companies to protect Europeans’ personal data. It requires the United States to more robustly monitor and enforce, and to cooperate with European Data Protection Authorities. See Christopher Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, 18 GERMAN L.J. 881, 882–84 (2017); Beata A. Safari, *Intangible Privacy Rights: How Europe’s GDPR Will Set a New Global Standard for Personal Data Protection*, 47 SETON HALL L. REV. 809, 816–20 (2017). Harmonization of the right to be forgotten would allow the United States to better satisfy the obligations of the Privacy Shield agreement. For a deeper explanation of the adequacy requirement with E.U. regulation, the privacy shield arrangement, and potential problems, see Kuner, *supra*, and Schwartz, *supra* (manuscript at 12, 20).

the context in which information is disseminated, and may exacerbate dignitary harm. For example, facial recognition technology enables the automatic linking between a person and his picture.<sup>178</sup> Technologies that allow tagging people make it easier to find embarrassing information about them long after the initial dissemination.<sup>179</sup> Furthermore, search engines index content and allow it to easily be found, even years after it was first disseminated.<sup>180</sup>

The digital environment challenges traditional methods of protecting fundamental rights. Therefore, current law must address new risks and dignitary damages.<sup>181</sup> The scope and velocity of dissemination and the ability to easily find information on particular individuals justify new remedies, even when the harm does not result from a criminal offense or a civil tort. This is precisely the time to develop a comprehensive understanding of dignitary harm and to make an explicit commitment to protect it. The current legal environment would greatly benefit from the evolution of remedies. Recognizing general dignitary harm, in addition to traditional sanctions or compensation under criminal or civil liability, allows for a soft remedy for the infringement of dignitary interests resulting from digital dissemination.

This remedy would provide for the removal of links to search results of shaming expressions in certain situations. It would not preclude additional investigation and sanctions of the direct offenders, compensation, or other remedies when the dignitary harm reaches the

---

<sup>178</sup> See, e.g., Woodrow Hartzog & Evan Selinger, *Why You Can No Longer Get Lost in the Crowd*, N.Y. TIMES (Apr. 17, 2019), <https://www.nytimes.com/2019/04/17/opinion/data-privacy.html>; Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html> (describing China's use of facial recognition technology); see also sources cited *supra* note 17.

<sup>179</sup> See generally SUNSTEIN, *supra* note 39, at 4 (“[T]he whole idea of the hashtag is to enable people to find tweets and information that interests them. It’s a simple and fast sorting mechanism.”).

<sup>180</sup> The ability to search information turns the past into present. See Solove, *supra* note 20, at 15–19; BOYD, *supra* note 20, at 10–11 (referring to constant visibility of conversation and the ability to search information); see also EVGENY MOROZOV, *TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM* 279–80 (2013).

<sup>181</sup> In the related context of the scope of the First Amendment right to record in light of dignitary interests, see Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 217 (2017) (“[T]he scope of the protectable right changes because the nature of the harm changes.”).

threshold of a criminal offense or a civil tort, nor would it preclude extra-legal tools. This proposed remedy for dignitary harm also would not depend on the publisher's fault or wrongful act. It would allow for a nuanced remedy for digital dignitary harm, even when traditional law does not provide redress.

The principles of speech torts are well suited to recognizing and addressing digital dignitary harm, and can provide a basis of duty and a source for the remedy. A new remedy for dignitary harm not caused by a criminal offense or a civil tort is in line with defamation or false light claims. The rationale for recognizing these claims is that even information that was true at the date of publication may fail to reflect reality when it remains widely accessible and available years after its first publication.<sup>182</sup> Thus, it may turn into defamation when time passes.<sup>183</sup>

The idea or legal recognition of new remedies for digital dignitary harm was debated in literature in a related context. Recent scholarly literature recognizes the dignitary harm of collection and analysis of data on individuals by using big data, algorithms, and AI that manipulate individuals, influence their opportunities, ties them to their past actions, and infringes on their "right to future tense."<sup>184</sup>

As a response to the transformative change in the ability to collect and analyze data, Professor Jack Balkin proposed accommodating fiduciary and tort laws to the digital age. First, Balkin develops the concept of information fiduciaries.<sup>185</sup> Accordingly, intermediaries should neither breach user trust nor take actions that users would

---

<sup>182</sup> JONES, *supra* note 79, at 149–50.

<sup>183</sup> Lavi, *supra* note 40 (focusing on a related context of repeated dissemination of speech and suggesting that, even if the original speech was not defamatory, it can turn into defamation when context changes—for example, when speech is disseminated selectively or when disseminators add headlines to the content. Similarly, old and irrelevant information that is taken out of its original context and appears in a search result can in some circumstances be considered defamation).

<sup>184</sup> ZUBOFF, *supra* note 25, at 58, 329; Balkin, *supra* note 42.

<sup>185</sup> See Balkin, *supra* note 42, at 1161 (analogizing intermediaries' duties towards users' information to doctors' and lawyers' fiduciary duties towards their patients, and explaining that digital companies collect vast amounts of user data and utilize this information to predict and influence user activity. Therefore, Balkin suggests referring intermediaries as information fiduciaries).

reasonably consider unexpected or abusive.<sup>186</sup> Second, Balkin develops the concept of algorithmic nuisance for accommodating intermediaries' infringements of rights towards people with whom they lack a contractual relationship by classifying them and constructing their identities and reputations.<sup>187</sup> Thus, new concepts aspire to allow a relief for individuals who bore dignitary harm due to the use of their information.

Dissemination of information that is reflected on digital platforms and can be found by using search engines also requires policymakers to rethink new remedies for dignitary harm. Today, there are no legal remedies for dignitary harm that was not a result of bad shaming under the U.S. law. Adopting the right to be forgotten will allow a soft remedy for more types of shaming that can be added to existing legal and extralegal remedies.

E. *Normative Considerations on the Right to Delist (Right to Be Forgotten)*

After overviewing two dichotomous approaches towards the right to be forgotten (the E.U. approach of oblivion and the U.S. approach of memory), this Section focuses on the normative considerations regarding the right to delist links to shaming search results of private individuals. The analysis serves as a first step in considering whether and when to apply this right.

---

<sup>186</sup> See Balkin, *supra* note 42 (referring to the collection, analyzing, and manipulation of information by online intermediaries as a breach of fiduciary for platforms users). It should be noted that the information fiduciary concept raises challenges regarding its feasibility, enforceability, and scope. For recent criticism that identifies tensions and ambiguities in the theory of information fiduciaries, see Lina Khan & David Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. (forthcoming 2019).

<sup>187</sup> See Balkin, *supra* note 42, at 1165, 1168. This concept builds on an analogy to the common law concepts of public and private nuisance.

### 1. In Praise of a Right to Delist

A central argument in favor of a right to be forgotten is the change in the balance between memory and oblivion in the digital age.<sup>188</sup> Today, everyone can publish or disseminate information, whether harmful or not. The number of posts online increases the prevalence of bad shaming and the likelihood that other types of shaming evolve into bad shaming. Even good shaming might become unjust over time. By barring the right to delist, the balance of just punishment might be breached.<sup>189</sup>

In most cases, the arguments in favor of good shaming lose weight after the norm was enforced and deterrence was achieved.<sup>190</sup> Bad shaming that contains defamation or nonconsensual intimate photos has no benefits to begin with. Shaming that was taken out of context and evolved into defamation, cyberbullying, or harassment loses its benefits.<sup>191</sup> The arguments in favor of shaming the ugly behavior also lose their force over time. Often, shaming can lead to legal sanctions against a person who committed a felony. Yet, after the person was punished, it is unjust to keep excluding him from society. Similarly, shaming for violation of norms can be justified a few months after the norm was violated, but becomes disproportionate after a while. Tying the shamed individual to his past infringes on elemental rights that bear on his sovereignty and his right to future tense.<sup>192</sup>

---

<sup>188</sup> See Tutt, *supra* note 11, at 1154 (permanence and easy stand to impinge on reversibility in a new significant way).

<sup>189</sup> See Pasquale, *supra* note 123, at 533 (explaining that wiping off a credit report according to the Fair Credit Reporting Act does no good if it can be easily found via Google search).

<sup>190</sup> Indeed, there are exceptions; the rationales for shaming may still apply when the crime is serious. For example, the public has a right to access information about sexual offenses and significant violent behavior. In such cases, the public interest outweighs any interest to the offender himself or the societal value in rehabilitation. Legal frameworks already establish the significance of the public's right to information. For example, there are laws that require sex offenders to register in federal databases and report their crimes to neighbors, and a right to be forgotten should not apply to delisting links to this type of information. As one proponent of the right to be forgotten states, "some criminal activity will never be considered for informational forgiveness." Antani, *supra* note 128, at 1197.

<sup>191</sup> See *supra* Section II.B.

<sup>192</sup> See ZUBOFF, *supra* note 25, at 58, 329.

Everlasting shaming of ordinary people is unjustified. In contrast to public figures and celebrities, ordinary people rarely have a desire to be in the limelight. Their interest in privacy is typically stronger, and the public's interest in the information is lower.<sup>193</sup> This realization calls for a reconsideration of the balance between memory and oblivion.

The right to be forgotten narrows social inequality. Not extending the right to delist will result in leaving only poor people shamed, because rich people can afford reputation management services.<sup>194</sup> In addition, poor people and minorities in particular are shamed more frequently than are privileged segments of society. Leaving them with a tarnished mark undermines their economic and educational opportunities and reinforces social gaps.<sup>195</sup> The right to delist will promote distributive justice and narrow social gaps because it will equalize privileged individuals who can afford reputation management services with those who lack the resources.<sup>196</sup>

Acknowledging a right to delist has many benefits. Yet there are objections to this right. The following Subsections will address them.

---

<sup>193</sup> See Rustad & Kulevska, *supra* note 26, at 407; see also Klonick, *supra* note 26.

<sup>194</sup> See Ronson, *supra* note 9, at 263–74 (online reputation management services can be very expensive, especially when the shaming expressions were spread widely).

<sup>195</sup> See Koenig & Rustad, *supra* note 113, at 506 (explaining that social media amplifies stereotypic images of the poor and minorities in particular because they are not mainstream); see also Hannah L. Cook, *Flagging the Middle Ground of the Right to Be Forgotten: Combatting Old News with Search Engine Flags*, 20 VAND. J. ENT. & TECH. L. 1, 4 (2017) (“[A]most 80 percent of employers use search engines to learn about job applicants, and most of those (almost 70 percent) will reject applicants based on what they find.”); Megan Angelo, *You Are What Google Says You Are*, WIRED (Feb. 11, 2009, 11:43 AM), <https://www.wired.com/2009/02/you-are-what-go> [<https://perma.cc/5Y39-ARKY>]; Press Release, CareerBuilder, Number of Employers Using Social Media to Screen Candidates at All-Time High, Finds Latest CareerBuilder Study (June 15, 2017), <http://press.careerbuilder.com/2017-06-15-Number-of-Employers-Using-Social-Media-to-Screen-Candidates-at-All-Time-High-Finds-Latest-Career-BUILDER-Study> [<https://perma.cc/SH45-NUU6>]; Erica Swallow, *How Recruiters Use Social Networks to Screen Candidates*, MASHABLE (Oct. 23, 2011), <https://mashable.com/2011/10/23/how-recruiters-use-social-networks-to-screen-candidates-infographic> [<https://perma.cc/6HHK-2DCX>].

<sup>196</sup> Obscuring shaming may take time. Therefore, allowing the removal of links after a while equalizes between shamed individuals who use reputation management services and those who cannot afford these services.

## 2. A Right to Delist: Addressing the Objections

The first objection to the right to delist links is the expected chilling effect on free speech and infringement of the speakers' right to publish expressions without censorship. Delisting links will hinder the public's right to receive information. As a result, users will not have complete information on reputation of others and might be engaged in inefficient transactions that they could have avoided had they been given full disclosure.

The right to delist links to shaming posts may curb speech. Yet, if a limited right to delist were given, the chilling effect would be proportional and would lead to a just and efficient result, as the following Subsection will explain.

*First*, shaming may exclude the shamed individual or cause self-exclusion from conversations. By not extending the right to delist, the shamed individual's speech is curbed and the public discourse will no longer serve the purpose of democratic legitimation.<sup>197</sup> If the right to delist links was granted, free speech might be promoted because the balancing act between free speech and dignity must include the shamed individual's speech as well. This balance was adopted voluntarily by some content providers such as Facebook.<sup>198</sup> A right to be forgotten for shamed ordinary people is not different.

*Second*, delisting links to names of shamed individuals obscures access to the information, but does not delete it. The information remains on the website of origin and is not removed completely, yet it will not appear in the search results.<sup>199</sup> The content could be used for

---

<sup>197</sup> See Post, *supra* note 26, at 1009 (“[I]f the public discourse becomes sufficiently abusive and alienating persons are unlikely to experience it as a medium through which they might influence the construction of public opinion. In such circumstances, public discourse will no longer serve the purpose of democratic legitimation and hence the democratic justification of speech will pro tanto diminish.”). Thus, even the public interest in search results is not absolute and should be balanced against other interests. For a discussion of free speech on both sides, see Kessler & Pozen, *supra* note 84.

<sup>198</sup> See *Community Standards: Bullying and Harassment*, FACEBOOK, <https://www.facebook.com/communitystandards/bullying> [<https://perma.cc/S5NT-UT8P>] (last visited May 11, 2019) (Facebook will “remove content that’s meant to degrade or shame, including, for example, claims about someone’s sexual activity.”).

<sup>199</sup> A negative review that was published about a shamed individual will not appear as a result of a search query for his name; yet the public can still access all the reviews on this person



research purposes or data analyzing, and promote efficiency. The chilling effect on the speaker's speech is reduced; thus, in some cases, the chilling effect of such right is proportional.

*Third*, although data is considered speech,<sup>200</sup> the value of speech is not absolute. With time, data may express fewer elements of free speech. The information may be taken out of context and may lead the reader to wrong conclusions, as they are not fully aware of the age of the information, the circumstances of the publication, and factual developments that occurred afterwards.<sup>201</sup> Therefore, nuanced protection of speech should be promulgated. It should take into account the time that had passed from publishing the original expression to the present.<sup>202</sup>

The second objection to the right to be forgotten concerns the freedom of the press that is expressed in search engines' role as an archive that preserves collective memory and the integrity of structure of communication.<sup>203</sup> One can argue that by establishing the infrastructure that sustains a public sphere of this kind, Google serves the same essential democratic interests as does the traditional press because it allows a mass audience to acquire information responsive to their own interests. The right to be forgotten creates memory holes and narrows freedom of the press.<sup>204</sup>

However, freedom of the press is not absolute and should be balanced against the constitutional rights of the shamed individual.

---

when using the website. It may also appear in search results of other search queries. See BRUNTON & NISSENBAUM, *supra* note 108 (expanding on practices of obscuring information). This balance justifies the separation of the website and Google. For criticism of this separation, see Post, *supra* note 26.

<sup>200</sup> Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014) (explaining that even raw data is a speech when it promotes the creation of knowledge; as such, it can be protected by the First Amendment).

<sup>201</sup> For example, they might not be aware that charges against an individual were dropped at a later stage. See, e.g., *supra* note 166.

<sup>202</sup> See NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 82 (2015); JONES, *supra* note 79, at 147–63 (data might be considered speech, but the scope of the First Amendment in regards to protecting data is not absolute).

<sup>203</sup> See Antani, *supra* note 128, at 1205; Post, *supra* note 26, at 1015 (“[T]he public also has a fundamental interest in maintaining the integrity of the structure of communication that makes public discourse possible.”). Post argues that policymakers should refer to the public interest in search results in a similar way to the public interest of freedom of the press.

<sup>204</sup> See Post, *supra* note 26.

When the information is on ordinary people, there are more reasons to prefer their interests.<sup>205</sup> In addition, memory holes already exist on the internet even in the absence of the right to be forgotten.<sup>206</sup> Digital information is less stable than analog, and a long list of errors may prevent long-term access to digital content.<sup>207</sup> Older links often suffer from routing failures, preventing access to information.<sup>208</sup> Since the internet is not as permanent as it appears, the right to delist links from search results is not unheard of, and exists in the natural development of the web. Not extending the right to be forgotten results in extensive arbitrariness and inequality when some people are automatically delisted after a while and others cannot even request to delist.

Moreover, permanent memory of bad shaming perpetuates mistakes and falsehoods. In such cases, the right to be forgotten does

---

<sup>205</sup> See Klonick, *supra* note 26 (referring to a related context of content moderation and proposing that moderation should depend on context. When the intermediary focuses on harmful expressions directed at private people, the intermediary operates as a court and has to evaluate the expressions and prefer errors that remove expressions to errors that leave harmful expressions online. In contrast, when the intermediary moderates content on public figures, it operates as the press and should value the newsworthiness of the expressions. In these situations, the intermediary should prefer errors that leaves content online to errors that remove too much newsworthy content).

<sup>206</sup> See Antani, *supra* note 128, at 1207 (“[S]tudies on internet content persistence have shown that a significant amount of content disappears within a day”). For example, when scores of nude photos of celebrities were stolen from their personal databases and reposted on Reddit (a social media website), the members of Reddit’s community immediately pulled down some subpages that were linking to the images. See *id.* at 1205; Meg Leta Ambrose, *It’s About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten*, 16 STAN. TECH. L. REV. 369, 372 (2013).

<sup>207</sup> See JONES, *supra* note 79, at 105 (explaining that listing errors prevent access to information, such as media and hardware errors, software failures, communication channel errors, network service failures, component obsolescence, operator errors, natural disasters, internal and external attacks, and economic and organizational failures).

<sup>208</sup> See JONES, *supra* note 79, at 106–07 (referring to Wallace Koehler, *A Longitudinal Study of Web Pages Continued: A Consideration of Document Persistence*, 9 INFO. RES. 174 (2004)); Daniel Gonez & Mário J. Silva, *Modelling Information Persistence on the Web*, in PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON WEB ENGINEERING 193 (2006) (researchers reveal that 28% of content items on the internet are not accessible via the link in the search results in two years after the information was published); see also Jonathan Zittrain, Kendra Albert & Lawrence Lessig, *Perma: Scoping and Addressing the Problem of Link and Reference Rot in Legal Citations*, 14 LEGAL INFO. MGMT. 88 (2014) (researchers from Berkman Klein Center found that 50% of the links on the U.S. Supreme Court website do not lead to the content they originally referred to).

not result in serious memory holes. On the contrary, it reduces the damage of falsehood and misrepresentations, and will not infringe on freedom of the press disproportionately.

The third objection to the right to be forgotten concerns collateral censorship that occurs when a (private) intermediary suppresses the speech of others in order to avoid liability that otherwise might be imposed on him because of that speech.<sup>209</sup> This objection concerns the implementation of the right to delist by search engines and the over-censorship that this privatizing of bureaucracy might cause.<sup>210</sup>

Indeed, a chilling effect is a possible result of a right to delist, yet Google strives to encourage universal accessibility of content online as part of its business model and is not driven only by legal considerations.<sup>211</sup> As the implementation of the right to be forgotten in the European Union demonstrates, Google is very selective in delisting links and rejects about sixty percent of the requests.<sup>212</sup> Therefore, the concerns of collateral censorship and a chilling effect are overstated.

In addition, complementary measures can mitigate the concern of collateral censorship even more. Outlining clear guidelines for structuring the discretion of search engines can mitigate the problem. In

---

<sup>209</sup> See Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293 (2011); see also Balkin, *supra* note 42, at 1203 (“[T]he right to be forgotten is a classic example of collateral censorship. Instead of going after the speaker, the state targets the infrastructure provider, and it threatens to hold the search engine company liable if it does not delink embarrassing articles from newspapers. The government puts pressure on the infrastructure owner to muffle (but not completely silence) the voice of the original speaker.”).

<sup>210</sup> See Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011 (2018) (referring to the privatizing of bureaucracy as a result of the move from “old school regulation” between the state and the speaker, and the “new school” that involves a triangle of state-intermediary speaker).

<sup>211</sup> Even in the related context of intellectual property, Google objected in court to delist links from all the domains of a website, even though the order requested aimed to prevent selling infringing goods and did not aim to remove speech that engages freedom of expression, as the court ruled. “We have not, to date, accepted that freedom of expression requires the facilitation of the unlawful sale of goods.” See *Google LLC v. Equustek Solutions Inc.*, No. 5:17-cv-04207-EJD, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017). Google sued in the United States for “a declaratory judgment that the Canadian court’s order cannot be enforced in the United States.” The district court granted the order. See *id.*

<sup>212</sup> See Lee, *supra* note 146, at 1074. According to Google’s transparency report, within six months of the CJEU decision, Google received over 160,000 removal requests and denied a majority (approximately 58%) of them. See *id.* at 1021; see also Kelly & Satola, *supra* note 157.

addition, limiting the legal liability for not removing links to shaming expressions might also reduce the concern.<sup>213</sup> Furthermore, the mechanism of removal can be improved by imposing transparency and due process obligations on intermediaries.<sup>214</sup> Other improvements might be achieved by creating a mechanism for reconsidering complex decisions,<sup>215</sup> or even by creating a hybrid authority for removal that will be composed of industry and governmental representatives.<sup>216</sup> Yet, in itself, this objection should not undermine the idea for a right to be forgotten for the shamed ordinary people.

The fourth objection to the “right to be forgotten” argues that social norms develop over time and allow society to forgive the shamed individual. Indeed, social norms might mitigate the harm caused by shaming. Yet one might claim that in order to forgive, one must also forget.<sup>217</sup> Due to the negativity bias, negative information has a greater impact on the audience than does positive information; therefore, norms will not lead to total forgiveness.<sup>218</sup>

The fifth objection to the right to be forgotten posits that it may hinder the values of shaming: norm enforcement, deterrence, and efficiency. Indeed, an absolute right to be forgotten may undermine the benefits of shaming. But this right is not expected to hinder the benefits of shaming if we limit its scope by identifying its differential nuances. Applying a right to be forgotten for bad shaming will not hinder the benefits of shaming because bad shaming does not promote norm enforcement and efficient deterrence. In the other types of shaming,

---

<sup>213</sup> For example, policymakers can determine that, when bad shaming is *not* evident, the search engine does not remove the link immediately, and the shamed person files an action in court, the court can determine that the link should be removed but will not force the search engine to compensate the victim for not removing the link expeditiously upon a request to delist.

<sup>214</sup> See Balkin, *supra* note 210, at 41.

<sup>215</sup> In a related context, Kadri and Klonick discussed a suggestion to establish an independent diverse body that would make policy and appeal determinations on Facebook. See Kadri & Klonick, *supra* note 26 (manuscript at 38). On the plan to establish an oversight board on Facebook, its benefits and limitations, see Evelyn Douek, *Facebook's 'Oversight Board': Move Fast with Stable Infrastructure and Humility*, 21 N.C. J.L. TECH. (forthcoming 2019). A similar body can be established for search engines.

<sup>216</sup> See Lee, *supra* note 146, at 1086.

<sup>217</sup> See MAYER-SCHÖNBERGER, *supra* note 123, at 155.

<sup>218</sup> See Baumeister, *supra* note 24.

access to the information years after the discussion faded is not expected to significantly improve norm enforcement either. The shamed individual may have learned his lesson, yet people may continue to avoid efficient transactions with him. This may also result in over-deterrence and exclusion of the shamed individual from society, and hinder free speech.

This Article does not argue that law should adopt an absolute right to be forgotten. In many cases, it is efficient and just to postpone the right to delist, or to not allow delisting at all. Yet a dichotomous perspective that chooses between oblivion (as is the case in the European Union) and permanent memory (as is the case in the United States) is inappropriate. The law should allow nuances of digital oblivion in order to balance the interests and values.

## V. GUIDELINES FOR APPLYING THE RIGHT TO DELIST

This Part outlines a nuanced right to delist that differentiates between the types of shaming that were presented in Part II (good shaming, bad shaming, and shaming the ugly behavior). The suggested rules of thumb will be a proxy for the scope of remedy for digital dissemination that results in dignitary harm. They will instruct search engines and judicial tribunals to efficient decisions on delisting links to shaming information, lead to more certainty and efficiency, and properly balance dignitary rights and speech.<sup>219</sup> Yet, as the following Part will show, applying them by search engines and judicial tribunals allows flexibility in special circumstances.

### A. *Delisting Links to Good Shaming*

Shaming a defendant following a court recommendation usually fulfills the purpose of shaming. It promotes freedom of expression, norm enforcement, deterrence, and efficiency. The objections to shaming weaken when a judicial decision is the trigger for shaming.

---

<sup>219</sup> The analysis will focus on the dignitary aspects of the right to be forgotten and not on the instrumental ones. For differentiation, see Post, *supra* note 26.

Yet even this type of shaming raises the question of proportionality. Should shaming remain accessible even after the norm was enforced following the shaming? For example, this may happen when a court orders the shaming of a person for not obeying a judicial decision, and as a result, the person obeys. Or when shaming reports on a conviction exist even after expungement laws allow the deletion of the crime from official records.

Allowing shaming to continue years after the wrongful behavior ended might be unjust, inefficient, and lead to over-deterrence. It might also stand in contrast to principles of legal forgiveness and rehabilitation.<sup>220</sup> A nuanced right to delist from search results may mitigate these problems. Indeed, when the public has a right to access the information and this right outweighs the interests of the shamed individual, shaming should not be subjected to a right to delist.<sup>221</sup> This may be when a shamed individual committed serious crimes, including sexual offenses against a person's body.

Yet courts are well-versed in the facts, circumstances, and context of their cases and can determine—as part of rulings—the duration of shaming and when a defendant can request to delist a judicial decision that orders the public to shame him and the shaming expressions that follow. For example, a court may determine that an individual who had been shamed for not obeying a court order will have a right to delist the links to the shaming expressions after complying with the judicial decision. In addition, an individual should have a right to delist links to convictions whenever expungement laws allow deleting the information from public records. Thus, digital media will not thwart the purpose of expungement laws disproportionately.<sup>222</sup>

---

<sup>220</sup> See Antani, *supra* note 128, at 1196.

<sup>221</sup> *Id.* at 1197; see also Kydo, *Tokyo High Court Overturns Man's 'Right to Be Forgotten'*, JAPAN TIMES NEWS (July 13, 2016), <http://www.japantimes.co.jp/news/2016/07/13/national/crime-legal/tokyo-high-court-overturns-mans-right-forgotten/#.WGung1V97cs> [https://perma.cc/GB2R-MWMX] (the high court in Japan rejected a person's petition to delist from search results' links to reports about his arrest for involvement in child prostitution and pornography because child prostitution is a matter of grave concern and the public interest has not been lost even five years after the incident).

<sup>222</sup> See Antani, *supra* note 128, at 1197; Eric Posner, *We All Have the Right to Be Forgotten*, SLATE (May 14, 2014, 4:37 PM), [http://www.slate.com/articles/news\\_and\\_politics/view\\_from\\_chicago/2014/05/the\\_european\\_right\\_to\\_be\\_forgotten\\_is\\_just\\_what\\_the\\_internet\\_needs.html](http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html) [https://perma.cc/6TG3-NV99] (explaining that Google makes money out of private

The proposed limited right to delist would preserve the benefits of shaming and accommodate the problem of disproportionality in the digital age.

### B. *Delisting Links to Bad Shaming*

Bad shaming includes the dissemination of defamation and condemnations for something a person has not done, condemnations that are not protected by defamation law defenses, or the dissemination of information without legitimate cause in order to inflict harm. An example of this would be the shaming of a person only for his race, or spreading his intimate picture without consent. Bad shaming may also start as a legitimate condemnation, get out of control in the process of dissemination, and develop into defamatory speech, threats, cyberharassment, or cyberbullying directed deliberately at the shamed individual repeatedly.<sup>223</sup> In most cases, this type of shaming falls under a civil tort or crime.<sup>224</sup>

As explained above, when shaming includes defamation, racial speech, or nonconsensual dissemination of intimate photos, there are no benefits to the shaming content. From the moment shaming spins out of control, gets taken out of context, and evolves to defamation, cyberharassment, and cyberbullying, it ceases to promote the benefits of shaming. This results in inefficiency and infringes on the shamed individual's free speech by excluding him from society.<sup>225</sup> Limiting this type of shaming can be consistent with the First Amendment.<sup>226</sup> There is no public interest in allowing enhanced accessibility to this type of

---

information and therefore should ensure that historical embarrassing information, of little meaning to others, does not turn up at the top of search results).

<sup>223</sup> This may include publishing personal information on the shamed individual such as his phone number, encouraging the public to harass him and leading to calls of harassment.

<sup>224</sup> For example, this includes defamation, threatening, and unauthorized disclosure of sexually explicit images.

<sup>225</sup> See *supra* Section II.B.

<sup>226</sup> See Citron, *supra* note 84, at 218; Geoffrey R. Stone, *Privacy, the First Amendment and the Internet*, in *THE OFFENSIVE INTERNET*, *supra* note 20, at 174, 182; see also *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 245–46 (2002) (“The freedom of speech has its limits; it does not embrace certain categories of speech, including defamation, incitement, obscenity, and pornography produced with real children.”).

content. Therefore, the shamed individual should have an immediate right to request the removal of links to bad shaming. The search engine must remove links to bad shaming when it is evident that the shaming expressions are a tort or criminal offense. The search engine may remove the link when there is doubt regarding the speech, yet in such cases can wait for a court ruling and remove the link only after a court determined that the expressions constitute a tort or crime. The court will not impose compensation on the intermediary for not removing links to non-evident bad shaming expressions upon request before the court's decision.

It should be noted that the search engine does not have to initiate the removal of links to bad shaming results. Rather, the victim has to bear the burden of notifying the search engine of links to bad shaming. Thus, if other types of shaming developed into bad shaming in the process of dissemination and resulted in more shaming search results, it is the victims' responsibility to request to remove search results that link to them.

### C. *Delisting Links to Shaming of Ugly Behavior*

Shaming individuals for violating consensual norms by publishing their antisocial behavior and condemning it has many virtues that exceed its flaws.<sup>227</sup> Yet, by allowing easy access to these expressions long after the discussion has faded away and the goals of shaming were achieved, over-deterrence and chilling effects may occur.

The importance of the right to delist links in this context is reinforced in light of the availability of reputation management services that can obscure content.<sup>228</sup> As explained, these services can downgrade shaming from the top of search results. However, they are costly and may take time.<sup>229</sup> Not extending a right to delist links to the wider public

---

<sup>227</sup> See *supra* Section II.C (explaining that this type of shaming may condemn a violation of a nonconsensual norm).

<sup>228</sup> See *supra* Part III (explaining that the shamed individual can try to obscure the information by bombarding the internet with neutral information that is not related to the shaming, causing the page rank of the shaming search results to downgrade).

<sup>229</sup> See RONSON, *supra* note 9, at 263–74 (reputation management takes time).



increases social gaps between individuals who have resources to pay for these services and individuals who do not. Arguably, it also increases the gap between those who got to delist due to the natural instability of digital information and those who did not.<sup>230</sup> Thus, it infringes on equality.

In order to preserve the benefits of this type of shaming and to minimize its potential harm, a limited, delayed right to delist should be implemented. Accordingly, shaming the ugly behavior should be considered irrelevant a year after the information was first published.<sup>231</sup> Search engines will have the discretion to deviate from the default of removal in exceptional cases when there is a persisting public interest to keep the information listed on the search results. The public interest in keeping the information listed exists when removal requests refer to dissemination of reports on convictions of serious crimes against the individual's body, such as serious violence and sexual offenses, when the reports were published separately from the verdict.<sup>232</sup> In addition, when the shaming is due to claims for violent crimes against an individual's body, even if the person was not convicted of a crime, search engines should have discretion not to delist links to shaming the ugly behavior upon request after a year.<sup>233</sup> In such cases, they will be required to

---

<sup>230</sup> On the instability of digital information, see *supra* note 227.

<sup>231</sup> When a removal is requested, search engines and courts are expected to know the date of publication by the date on the website and metadata. For a discussion on metadata, see generally Paula Kift & Helen Nissenbaum, *Metadata in Context—An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program*, 13 I/S: J.L. & POL'Y 333, 336–38 (2017).

<sup>232</sup> It should be noted that the publication of the verdict itself and linking to it in search results is not shaming. In some jurisdictions, access to publication of a verdict can even be required by law, especially in criminal procedures because it promotes freedom of information and the public's right to know about the verdict. See generally Jeanne L. Nowaczewski, *The First Amendment Right of Access to Civil Trials After Globe Newspaper Co. v. Superior Court*, 51 U. CHI. L. REV. 286 (1984). Yet, the proposal refers to additional active dissemination of reports on the verdict. When the reports refer to serious crimes, there can be public interest in not de-indexing the links to the reports. In such cases, the search engines are not obligated to remove the link upon request after a year. On forgiveness and serious crimes, see Antani, *supra* note 128, at 1196 (“The right to be forgotten should not affect internet content chronicling certain serious crimes, including those involving sexual offenses and significant violent behavior, since the public has a strong right to access the information about this behavior.”).

<sup>233</sup> For example, consider a situation in which the shaming includes a video in which the shamed individual is seen violently beating another person, even if the case had not reached prosecution in court, or when the shaming includes claims to sexual offenses against the body, even without conviction. The search engine will have to reason the refusal to de-index, and the

reason their refusal to delist. The shamed individual can challenge the decision not to delist in court.<sup>234</sup> In such cases, a court can order the search engine to delist, but should avoid imposing compensation for failure to delist before the court decision.

Allowing a right to delist will not lead to deletion of the information, but instead will obscure it. The information will remain accessible on the website of origin and may appear in search queries that do not include the individual's name.

These guidelines are expected to preserve the benefits of shaming, mitigate the problem of disproportionality, and promote equality and distributive justice.

---

victim should have a right to appeal because the video might be taken out of context or may not reflect the truth. The shamed individual, whose shaming source had not been delisted, can apply to court, which may order the search engine to delist the source.

<sup>234</sup> In such cases, if the court determines that there is no public interest in allowing continuing access to the link and declines the reasoning of the search engine, the remedy of the victim will be limited to injunction of removal and will not include compensation from the search engine.

*Table 1. A Summary of the Guidelines for Removing Links to Different Types of Shaming:*

Type of Shaming	“Good Shaming”	“Bad Shaming”	“Shaming the Ugly Behavior”
Description	<ul style="list-style-type: none"> <li>• A court order, or a judicial recommendation to shame an individual.</li> <li>• An instruction to actively publish judicial decision that describes law violations on social networks.</li> </ul>	<ul style="list-style-type: none"> <li>•Publishing and disseminating information that reaches the threshold of a civil tort, or a criminal offence</li> <li>•Publishing defamation on an individual and condemning him for acts he did not commit,</li> <li>•Dissemination of information without legitimate cause in order to harm third parties. For example spreading intimate pictures of an individual without consent.</li> <li>•taking content out of context in the process of dissemination and turning it into defamation.</li> <li>•Dissemination that got out of control and turned into cyber-bullying or cyber harassment (shaming that turns into a criminal offence).</li> </ul>	<ul style="list-style-type: none"> <li>•Shaming individuals for violating norms by condemning the violation.</li> </ul>
Date of granting a request to delist from search results and obscuring the information.	<ul style="list-style-type: none"> <li>•Courts should determine when the defendant may request to be delisted from search results.</li> <li>•The shamed individual should have a right to delist when expungement laws allows the deletion from public records.</li> <li>•Courts can decline to allow a right to delist when the shamed individual committed serious crimes, involving significant violent behavior, since the public has a right to access the information</li> </ul>	<ul style="list-style-type: none"> <li>•An immediate right to delist defamation, racial speech and expressions that has no legitimate cause other than inflicting harm.</li> <li>•A right to delist from the moment a legitimate expression evolved into civil torts or criminal offences.</li> </ul>	<ul style="list-style-type: none"> <li>•A right to be delisted a year after the information was first published.</li> <li>•Search engines should have the discretion to deviate from the default setting in exceptional cases when there is a public interest to keep the search results.</li> <li>•Deviation will be subjected to judicial review.</li> </ul>

#### D. *The Benefits of Bright-Line Rules for Delisting Shaming Expressions*

The proposed rules aim to instruct search engines’ employees and courts. These rules are different from the guidelines of Article 29 Working Party in the European Union, which outline flexible criteria

for the right to delist.<sup>235</sup> Instead, they outline rules for applying the right to delist shaming expressions.

One can argue that applying the proposed rules will lead to less accuracy relative to flexible open standards. Yet, as the following Part will show, the proposed rules are superior to open ended standards. First, the decision to delist links is made by search engines' employees. They receive large volumes of requests.<sup>236</sup> Therefore, it is difficult to expect them to think deeply into every case and apply open standards efficiently.<sup>237</sup> The proposed rules are much simpler, and therefore may actually lead to more accuracy and consistency relative to open standards.

Second, open standards are vague. Due to the uncertainty of the exposure to liability, search engines may apply higher standards than intended in order to meet legal requirements.<sup>238</sup> In the context of the right to delist, open-ended standards may cause disproportionate chilling effects. In contrast, the proposed rules lead to clarity and are expected to reduce over-delisting.

---

<sup>235</sup> See Art. 29 Data Prot. Working Party, Guidelines, *supra* note 159. On differences between rules and standards, see William McGeeveran, *The Duty to Data Security*, 103 MINN. L. REV. 1134, 1197 (2019) (“[R]ules stipulate brighter lines while standards rely on more general criteria . . . rules already contain their principal substance before the occurrence of whatever activity they regulate, while adjudicators supply content to standards only after the fact.”).

<sup>236</sup> See Anupam Chander & Uyên P. Lê, *Free Speech*, 100 IOWA L. REV. 501, 504 (2015).

<sup>237</sup> Nick Hopkins, *Revealed: Facebook's Internal Rulebook on Sex, Terrorism and Violence*, GUARDIAN (May 21, 2017, 1:00 PM), <https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence> [https://perma.cc/LP44-SJKC] (noting that moderators are “overwhelmed by the volume of work, which means they often have ‘just 10 seconds’ to make a decision.”). For expansion on this subject, see TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET: PLATFORMS, CONTENT MODERATION, AND THE HIDDEN DECISIONS THAT SHAPE SOCIAL MEDIA 111 (2018); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1631–32 (2018) (explaining that a simple standard against something like gratuitous violence is able to reach a more tailored and precise measure of justice that reflects the norms of the community, but it is vague, capricious, fact dependent, and costly to enforce. Therefore, moderation is performed according to rules and not standards).

<sup>238</sup> See KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 242 (2015) (explaining that vagueness in regulatory standards leads companies to implement higher standards of regulation).

Third, as technology develops, enforcement of law shifts to automatic algorithms, AI, and machine learning.<sup>239</sup> Online intermediaries already use technologies to remove infringing content from their platforms automatically, and even to ensure such content would stay down in related contexts of copyright infringement,<sup>240</sup> inciting content,<sup>241</sup> and revenge porn.<sup>242</sup> Currently, algorithmic enforcement is not sensitive enough to context of words in text-based expressions, and thus, at this stage, automatic algorithmic enforcement may result in over-removal.<sup>243</sup> But technologies develop and improve. Rules are expected to allow implementing the right to delist shaming expressions into technology when it develops and becomes more sensitive to context.<sup>244</sup> This shift may allow every private person to file a

---

<sup>239</sup> For discussion in a related context, see Niva Elkin-Koren, *Fair Use by Design*, 64 UCLA L. REV. 1082, 1097 (2017).

<sup>240</sup> See Maayan Perel & Niva Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, 19 STAN. TECH. L. REV. 473, 485, 487 (2016) (reviewing this practice and criticizing it by alerting the problem of algorithmic compliance with the rule of law: “algorithms cannot process reliable decisions about copyright infringement and fair use”); Martin Husovec, *The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which Is Superior? And Why?*, 42 COLUM. J.L. & ARTS 53, 67 (2018) (“The capabilities of automation are dependent on the state of technological development, such as of artificial intelligence.”).

<sup>241</sup> See Susan Klein & Crystal Flinn, *Social Media Compliance Programs and the War Against Terrorism*, 8 HARV. NAT’L SEC. J. 53, 79–81 (2017).

<sup>242</sup> See Olivia Solon, *Facebook Asks Users for Nude Photos in Project to Combat ‘Revenge Porn’*, GUARDIAN (Nov. 7, 2017, 5:15 PM), <https://www.theguardian.com/technology/2017/nov/07/facebook-revenge-porn-nude-photos> [<https://perma.cc/53PC-A79T>].

<sup>243</sup> See Natasha Duarte, Emma Llansó & Anna Loup, *Mixed Messages? The Limits of Automated Social Media Content Analysis* 1, 3 (Ctr. for Democracy & Tech. Paper, 2017), <https://cdt.org/files/2017/12/FAT-conference-draft-2018.pdf> [<https://perma.cc/N6EZ-23ZT>] (“Today’s tools for analyzing social media text have limited ability to parse the meaning of human communication or detect the intent of the speaker.”); Danielle Keats Citron & Neil M. Richards, *Four Principles for Digital Expression (You Won’t Believe #3!)*, 95 WASH. U. L. REV. 1353, 1362 (2018); GILLESPIE, *supra* note 237, at 98.

<sup>244</sup> Pasquale believes in a complementary approach of law and machine. See Frank Pasquale, *A Rule of Persons, Not Machines: The Limits of Legal Automation*, 87 GEO. WASH. L. REV. 1 (2019) (“[T]he more formalized law becomes, the easier it is to convert its rules to the types of expert systems deployed in a program . . .”). Arguably, there are types of decisions in which looser standards can be superior to rules; yet, in the case of the right to delist, the decision concerns present classification and not the future. Therefore, rules are likely to outperform standards. See Saul Levmore & Frank Fagan, *The Impact of Artificial Intelligence on Rules, Standards, and Judicial Discretion*, 93 S. CALIF. L. REV. (forthcoming 2019).

request to delist links by using an automatic system that will delist shaming links according to the proposed rules. They will allow the coding of good shaming into technology and the avoidance of responding to requests to remove shaming before the date of delisting in a court's judicial decision to shame. In addition, coding rules into technology will allow for the automatic delisting links to bad shaming.<sup>245</sup>

Fourth, bright-line rules will allow avoiding cumbersome litigation, better court instructions, and promote more consistent and fair decisions on the right to delist.

### E. *The Proposed Rules and Law*

#### 1. Section 230 of the CDA

The proposed rules outline a nuanced right to be delisted from links for ordinary people. It offers a nuanced balance between free speech and the right to privacy, depending on the type of shaming. However, the current law provides immunity for intermediaries.<sup>246</sup> Therefore, in general, search engines are not legally obligated to delist links to content from search results.

This absolute immunity scheme was constructed when the internet was in its infancy. As the internet matures, this regime should be refined.<sup>247</sup> This is a crucial juncture where change in the current legal infrastructure is needed.<sup>248</sup> Such a change will likely call for amending the relevant law, such as section 230 of the CDA, and allow for the

---

<sup>245</sup> Intermediaries are already using technologies to automatically remove some types of bad shaming. See generally *infra* Section V.F.2.

<sup>246</sup> See 47 U.S.C. § 230 (2018).

<sup>247</sup> See Olivier Sylvain, *Intermediary Design Duties*, 50 CONN. L. REV. 203 (2018) (suggesting a narrow interpretation of the immunity by courts. Accordingly, because intermediaries structure, sort, and sometimes sell users' data, they are not passive conduits, courts should rethink the scope of immunity in a way that is adapted to the oversized influence that online intermediaries have on users' conduct today and be attentive to intermediaries' design).

<sup>248</sup> Citron, *supra* note 79, at 66 ("We find ourselves at a very different moment now than we were in five or ten years ago, let alone twenty years ago when Section 230 was passed. The pressing question now is not whether the safe harbor will be altered, but to what extent.").

creation of a legal obligation to delist links to shaming in search results.<sup>249</sup>

The proposed guidelines are not likely to cause a legal revolution because lawsuits filed today against intermediaries often continue beyond preliminary stages of trial.<sup>250</sup> For example, there are plaintiffs who bypass section 230 of the CDA by raising direct and contributory claims that exceed a trivial secondary liability framework.<sup>251</sup> Many

---

<sup>249</sup> See Posner, *supra* note 222 (the problem of old embarrassments staying with a person forever online has not yet been dealt with in American law. It is a problem that is actually worse for people who are not public figures—those who are supposed to receive greater privacy protections from the law. Posner suggests that new laws and rulings should give people back their privacy, which technology has taken away).

<sup>250</sup> Today, more than a third of the claims already circumvent a section 230 defense. See David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 493 (2010); Jeff Kosseff, *The Gradual Erosion of the Law That Shaped the Internet: Section 230's Evolution over Two Decades*, 18 COLUM. SCI. & TECH. L. REV. 1 (2016); see also Eric Goldman, *Ten Worst Section 230 Rulings of 2016 (Plus the Five Best)*, TECH. & MARKETING L. BLOG (Jan. 4, 2017), <http://blog.ericgoldman.org/archives/2017/01/ten-worst-section-230-rulings-of-2016-plus-the-five-best.htm> [https://perma.cc/LJK9-FGMD]; Michal Lavi, *Evil Nudges*, 21 VAND. J. ENT. & TECH. L. 1, 84 (2018).

<sup>251</sup> For instance, plaintiffs might bring contractual claims, failure-to-warn claims, and even fraud claims. See *Doe v. Internet Brands, Inc.*, 767 F.3d 894, 895 (9th Cir. 2014), *reh'g granted, opinion withdrawn*, 778 F.3d 1095 (9th Cir. 2015); *Beckman v. Match.com*, 668 F. App'x 759 (9th Cir. 2016) (basing their claim on negligence theory); *Moore v. Angie's List, Inc.*, 118 F. Supp. 3d 802, 807 (E.D. Pa. 2015) (basing their claim on fraud); *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1109 (9th Cir. 2009) (basing her claim on a contractual claim). In addition, some lawsuits on intermediaries' liability for speech-related torts are not barred in preliminary stages in light of courts' interpretation of the terms "creation" and "development" of information in section 230 of the CDA. Thus, intermediaries are already exposed to liability when a plaintiff files claims based on direct or contributory liability theories. These claims exceed this discussion and focus on secondary liability. Immunity is therefore broad, but not hermetic. See *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 489 F.3d 921, 932 (9th Cir. 2007), *rev'd en banc*, 521 F.3d 1157 (9th Cir. 2008) (concluding that the content provider "developed" content by designing discriminatory drop-down menus); *Daniel v. Armslist, LLC*, 913 N.W.2d 211, 215 (Wis. Ct. App. 2018 (immunity was not applied to a design of a gun sales platform), *rev'd*, *Daniel v. Armslist, LLC*, 926 N.W.2d 710 (Wis. 2019) (the Supreme court of Wisconsin reversed the decision, upheld section 230 and ruled in favor of the defendant). *Harrington v. Airbnb, Inc.*, 348 F. Supp. 3d 1085 (D. Or. 2018); see also *Huon v. Denton*, 841 F.3d 733, 736–37 (7th Cir. 2016) (basing the claim on direct liability of the intermediary and its workers and alleging that they wrote the defaming expressions). See generally *Jones v. Dirty World Entm't Recordings, LLC*, 965 F. Supp. 2d 818 (E.D. Ky. 2013), *rev'd and vacated*, 755 F.3d 398 (6th Cir. 2014) (even though the content provider was ultimately exempt from liability, the litigation was extensive and passed through a number of courts).

courts accept these claims and do not dismiss the suit. Clearly, immunity has eroded over time.<sup>252</sup> In addition, legislators are already striving to exclude certain claims from immunity.<sup>253</sup> If narrowing section 230 will not be achieved by interpretation, a legislative change can be promulgated<sup>254</sup> and accommodate cases of a failure to de-index links to types of shaming in specific circumstances upon notice.

The proposed framework recognizes a nuanced limited right to be delisted. It does not grant individuals a right to delist from search results as they see fit. Instead, it sets forth differential guidelines for

---

<sup>252</sup> See Kosseff, *supra* note 250.

<sup>253</sup> See, e.g., Stop Enabling Sex Traffickers Act, S. 1693, 115th Cong. (2017) (developed into the Allow States and Victims to Fight Online Sex Trafficking Act) (the bill aimed to undercut section 230 protections for preventing sex trafficking; accordingly, intermediaries would be held liable if a minor is trafficked on their sites); see also Daren Zhang, *Senate Introduces Stop Enabling Sex Traffickers Act*, JOLT DIGEST (Oct. 7, 2017), <http://jolt.law.harvard.edu/digest/senate-introduces-stop-enabling-sex-traffickers-act> [<https://perma.cc/725Z-9ADY>]; Citron & Wittes, *supra* note 173, at 409. For criticism, see Eric Goldman, *Manager's Amendment for SESA Slightly Improves a Still-Terrible Bill*, TECH. & MARKETING L. BLOG (Nov. 6, 2017), <http://blog.ericgoldman.org/archives/2017/11/managers-amendment-for-sesta-slightly-improves-a-still-terrible-bill.htm> [<https://perma.cc/7XH5-49DP>]. Recently, Congress passed Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018) (codified as amended at 18 U.S.C. §§ 1591, 1595, 2421A and 47 U.S.C. § 230). See Zeynep Ulku Kahveci, *Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA): Senate Passes Bill Making Online Platforms Liable for Third-Party Content Enabling Illegal Sex-Trafficking*, JOLT DIGEST (Apr. 4, 2018), <https://jolt.law.harvard.edu/digest/allow-states-and-victims-to-fight-online-sex-trafficking-act-fosta-senate-passes-bill-making-online-platforms-liable-for-third-party-content-enabling-illegal-sex-trafficking> [<https://perma.cc/N469-76LE>]; Eric Goldman, *'Worst of Both Worlds' FOSTA Signed into Law, Completing Section 230's Evisceration*, TECH. & MARKETING L. BLOG (Apr. 11, 2018), <https://blog.ericgoldman.org/archives/2018/04/worst-of-both-worlds-fosta-signed-into-law-completing-section-230s-evisceration.htm> [<https://perma.cc/3BSR-PHJN>]; Eric Goldman, *The Complicated Story of FOSTA and Section 230*, 17 FIRST AMEND. L. REV. 279 (2018); see also Mary Graw Leary, *The Indecency and Injustice of Section 230 of the Communications Decency Act*, 41 HARV. J.L. & PUB. POL'Y 553 (2018). Courts are already denying motions to dismiss. See, e.g., *Florida Abolitionist v. Backpage.com LLC*, No. 6:17-cv-218-Orl-28TBS, 2018 WL 1587477 (M.D. Fla. Mar. 31, 2018).

<sup>254</sup> See Citron & Wittes, *supra* note 173, at 415 (explaining that the CDA's immunity provision should be available to operators only when they behave reasonably to stop illegal activity. The consequence of that failure will not impose automatic liability, but rather remove the absolute shield from liability. A sustained failure to remove harmful content despite notifications should strip intermediaries' immunity at least in cases of failure to delist links to bad shaming); Ari Ezra Waldman, *Safe Social Spaces*, WASH. U. L. REV. (forthcoming 2019) (manuscript at 49), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3278719](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278719).



determining when content is inadequate or no longer relevant. It differentiates between different types of shaming and balances all the relative interests in the case. This balance preserves the benefits of shaming, and it mitigates a disproportionate chilling effect on speech while protecting the public's right to receive information. Applying the proposed guidelines will also mitigate the problem of disproportionate infringement on the shamed individual's constitutional rights.<sup>255</sup>

## 2. The Proposed Rules and Substantive Law

The proposal in this Article recognizes nuances of shaming. It outlines a differential remedy for dignitary harm even in cases of lawful dissemination of expression that causes dignitary harm. How should this framework be anchored in substantive law after a case of failure to de-index links to shaming progressed beyond preliminary stages? What is the proper doctrinal basis for the proposed remedy of a nuanced right to be forgotten?

This Section argues that the normative legal basis for the remedy is defamation law, even when the original publication enjoys defamation law's absolute privilege of truth.<sup>256</sup> The justification for applying the defamation law framework is that even a true story at the time of publication can turn into and be classified as defamation later.<sup>257</sup> Not delisting links to information about ordinary people and leaving it in the search results years after the information was published takes the data subject out of her current context and, in fact, defames her. Therefore, although the original publication enjoys defamation law defenses,

---

<sup>255</sup> See Antani, *supra* note 128, at 1210 (arguing that the right to be forgotten should be tailored to narrow contexts such as where analogs already exist—for example, the Fair Credit Reporting Act sets rules for preventing credit reporting agencies from including stale and obsolete information in someone's credit report; cyberbullying content; or nonconsensual revenge porn). Narrowly tailored rules may not violate the First Amendment. See JONES, *supra* note 79, at 164 (“Even in the U.S., there are ways to make the Digital Age a forgiving era, but the ways must be within the bounds of what makes Americans the most free.”).

<sup>256</sup> RESTATEMENT (SECOND) OF TORTS § 581A cmt. f (AM. LAW INST. 1977); W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 116 (5th ed. 1984); *Maheu v. Hughes Tool Co.*, 569 F.2d 459, 459–65 (9th Cir. 1977); *Browne-Barbour*, *supra* note 169, at 1515.

<sup>257</sup> See JONES, *supra* note 79, at 149. For expansion of taking out of context at defamation, see Lavi, *supra* note 40, at 193.

knowingly leaving the link to the publication is not privileged. When time passes, the context changes and the information does not reflect the absolute truth anymore.<sup>258</sup>

Since even true expressions can become defamatory when taken out of context,<sup>259</sup> the remedy of de-indexing should be based on defamation law. Yet, unlike other jurisdictions,<sup>260</sup> existing tort law does not provide a remedy for individuals who are being harmed by truthful but misleading information such as a mistaken arrest.<sup>261</sup> U.S. law does not impose legal obligations to update reports,<sup>262</sup> and courts analyze liability in a tort at the time of publication.<sup>263</sup> In addition, the general rule in U.S. courts is that injunctive relief relating to libelous statements is unavailable.<sup>264</sup>

Yet laws governing liability for defamation evolved long before the digital age.<sup>265</sup> As technologies advance, the internet becomes more prevalent, and connects and remembers almost everything. Shaming can easily be taken out of the context of its original time. Consequently, search results that represent the shamed individual falsely and misleadingly can lead to substantial harm. Therefore, it is time to address the context of time in shaming search results by allowing remedies in U.S. defamation law. This can be done by outlining a new relief in defamation law that will allow update-by-delisting.<sup>266</sup>

---

<sup>258</sup> See Lavi, *supra* note 40, at 193 (demonstrating the out of context principle in republication, which is applicable to the context of time).

<sup>259</sup> *Id.*

<sup>260</sup> See, e.g., Vincent R. Johnson, *Comparative Defamation Law: England and the United States*, 24 U. MIAMI INT'L & COMP. L. REV. 1, 72–81 (2016) (discussing Defamation Act 1996, c. 31, § 8, § 9 (U.K.); and Defamation Act 2013, c. 26, § 13 (U.K.)); see also Defamation Law, 5725–1965, 19 LSI 254 (1964–65) (Isr.) (defamation law in Israel).

<sup>261</sup> Cook, *supra* note 195, at 15.

<sup>262</sup> *Id.* at 2 (“The newspapers have no legal obligation to update their reporting or to allow you to set the record straight.”); see *Martin v. Hearst Corp.*, 777 F.3d 546, 553 (2d Cir. 2015).

<sup>263</sup> Cook, *supra* note 195, at 16 & n.89 (citing *Tomblin v. WHCS-TV8*, 434 F. App'x 205, 211 (4th Cir. 2011); *Stepanov v. Dow Jones & Co.*, 987 N.Y.S.2d 37, 42 (App. Div. 2014)).

<sup>264</sup> Johnson, *supra* note 260, at 77.

<sup>265</sup> *Id.* at 55.

<sup>266</sup> In some jurisdictions, a person who was accused of a criminal offense but the charges against him were dropped can request traditional media that reported on his criminal charges to update the public regarding the drop of charges. See, e.g., Defamation Act 1996, § 25A (Isr.). In contrast, in the United States, traditional media and online outlets have no legal obligation to update their reporting. See Cook, *supra* note 195, at 2. Yet, due to the ability to find

Accordingly, a court may order a search engine to delist links to shaming content that developed into defamation even if defamation law defenses protect the original publisher at the time of publication. Yet, if the original publication is protected by defamation law defenses, the obligation to delist will apply a year after the publication, at the earliest.<sup>267</sup>

It should be noted that when defamation law defenses protect the original publisher, but the expression developed into defamation in the context of time, the shamed individual will not be entitled to remedies of compensation from the publisher or the search engine. The only remedy is update-by-delisting from search results, except in rare cases when search engines avoid delisting upon notice without reasonable justification. A relief of update-by-delisting focuses on the shaming expression, not on the publisher, and will allow a remedy from the search engine that permits the continuation of the shame. This relief of update will promote the fulfillment of defamation law's goals.

While the E.U. right to be forgotten<sup>268</sup> and the proposed relief of delisting links to shaming partly overlap, the scope of their application is different. The E.U. right focuses on data protection and dignitary privacy in personal information.<sup>269</sup> In contrast, the proposed relief of delisting focuses on mitigation of reputational harm caused by information that the public can perceive as misleading or defamatory.<sup>270</sup>

---

information via search engines easily, it is time to adopt a right to delist information when a change in circumstances justify it. A right to delist is superior to a right to request an update or correction, which may have an adverse effect. *See* SUNSTEIN, *supra* note 21, at 25–26.

<sup>267</sup> The new relief of update can be articulated broadly within defamation law and apply to all information that turned into defamation, not only to ordinary people. Courts can consider the identity of the shamed individual, the character of the publication, the time passed from the first publication, and the damage to the plaintiff in not delisting the link, against the infringement of the public's interest by delisting the link. Courts will apply the relief on a case-by-case basis for shaming expressions that search engines refused to delist.

<sup>268</sup> *See supra* Section IV.C.1.

<sup>269</sup> *See* Post, *supra* note 26 (demonstrating that the decision in *Google Spain* mixes the rationale of data protection and dignitary privacy).

<sup>270</sup> Thus, for example, under the E.U. right to be forgotten, one who does not feel comfortable seeing a post published by him appear in search results can claim that the post is irrelevant and request to delist, even if there is nothing negative in the post. In contrast, under the proposed right to relief, that post will not be removed because the rationale is mitigating dignitary reputational harm.

## F. *The Scope of the Right to Be Forgotten*

### 1. Should Delisting Be Local or Global?

There are major legal battles in courts on the scope of the right to delist links from search results regarding the right to be forgotten<sup>271</sup> and in related contexts.<sup>272</sup> Plaintiffs file lawsuits in order to obtain injunctions for worldwide delisting links from search results, and do not settle with local delisting. How should courts apply the right to delist links to shaming information? This Article proposes to limit delisting shaming to the local domain.

Traditionally, shaming aims to condemn a violation of norm in a given society. What is considered a violation in a given territory can be appropriate in another society.<sup>273</sup> In addition, a global right to delist is overbroad because it enforces extraterritorial values on other societies where everyone has different values and different balances between fundamental rights.<sup>274</sup> The more the internet becomes embedded in our

---

<sup>271</sup> See, e.g., *supra* note 160 and accompanying text; see also Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 342–43 (2018); Miquel Peguera, *Right to Be Forgotten and Global Delisting: Some News from Spain*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y (Dec. 17, 2017, 4:37 AM), <http://cyberlaw.stanford.edu/blog/2017/12/right-be-forgotten-and-global-delisting-some-news-spain> [<https://perma.cc/WD7T-8CGL>]. It should be noted that a preliminary opinion of the ECJ found that the right to be forgotten should be enforced locally. See *supra* note 160.

<sup>272</sup> See, e.g., *Google Inc. v. Equustek Solutions, Inc.*, [2017] 1 S.C.R. 824 (Can.) (granting an injunction ordering Google to globally delist links to websites that contained pages selling a product that infringed on intellectual property rights); see Woods, *supra* note 271, at 343–44.

<sup>273</sup> See Woods, *supra* note 271, at 405–06 (“What is appropriate in New York may not be appropriate in Bangkok and vice versa. This trend is only likely to continue as the physical and digital worlds merge . . .”). For example, serving a dessert in a shoe can be seen as artwork in the Israeli eye, however, but serving such dessert to a Japanese person will likely offend him. See Stuart Winer, *Japan PM Said Offended by Dessert Served in Shoe at Netanyahu Home*, TIMES ISR. (May 7, 2018, 12:26 PM), <https://www.timesofisrael.com/japan-pm-said-offended-by-dessert-served-in-shoe-at-netanyahu-home> [<https://perma.cc/ZG2C-LEC2>].

<sup>274</sup> See Balkin, *supra* note 210, at 2027; Woods, *supra* note 271, at 359 (“[C]ompeting claims of sovereign authority over the internet will be an enduring feature of internet lawsuits. Ultimately, this means that courts will have to adapt sovereign-deference doctrines to the internet.”); see also Kristen Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. (forthcoming 2019) (manuscript at 43–44), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3205368](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205368) (“[C]ompanies might fight government orders, especially when purportedly local law infringes on the rights of users outside the ordering country.”).

everyday lives and the more it is constituted by data that reflects our real-world experiences, the more likely it is that the internet will need to reflect the very real differences in those experiences. Professor Woods correctly explains that the internet governance question is not whether the internet should be a global internet or splinternet; rather, the key question is how the internet will bend to accommodate sovereign differences in a sensible, mutually agreeable manner.<sup>275</sup>

Moreover, even if a global right to delist is possible, it is undesirable. A global right to delist leads to disproportionate censorship and threatens the global public good of the internet and the market of ideas.<sup>276</sup> Geo-local delisting embraces sovereign differences.<sup>277</sup> It only obscures the information, and therefore balances constitutional rights properly and does not infringe on the public good of the internet.<sup>278</sup>

Indeed, at this point, one can argue that limiting delisting to the local domain may infringe on the rights of the “global person” who operates in several countries. Thus, it creates a gap between the scope of protection for the global person and the “local person” who operates in a single domain. This gap may result in inequality. The global person can turn to the search engine in every state in which he operates; however, filing a request to delist in several countries may be burdensome and the inequality remains. But every rule should be evaluated against the alternatives. A global removal will lead to a “race to the bottom” and global over-delisting. As a result, the internet will eventually be governed by the most censorious regime.<sup>279</sup> This will disproportionately undermine beneficial information flows and the global public good of a free internet. Limiting the right to delist to the local domain is only obscuring it, thus leading to a better balance between fundamental rights.

Another reason for limiting delisting is practicality. Limiting the right to delist to the local domain increases the likelihood of search engines complying with requests to delist and court injunctions. As

---

<sup>275</sup> See Woods, *supra* note 271, at 406.

<sup>276</sup> See Balkin, *supra* note 42, at 1203–06.

<sup>277</sup> On embracing sovereign differences, see Woods, *supra* note 271, at 366–69.

<sup>278</sup> On the difference between deleting information and obscuring it, see Brunton & Nissenbaum, *supra* note 199, at 46–47; and Post, *supra* note 26, at 1066 n.362 (local delisting is another form of obscuring information).

<sup>279</sup> See Balkin, *supra* note 42, at 1205–07.

demonstrated in practice repeatedly, intermediaries are less likely to obey extraterritorial global requests to delist or to remove information. They even file suits to block the enforcement of global injunctions and are granted injunctive relief.<sup>280</sup> Fragmentation of the internet is already here.<sup>281</sup> Thus, pragmatic considerations also advocate for limiting delisting to the local domain of the search.

## 2. The Challenge of Bad Shaming, Fake Stories, and the Like

This Article argues that shaming is not monolithic. Therefore, a dichotomous perspective that chooses between oblivion and permanent memory is inappropriate. The Article outlined differential guidelines for delisting links to shaming. These guidelines depend on the type of shaming and the public interest in gaining access to the information. Applying these guidelines will preserve the benefits of shaming and allow reversibility to most ordinary people who have been shamed.

A right to delist links obscures shaming. Yet the information remains on the website of origin. In many cases, platforms include internal tools for searching specific content on the website. Information that was published on a central platform may be traced by using an internal search engine. A person seeking shaming information might find it easily by searching in several central online social networks.<sup>282</sup> In some cases, users can tag the shaming information with the individual's name by using hashtags (#) and make it easier to find, even though it is

---

<sup>280</sup> See, e.g., *Google LLC v. Equustek Solutions Inc.*, No. 5:17-cv-04207-EJD, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017) (granting preliminary injunctive relief in context of intellectual property rights). The Supreme Court of British Columbia dismissed Google's motion to set aside the global injunction against it that had been affirmed by the Supreme Court of Canada. See *Equustek Solutions Inc. v. Jack*, 2018 BCSC 610 (Can.) (holding that Google was not able to show that the global delisting order made against it violated its First Amendment rights in the United States); see also *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 379 F.3d 1120 (9th Cir. 2004) (declining to enforce the order mandating global removal of Nazi material); *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001) (declaring that the First Amendment precludes enforcement of a French order in the United States intended to regulate internet speech).

<sup>281</sup> See Woods, *supra* note 271, at 338–39.

<sup>282</sup> For example, by the internal search engine in Twitter that allows to seek people and content.

less accessible than information that could be found by using Google.<sup>283</sup> Obscuring good shaming and shaming of ugly behavior without deleting the information altogether leaves true and legitimate statements on the internet and avoids a disproportionate chilling effect on free speech. This limited right to be forgotten may lead to an appropriate balance between the fundamental rights of shamed individuals and the public.

Yet this conclusion is not true for bad shaming, especially when it contains defamation and falsehoods. These expressions are more common today than ever before<sup>284</sup> and may cause extensive harm. As recent research demonstrates, people may continue to believe in a falsehood even if it is rebutted.<sup>285</sup> Today, truth is no longer as important as appearing to be true. In this environment, combating bad shaming is of particular importance. Moreover, other research reveals that

---

<sup>283</sup> A hashtag is a short statement that categorizes a post and allows it to be found easily. See *How to Use Hashtags*, HELP CTR: TWITTER, <https://help.twitter.com/en/using-twitter/how-to-use-hashtags> [<https://perma.cc/GQ44-95XG>] (last visited Apr. 1, 2019); SUNSTEIN, *supra* note 39, at 4; TUFEKCI, *supra* note 84, at 129 (explaining how hashtags allow people to find information and gather around specific topics of discussion). See also XIAO MINA, *supra* note 13 at 55 (explaining that algorithms behind Twitter's trending catch hashtags and highlight the content hashtagged in a section on the site that is visible to many, which in turn drives this content even more attention).

<sup>284</sup> For example, consider the negative fake stories on Hillary Clinton and positive fake stories on Donald Trump that spread like wildfire; some believe these stories influenced 2016 election results. See YOCHAI BENKLER, ROBERT FARIS & HAL ROBERTS, NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 85 (2018); Zeynep Tufekci, *Mark Zuckerberg Is in Denial*, N.Y. TIMES (Nov. 15, 2016), <https://www.nytimes.com/2016/11/15/opinion/mark-zuckerberg-is-in-denial.html> [<https://perma.cc/6SDL-RGTC>]. In this case, the stories were spread about public figures, but fake stories can also spread about ordinary people. See TUFEKCI, *supra* note 84, at 264–65.

<sup>285</sup> Research shows that trying to rebut a falsehood exacerbates its prominence and the weight ascribed to it. See Pennycook et al., *supra* note 21. Other researchers have found that misinformation on climate change can psychologically cancel out the influence of accurate statements. They suggest adding a small dose of misinformation to the fact in order to cancel the distortion misinformation. This “inoculation” might help shift and hold opinions closer to the truth. See Sander van der Linden et al., *Inoculating the Public Against Misinformation About Climate Change*, 1 GLOBAL CHALLENGES 1 (2017). Yet, it seems that this tactic can backfire because one cannot know what dosage of misinformation “inoculates” the public. In addition, adding more misinformation to news may expose more people to fake news and pollute the flow of information. For a related context, see Richards & Hartzog, *supra* note 115, at 1186 (criticizing obfuscation for the same reasons).

falsehoods are diffused significantly farther, faster, deeper, and more broadly than the truth.<sup>286</sup>

In many countries in Europe, teams of communications experts are trying to debunk bogus news items on social networks and publish daily reports on fake news.<sup>287</sup> However, these efforts are more likely to focus on shaming of public figures and not ordinary people. Further, adding more information to online websites may be inefficient because rumors spread on the internet to a wide audience regardless of these efforts.<sup>288</sup> This strategy can even backfire because it exposes more people to debunked rumors, who may believe the rumor and not the correction.<sup>289</sup> Automatically screening websites for bad shaming and removing links are likely to cause over-censorship because this strategy may not take into account the context of the speech and may result in the removal of legitimate content.<sup>290</sup> Therefore, other solutions are required.

---

<sup>286</sup> See Soroush Vosoughi et al., *The Spread of True and False News Online*, 359 SCI. 1146 (2018).

<sup>287</sup> See Mark Scott & Melissa Eddy, *Europe Combats a New Foe of Political Stability: Fake News*, N.Y. TIMES (Feb. 20, 2017), [https://www.nytimes.com/2017/02/20/world/europe/europe-combats-a-new-foe-of-political-stability-fake-news.html?\\_r=1](https://www.nytimes.com/2017/02/20/world/europe/europe-combats-a-new-foe-of-political-stability-fake-news.html?_r=1) [<https://perma.cc/W2YP-FT2P>] (describing examples, focusing on a Brussels team known as East Stratcom that serves as Europe's front line against fake news. The team tries to debunk bogus items in real time on Facebook and Twitter, and publishes daily reports and a weekly newsletter on fake stories to its more than 12,000 followers on social media); see also NORMAN VASU ET AL., FAKE NEWS: NATIONAL SECURITY IN THE POST-TRUTH ERA 18–20 (2018), [https://www.rsis.edu.sg/wp-content/uploads/2018/01/PR180313\\_Fake-News\\_WEB.pdf](https://www.rsis.edu.sg/wp-content/uploads/2018/01/PR180313_Fake-News_WEB.pdf) [<https://perma.cc/8XP6-LKKN>]. Additionally, see recommendations for developing a media literacy strategy and an online safety News Guard in the United Kingdom regarding Fake News. HM GOV'T, ONLINE HARMS WHITE PAPER 90–91 (2019) (box 37 and 39), [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/793360/Online\\_Harms\\_White\\_Paper.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf) [<https://perma.cc/Q8JG-7NNK>].

<sup>288</sup> See Mark Scott, *supra* note 287 (“[C]atching every fake news story would be nearly impossible, and the fake reports the team does combat routinely get a lot more viewers than its myth-busting efforts. Despite the region wide push to counter false reports, experts question whether such fact-checking efforts by governments and publishers will have a meaningful effect.”).

<sup>289</sup> See SUNSTEIN, *supra* note 106 (arguing that sometimes it is better to leave an expression un rebutted); see also Pennycook et al., *supra* note 21; BENKLER ET AL., *supra* note 284, at 377.

<sup>290</sup> See Gillespie, *supra* note 237, at 98–106. In a related context of using algorithms for enforcing copyright infringement, see Perel & Elkin-Koren, *supra* note 240 (explaining the growing use of algorithms by online intermediaries and the challenges of such enforcement); Benjamin Boroughf, *The Next Great YouTube: Improving Content ID to Foster Creativity, Cooperation, and Fair Compensation*, 25 ALB. L.J. SCI. & TECH. 95, 107–08 (2015) (describing



From a normative perspective, it is high time to refine the immunity regime given to intermediaries in section 230 and adopt a notice-and-takedown regime for online social networks.<sup>291</sup> This allows the removal of content that violates the law upon request. In previous work, I concluded that this regime is optimal for regulating secondary liability of intermediaries on social network platforms due to the extensive harm that this online setting may inflict on today's users.<sup>292</sup>

Yet the removal of offensive content might be achieved even without amending section 230. In most cases, U.S. laws allow the bad shaming victim to file an action against the original publisher.<sup>293</sup> Such a suit is only possible if the plaintiff identifies himself using his real name.<sup>294</sup> On many websites, the platform allows the original publisher to remove his statements. The publisher may remove the statements following the victim's request, after a direct lawsuit was filed against him or after a court orders the defendant to remove the statement. In spite of

---

the algorithmic mechanism of YouTube "Content ID," and explaining that this system is susceptible to false positives and blocks content that is not actually infringing). It should be noted that the problems of algorithmic enforcement may be ameliorated as technology advances. Yet, at this time, it is far from optimal and leads to over censorship. See generally BENKLER ET AL., *supra* note 284, at 365 ("[T]he promise of machine learning and artificial intelligence to accurately separate the good from the bad has not been realized"). In a related context of copyright, see, for example, *Lenz v. Universal Music Corp.*, 801 F.3d 1126 (9th Cir. 2015).

<sup>291</sup> A notice-and-takedown regime is a safe haven model that allows intermediaries to escape liability for harmful content if they remove it from their platforms promptly when its existence is brought to their attention. Many legislative regimes of intermediary liability, such as the American DMCA and European E-Commerce Directive, follow versions of this model for online enforcement of different types of harmful content. See BENKLER ET AL., *supra* note 284, at 364–65; Husovec, *supra* note 240, at 57.

<sup>292</sup> See Lavi, *supra* note 117, at 855, 930–31 (offensive speech on social network platforms causes greater harm relative to the same speech in other online settings).

<sup>293</sup> See, e.g., *Boulger v. Woods*, 917 F.3d 471 (6th Cir. Feb. 27, 2019) (case dismissed because the defendant added question marks to his defamatory tweets); see also Patrick H. Hunt, *Tortious Tweets: A Practical Guide to Applying Traditional Defamation Law to Twibel Claims*, 73 LA. L. REV. 559 (2013) (reviewing defamation lawsuits regarding libelous statements posted on Twitter); Lyrissa Barnett Lidsky & RonNell Andersen Jones, *Of Reasonable Readers and Unreasonable Speakers: Libel Law in a Networked World*, 23 VA. J. SOC. POL'Y & L. 155 (2016) (discussing the need to adjust defamation law privileges to social media).

<sup>294</sup> Many social network platforms, including Facebook, require their users to construct a profile that reflects their real identity ("real-name policy") and use their offline names when interacting within the platform. See *Statement of Rights and Responsibilities*, FACEBOOK, <https://www.facebook.com/terms> [<https://perma.cc/NT4L-6TTP>] (last visited March 4, 2016).

section 230 immunity, some courts may order the intermediary to remove the offensive statements after ruling that the expressions violate the law.<sup>295</sup> This may allow removal when the website is not coded to allow the original publisher to remove his own statements or when he refuses to take the statements down.

The removal of the original statement *ex post facto* may not be an efficient remedy because by the time of its removal, it might have been shared by numerous users.<sup>296</sup> After shaming spreads like wildfire, a victim will have to point to each virtual setting of bad shaming and apply to a number of re-publishers or intermediaries in order to efficiently remove the content.

Mass sharing and the problem of weeding out harmful content from the internet calls for a more efficient remedy to limit bad shaming from spreading. It would lead to the removal of defamatory remarks by focusing on the code of the platform, its constraints, and the possibilities it allows.<sup>297</sup> Scholars have suggested using the code and determining an expiration date for information, thus it would be deleted after a period.<sup>298</sup> This solution is less applicable to information that was disseminated by third parties. Moreover, it is next to impossible to anticipate the likelihood that shaming turns into bad shaming in the process of dissemination.

This Subsection proposes focusing on efficient removal *ex post facto*. Accordingly, intermediaries who implement features for sharing content should enable efficient removal of offensive content from all the profiles and locations to which it was spread. To do so, they can

---

<sup>295</sup> See, e.g., *Hassel v. Bird*, 203 Cal. Rptr. 3d 203 (Ct. App. 2016) (granting default judgment and injunctive relief to a lawyer who sued Yelp for a defamatory review). On appeal, the California Supreme Court reversed the ruling. *Hassell v. Bird*, 420 P.3d 776 (Cal. 2018); see also Eric Goldman, *The California Supreme Court Didn't Ruin Section 230 (Today)*—*Hassell v. Bird*, TECH. & MARKETING L. BLOG (July 2, 2018), <https://blog.ericgoldman.org/archives/2018/07/the-california-supreme-court-didnt-ruin-section-230-today-hassell-v-bird.htm> [https://perma.cc/T2XL-TB3N]. Recently, *Hassell* appealed to the U.S. Supreme Court, but the petition was denied. *Hassell v. Yelp, Inc.* 139 S. Ct. 940 (2019).

<sup>296</sup> Expression can spread intuitively without reflective thought by using the “share” or “retweet” buttons on social networks. See XIAO MINA, *supra* note 13, at 126 (referring to the problem of enforcement in the face of dissemination of rumors often in a decentralized way and via private social media).

<sup>297</sup> See LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 123–25 (2006).

<sup>298</sup> See MAYER-SCHÖNBERGER, *supra* note 123, at 83–119.

implement features such as an “embedded link” to the code. Embedded links allow users to pull in external web content and present it in their profiles.<sup>299</sup> They can also use a technology that allows data tethering, which changes the shared content according to the source.<sup>300</sup> Thus, the removal of the original post will result in deleting all replications disseminated by using the forward/share/retweet buttons. The intermediary can implement this feature in the code, architecture, or protocol during the platform’s design stage.<sup>301</sup>

This technology is in use today. However, choice architecture is value-laden, and reflects a particular set of preferences that should not be taken for granted. Every intermediary designs its platform pursuant to its objectives.<sup>302</sup> Some intermediaries structure the sharing mechanisms by linking to the original post. For example, a click on the share button on Facebook or the retweet button on Twitter links to the original content and embeds the shared content into the profiles of the disseminator and his friends. Yet, the internet is not monolithic and may include different attitudes towards the removal of offensive content.

In light of the potential harm of bad shaming, relying on voluntary regulation is insufficient and formal regulation is required. The law should adopt a notice-and-takedown regime for social networks but allow the intermediaries to benefit from their safe haven only if they

---

<sup>299</sup> See Aaron Parson, *What Is the Difference Between Embedding and Linking?*, IT STILL WORKS, <https://itstillworks.com/difference-between-embedding-linking-10052367.html> [<https://perma.cc/HW4C-ETQL>] (last visited Apr. 26, 2019) (explaining that embedding content plays a piece of media without leaving the current webpage. For example, a business might embed a YouTube demonstration of a product into its site, allowing visitors to see the clip without exiting the site). It should be noted that because this link allows for the viewing of embedded content without exiting the site, this type of link leaves open the question of legal liability of the person who embedded the content when the content embedded is harmful. See, e.g., Toby Headdon, *An Epilogue to Svensson: The Same Old New Public and the Worms That Didn’t Turn*, 9 J. INTELL. PROP. L. & PRAC. 662 (2014) (discussing issues with embedded links in the copyright context).

<sup>300</sup> See JONES, *supra* note 79, at 187 (explaining that technology can allow every copied piece of data to be tethered to its master copy).

<sup>301</sup> This approach allows governance via code. This type of governance regulates behavior and the flow of information, and additionally promotes values *ex ante*. See generally LESSIG, *supra* note 297, at 6, 120; Deirdre K. Mulligan & Kenneth A. Bamberger, *Saving Governance-by-Design*, 106 CALIF. L. REV. 697, 701 (2018).

<sup>302</sup> See Nancy Kim, *Website Design and Liability*, 52 JURIMETRICS 383, 402–03 (2012).

embed technology for the efficient removal of offensive content shared via their forward/share/retweet buttons. Thus, the victim of bad shaming will not have to point out on every location or contact every website or platform on which the content was spread, but rather it would be sufficient to approach the platform on which the original text was posted.

Alternatively, the law can narrow down platform immunity and impose a condition regarding the efficient removal of unwanted posts. In such cases, the platform will not bear liability for leaving the expressions online after being notified; yet the victim will be able to file a legal action against the original publisher, which may remove the original post with its replications. This solution mitigates the harm of the victim, enhances the publisher's control over his content, and allows him to remove the content *ex post facto*.

One can argue that conditioning the safe haven in an embedding mechanism for efficient removal infringes on the intermediaries' freedom to design their platform as they please. Indeed, companies should generally have the freedom to design technologies as they please, yet the freedom to design is not absolute, and should be balanced against the risk in operating platforms and the proportionality of limitations on design.<sup>303</sup> Accountable technological design is also a leading principal for improving the protection of human rights in policymaking in related contexts and jurisdictions.<sup>304</sup> In our context, an architecture that allows sharing to a large audience by the click of a button profoundly increases the risk of bad shaming damages. The proposed safe haven does not dictate the technological measurements that should be used in order to efficiently remove the shared content. In addition, it does not automatically impose liability for not adopting these measurements. An intermediary that adopts this solution will narrow its exposure to liability. Yet, in the absence of efficient removal

---

<sup>303</sup> See HARTZOG, *supra* note 29, at 121 ("Companies should generally have the freedom to design technologies how they please, so long as they stay within particular thresholds, satisfy certain basic requirements like security and accuracy, and remain accountable for deceptive, abusive, and dangerous design decisions.").

<sup>304</sup> For example, see the principle of "privacy-by-design" articulated in the GDPR, *supra* note 161, at art. 25; see also HARTZOG, *supra* note 29, at 51–55; Ari Ezra Waldman, *Privacy's Law of Design*, U.C. IRVINE L. REV. (forthcoming) (manuscript at 10), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3263000](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3263000).

mechanisms, liability will be examined on a case-by-case basis and not be imposed in all cases. Thus, the infringement of the freedom to design is proportional.

It should be noted that this solution would lead to the removal of all the content that was disseminated by using the platform's sharing feature buttons. However, it still allows every user to copy a defamatory post and paste it elsewhere without utilizing any of the platform's own re-sharing features. These replications will not be removed when the original offensive post is removed.

However, copying content and pasting it elsewhere is cumbersome and not as automatic as clicking a button. Therefore, most disseminators are likely to cling to the technological default and avoid sharing content in other ways.<sup>305</sup> Indeed, individuals with malice, who seek to inflict harm, can bypass the sharing features and copy the content manually. Yet the number of complaints the victim will have to send to the intermediary will be drastically lower for a platform governed by an efficient removal mechanism. Thus, while this is not a perfect solution, it is expected to mitigate the harm of bad shaming.

Complementary measures can improve this solution.<sup>306</sup> Voluntary cooperation among social media giants such as Facebook and Twitter can allow them to share unique digital fingerprints that they automatically assign to videos or photos of offensive content they have removed from their websites. This will allow their peers to identify the same content on their platforms and remove it. Websites are expected to cooperate if this measure is perceived as family-friendly, which might attract users who are inclined to that environment. As more websites join this initiative, more efficient removal of bad shaming could be achieved.<sup>307</sup> Yet, at this time, these tools of detection still have many

---

<sup>305</sup> See RICHARD THALER & CASS R. SUNSTEIN, *NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS* 8 (2008) (explaining that people have a strong tendency to go along with the status quo or default option).

<sup>306</sup> See Chesney & Citron, *supra* note 96, at 40 (“ISPs and social networks with millions of postings a day cannot plausibly respond to complaints of abuse immediately, let alone within a day or two,” yet “they may be able to deploy technologies to detect content previously deemed unlawful.”).

<sup>307</sup> See, e.g., Solon, *supra* note 242 (discussing the related contexts of revenge porn and inciting content); Klein & Flinn, *supra* note 241, at 79–81 (referring to the role of the National Center for Missing and Exploited Children in maintaining a database of thousands of photographs of child pornography that allows more efficient enforcement by Microsoft

flaws in interpretation and context. Therefore, removal of all replications of text-based expressions should not be used to automatically prevent the upload of content. Rather, it should be used for detection after the content is published on the platform and include human oversight to prevent removal of legitimate content.<sup>308</sup>

### G. *Addressing Objections and Challenges to the Proposed Framework*

Several objections to this framework can be anticipated and some wrinkles must be ironed. The first objection is directed at determining that search engines should delist links to shaming the ugly behavior

---

PhotoDNA, and explaining that the accuracy of this method regarding speech, as opposed to pictures, is not elaborated on) (“[R]eviewing speech for terms of service compliance is not presently accomplished solely with technology but involves human beings reading . . .”).

Yet intermediaries also use these practices regarding extremist content. See Julia Fioretti, *Web Giants to Cooperate on Removal of Extremist Content*, REUTERS (Dec. 5, 2016, 6:10 PM), <https://www.reuters.com/article/us-internet-extremism-database/web-giants-to-cooperate-on-removal-of-extremist-content-idUSKBN13U2W8> [<https://perma.cc/42T8-WUS6>]; Julia Fioretti, *Pressured in Europe, Facebook Details Removal of Terrorism Content*, REUTERS (June 15, 2017, 1:16 PM) <https://www.reuters.com/article/us-facebook-counterterrorism-idUSKBN1962F8> [<https://perma.cc/N9ME-EPA3>] (explaining that Facebook also uses AI in order to identify and remove inciting content quickly); Julia Fioretti & Lily Cusack, *EU Urges Internet Companies to Do More to Remove Extremist Content*, REUTERS (Dec. 6, 2017, 2:14 PM), <https://www.reuters.com/article/us-eu-internet-forum/eu-urges-internet-companies-to-do-more-to-remove-extremist-content-idUSKBN1E02Q7> [<https://perma.cc/54MG-27MB>] (“Over the summer, Microsoft (MSFT.O), Facebook, Twitter and YouTube formed a global working group to combine their efforts in removing extremist content from their platforms, and last year formed a database of known ‘terrorist’ images and videos which now contains more than 40,000 hashes, or digital signatures.”); see also Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035 (2018) (explaining that hashed material would not be immediately deleted from participant’s sites. Instead, each company would review flagged content under its own policies. However, the author criticizes these practices). It can be argued that if intermediaries apply these practices with transparency and use them only for speech that the law specifically prohibits, they might improve current policy. In time, AI may improve the accuracy of algorithmic enforcement. This technology has already been applied for decision-making processes and has the potential to improve online enforcement in this context as well. See Elkin-Koren, *supra* note 239, at 1096–97 (referring to the potential of AI to implement fair use measurements into algorithmic enforcement of copyright infringement).

<sup>308</sup> GILLESPIE, *supra* note 237, at 98–100 (explaining that these systems are not very good yet in handling interpretation and context); see also Duarte, Llansó & Loup, *supra* note 243, at 6. Therefore, there should be human oversight after the detection.

upon request after a year from the publication date. One may argue that this period is arbitrary and does not differentiate between different violations of norms. In addition, it can be argued that delisting links to shaming the ugly behavior after a year is too early. Deletion after a year may hinder the flow of information and result in wrong decisions regarding transactions in the market and inefficiency. In addition, delisting links to shaming that reflects violations of law may hinder the virtues of shaming.

Indeed, the period for delisting might seem arbitrary and could equally be different. Yet this does not undermine a uniform determination for delisting links to shaming the ugly behavior. The proposed rules already differentiate between types of shaming and forms a hierarchy of shaming. Trying to create another differentiation between norm violations will hinder the efficiency of the model and compel search engines to make a decision regarding the relief of delisting on a case-by-case basis. In addition, it is impossible to base a hierarchy of norm violations because different people may perceive the severity of a violation differently. Thus, some people might perceive the use of the internet in a computer store for a long time as a norm violation,<sup>309</sup> while others might not perceive it as a violation at all. Furthermore, the severity of the violation depends on the circumstances and context in which it was committed. Trying to base a hierarchy of norm violations is futile, and will result in inconsistency, uncertainty, and inefficiency.

Indeed, in some circumstances, delisting links to shaming the ugly behavior after a year can hinder efficient decision-making regarding transactions in the market. For example, a case of delisting links to a review on a person that provided a poor service. However, it does not undermine the proposed remedy for mitigating the dignitary harm of shaming the ugly behavior expressions after a year. Delisting links after a year is different from an immediate delist. After a year, the person who violated norms might have changed his behavior, so the shaming expressions do not reflect his current conduct,<sup>310</sup> but if he continues to

---

<sup>309</sup> See SOLOVE, *supra* note 6, at 83–84.

<sup>310</sup> In the context of review websites, negative reviews that shame a business can incentivize its owner to change its ways and improve. See Chrysanthos Dellarocas, *Reputation Mechanisms*, in 1 ECONOMICS AND INFORMATION SYSTEMS 629, 634 (Terrence Hendershott ed., 2006)

provide poor services, people are expected to shame him through additional negative reviews.<sup>311</sup>

The argument that delisting links to shaming that describes violation of laws hinders the virtues of shaming is far-reaching. As for links that condemn individuals who were convicted of serious crimes after a court made a decision regarding their liability,<sup>312</sup> or videos documenting serious crimes,<sup>313</sup> the public interest exception will allow search engines to avoid delisting. By contrast, links to shaming individuals for less severe legal violations should be delisted after a year. In such cases, dissemination of the shaming allows the condemnation of the behavior and can lead to prosecutions and a legal process in courts during that one year. Allowing the delisting of such shaming expressions after a year fulfills the goal of shaming and narrows disproportionality. One should remember that many cases of shaming the ugly behavior represent only one side and might not be accurate. Not extending a right to delist will lead to disproportionate dignitary harm and fail to balance properly between the justifications for shaming and the dignity of the shamed individual. Thus, the proposed rules are superior to the alternatives.

The second objection focuses on procedural difficulties in applying the proposed rules to good shaming and informing search engines to avoid delisting good shaming. Not informing search engines of good shaming will allow shamed individuals to claim that the expressions are

---

(explaining that reputation mechanisms play both a sanctioning and a signaling role. Thus, negative reviews allow consumers to sanction a business with bad reviews by not buying from it. As a result, the owner of the business will have a strong incentive to change its behavior). Similarly, shamed individuals can also change their ways because they do not want to be considered bad actors. For example, Justine Sacco tweeted a racist joke on Twitter and was shamed for it, and then changed her views and even volunteered with a nonprofit organization in Addis Ababa. See Klonick, *supra* note 57, at 1049. Due to the shaming, she will surely not post racist statements anymore.

<sup>311</sup> In such cases, the shamed individual will have to wait a year to delist from the date of each new publication of a negative review.

<sup>312</sup> For example, dissemination of judicial decisions of convictions with condemnation of the defendant. This Article refers to active dissemination of a judicial decision and condemning the behavior of the defendant, and does not refer to the publication of the judicial decision itself. The official publication of the decision by court is not shaming, but rather a publication that serves the public's right for information.

<sup>313</sup> For example, a video that documents serious violence.



shaming the ugly behavior and request to delist links to the shaming expressions.

However, there are ways to overcome this procedural difficulty. One possibility for informing search engines on good shaming is directing the public to link to the judicial decision that recommends the public to shame in their shaming posts. However, this solution might create another problem because some individuals may abuse these processes to make it difficult to delist links to bad shaming and shaming the ugly behavior by linking decisions of good shaming to other types of shaming posts. A complementary solution is creating an official public record of decisions of good shaming that will be shared with search engines. This record will allow search engines to vet whether a request to delist is based on good shaming or other types of shaming. Technology will allow a cross-check of the shaming content and identify it with content in the public record of good shaming by using AI algorithms that will verify that a court recommended the shaming.

The third objection is that search engines' employees and courts still need to use their discretion in classifying the shaming. There is no problem of classification regarding good shaming because a court would have explicitly defined it as such. Yet search engines' employees still have to differentiate between bad shaming and shaming the ugly behavior. Search engines have to delist links to obvious bad shaming, such as links to revenge porn or severe defamation. However, when there is doubt whether an expression benefits from defenses of defamation law, search engines have an option to delist them immediately upon notice or wait for a judicial decision. By contrast, delisting links to shaming the ugly behavior will occur a year after the original publication at the earliest. Thus, when the shaming is not an obvious bad shaming, search engines' employees have to decide whether to treat it as bad shaming or shaming the ugly behavior, and ambiguity remains.

Indeed, the transformation of moderation from standards to rules in general,<sup>314</sup> and in this Article in particular, still leaves discretion. However, the proposed rules are superior to the alternatives of adopting an E.U.-style general right to be forgotten and applying open standards for delisting. The rules structure the semi-judicial discretion of search

---

<sup>314</sup> Klonick, *supra* note 226; Hopkins, *supra* note 237.

engines. In contrast, an E.U.-style general right to be forgotten leaves wider ambiguity.<sup>315</sup> The E.U. right to be forgotten does not outline a clear date in which the information becomes irrelevant and outlines a general “public interest” exception that does not limit the discretion of search engines. In contrast, under the proposed rules, a search engine will delist links to good shaming of ordinary people only according to the instructions in the judicial decision. The search engine must delist obvious bad shaming and has discretion regarding delisting bad shaming when there is doubt regarding the application of legal defenses. Links to shaming the ugly behavior will be delisted only a year after publication. In addition, the public interest exception under the proposed rules is limited to specific circumstances.<sup>316</sup> Although the proposed rules leave ambiguity, the discretion in applying them is narrower relative to the alternative open standards. Thus, the proposed rules are superior to the alternative of the E.U.-style right to be forgotten, as they are expected to reduce ambiguity and increase consistency.

The fourth objection is that applying the proposed rules will result in over-delisting. Search engines have discretion to classify shaming in cases of doubt regarding legal defenses, and delist the source immediately even if the expressions are shaming the ugly behavior. They may also delist links to shaming the ugly behavior even when there is public interest in not delisting them a year after their publication.<sup>317</sup> Indeed, search engines have economic incentives for not delisting links. Yet these incentives might be insufficient, especially when the shamed individual was not convicted in court and search engines bear the burden to reason their failure to delist. Consequently, a chilling effect can be created.

---

<sup>315</sup> It should be noted that the guidelines proposed in the European Union for applying the right to be forgotten are open standards. The guidelines do not clarify the duration of time in which information remains relevant, and outline open criteria. See Art. 29 Data Prot. Working Party, Guidelines, *supra* note 159. The guidelines include a list of common criteria for handling complaints by the E.U. Data Protection Authorities. Yet the criteria are open ended. For example, the fifth criterion refers to the relevance of information. It comments that “[r]elevance is also closely related to the data’s age.” Yet it is not clear how much time has to pass before information loses its relevancy.

<sup>316</sup> See *supra* notes 232–34 and accompanying text.

<sup>317</sup> For example, search engines can delist a link to a video that indicates a severe crime a year after it was published.

The response to this objection is that the proposed framework outlines a legal adjustment for mitigating potential chilling effects and does not rely solely on market forces and economic incentives. According to the framework, courts should avoid imposing compensation on search engines for failing to delist links to non-obvious bad shaming. In such cases, the only remedy for the victim is a court order to delist. In addition, when search engines reasonably avoid delisting links to shaming the ugly behavior due to the public interest exception, and in the end a court orders to delist, the court will not impose compensation. Thus, the chilling effect is limited and there is less concern for disproportionate collateral censorship.

#### H. *A Concluding Remark on Good Shaming*

Shaming on social media is prevalent. Anyone can shame other individuals by disseminating posts or videos that describe their “ugly behavior.” Frequently, internet users abuse the internet for bad shaming that reaches the threshold of tort law or even criminal law and causes dignitary harm. In contrast, currently, good shaming is rare and hardly done.<sup>318</sup> This raises the question of justification to a separated category of good shaming.

Indeed, the cases of good shaming are rare. However, the number of cases does not negate the justification for a separated category. First, the source of authority for good shaming is different. Shaming is not committed according to the discretion of private individuals but rather directed from top down by court recommendations after a legal process and fact checking. Second, online shaming is relatively young and started developing with the emergence of social networks. It can be expected that, in a few years, more courts and judicial tribunals will instruct the public to shame, and the practice of good shaming will not

---

<sup>318</sup> In Israel, the only cases of good shaming occurred in the context of refusal to divorce. See *supra* notes 2–3. In the United States, a judge shamed defendants on social networks by himself. See Cheung, *supra* note 19. In addition, some courts developed non-conventional sanctions. See, e.g., Travis Furman, *Not Your Average Judge! Michael Cicconetti and His 11 Crazy Punishments*, ONEDIO (May 24, 2017, 5:05 PM), <https://onedio.co/content/not-your-average-judge-michael-cicconetti-and-his-11-crazy-punishments-16712> [https://perma.cc/HNT3-TTJR]. Yet, currently, the practice of good shaming is rare.

remain marginal. Therefore, academic research on this topic is important today, more than ever.

This Article is the first to differentiate between good shaming and other types of shaming, and it can pave the path for future discussions, scholarship, and lawmaking that will develop the practice of good shaming and outline its limitations. Not all court recommendations to shame promote fairness and efficiency; yet this practice has positive potential. In some contexts, it can even be more efficient from traditional legal sanctions. Courts should adopt this practice when the legal system is short-handed and cannot provide efficient remedy for law violations. This may occur in refusal to divorce cases,<sup>319</sup> and in situations of defendants who fled from a country, do not obey court orders, and there are difficulties in extraterritorial enforcement. Good shaming might also promote efficiency as an addition to traditional legal sanctions in cases of recidivism;<sup>320</sup> yet this is only an initial hypothesis for future research.

This Article is only the beginning, and it calls for future scholarship and lawmaking on good shaming that should architect the proper scope of this practice and its limitations. Good shaming is instructed by a court and committed by the public. This sanction is therefore different from a court order that can be legally enforced. However, one can argue that it is a sanction outlined by a court, and therefore guidelines, or at least an ethical code for applying good shaming by judges, should be articulated. In the absence of clear guidelines, it can be argued that the

---

<sup>319</sup> Under Jewish law, the husband has to willingly give a *gett* to his wife in order to release her from the marriage. Shaming can incentivize the husband to give a *gett* in cases of refusal to divorce. It can also deter others from refusing to give a *gett* because they know that shaming is likely. Even if the shaming does not result in a *gett*, it promotes the autonomy of the chained woman.

<sup>320</sup> It should be noted that the Jewish law advocates shaming when the shaming incentivizes a person to desist violations where: a) there is certainty that the violation occurred (this can be achieved by relying on a professional body such as the court); b) there were previous attempts to cause the violator to quiet the violations and these efforts did not succeed; c) the shaming intends to stop violations, without other interests; and d) the shaming is accurate and focuses on the wrongful violation. See Yehuda Zoldan, *Public Shaming in Social Networks*, 33 THUMIN 294 (2017) [Heb]. In cases of recidivism, traditional legal sanctions fall short in deterring the violator from future violations. Shaming the violator in such cases might be more efficient in its deterrence effect.

sanction is “void for vagueness.”<sup>321</sup> Thus, this Article recommends to draft guidelines for applying good shaming and articulating the boundaries of this tool and its relation to other traditional sanctions and punishments that are ruled by courts. Guidelines should be articulated carefully to promote consistency and prevent disproportionate harm that might be caused by good shaming. Due to the grave consequences of shaming on the dignity of the shamed individual and possible unexpected consequences of shaming, courts should not instruct the public to shame for violations that are not severe.<sup>322</sup> Yet there is a question of whether good shaming should be limited to cases in which the legal system is short-handed to provide efficient remedies for law violations. The Article leaves the question open for future research and policy discussions.

Due to the promise of good shaming, the guidelines for applying it should allow adjustments to future technologies.<sup>323</sup> The legal system should remove procedural barriers for applying good shaming<sup>324</sup> and promote an efficient implementation of it.<sup>325</sup> Guidelines for applying good shaming, removing procedural barriers, and promoting efficient implementation will allow fulfilling the promise of good shaming and reducing inconsistency and inefficiency.

---

<sup>321</sup> See *United States v. Evans*, 333 U.S. 483 (1948); *Connally v. Gen. Constr. Co.*, 269 U.S. 385 (1926); *United States v. Brewer*, 139 U.S. 278 (1891).

<sup>322</sup> For example, shaming a person that was convicted for driving while he was drunk. It should be noted that in a similar case, a governmental authority in the United States shamed people who were arrested for driving while drunk and their arrest was published online in “the wall of shame.” A court determined that shaming the drivers in this way went too far. See HARTZOG, *supra* note 29, at 254; *Bursac v. Suozzi*, 868 N.Y.S.2d 470 (Sup. Ct. 2008).

<sup>323</sup> See Goldman, *supra* note 6, at 450–51.

<sup>324</sup> For example, allowing revealing the names of pseudonym litigants (Jon Doe), after a conviction that justifies additional shaming removes a procedural barrier.

<sup>325</sup> Efficient implementation can be achieved by establishing a record of all the good shaming decisions given by a court and sharing the record with search engines. This record can allow the search engine to avoid delisting links to good shaming.

## CONCLUSION

*“When shamings are delivered like remotely administered drone strikes, nobody needs to think about how ferocious our collective power might be. The snowflake never needs to feel responsible for the avalanche.”*<sup>326</sup>

The rise of online social networks and the development of sharing features allow internet users to disseminate ideas to a large audience. In this environment, shaming is common more than ever. This Article focused on shaming ordinary people, as opposed to public figures and corporations. It reviewed the benefits of shaming and addressed the negative aspects of this phenomenon. It then explained that shaming is not a monolithic phenomenon and outlined a taxonomy of shaming that showed its benefits and flaws, which do not equally apply to different categories.

Following this analysis, the Article referred to the technological developments that allow finding shaming at a later stage. It argued that due to technological developments, a new balance between memory and oblivion should be adopted, and new remedies should be developed for dignitary harm. The Article showed that in many cases, the benefits of shaming are not valid after a period of time and can even stand in contrast to the logic behind expungement laws. Therefore, the law should allow reversibility to the shamed individuals. This can be done by imposing an obligation on search engines to remove the shaming information following a request of the shamed individual, thus obscuring the information. This Article argued that a dichotomous perspective that chooses between oblivion (deletion of the shaming information) and permanent memory (leaving the expression online without limitations) is inappropriate. Instead, the law should recognize different degrees of oblivion.

This Article outlined guidelines for applying a right to delist links to shaming. These guidelines allow a differential right to delist, depending on the type of shaming and the level of public interest contained in the information. The Article also argued that obscuring the information by granting a right to delist links in search results is an

---

<sup>326</sup> See RONSON, *supra* note 9, at 56.

insufficient remedy to bad shaming. Therefore, it concluded by offering a complementary solution for efficient removal of bad shaming from websites where the shaming expressions appear. The proposed solution balances dignity and free speech considerations, and it promotes efficiency and distributive justice.

The Article is not the final word on this topic. Looking ahead, it opens up new avenues for inquiry and inspires further discussions. For example, what is the normative scope of digital memory for public figures and celebrities who are shamed? What is the normative scope of the digital memory for corporations? What guidelines should be outlined for the dissemination of personal information other than shaming? How should the law combat bad shaming that is disseminated via applications for smartphones, such as WhatsApp, that are mere conduits and lack editorial control over content? Should the law develop additional remedies for dignitary harm of dissemination? And what about remedies for dignitary harm that result from processing and analyzing personal information and manipulating individuals without shaming them in public? These challenges and others are projects for another day.