Santa Clara University School of Law

Santa Clara High Technology Law Journal

Volume 32 | Issue 2 Article 2

8-11-2016

Can Digital Speech Loosen the Gordian Knot of Reputation Law?

Elizabeth A. Kirley

CAN DIGITAL SPEECH LOOSEN THE GORDIAN KNOT OF REPUTATION LAW?

Elizabeth A. Kirley[†]

This paper likens the current state of reputation law to a Gordian knot, entangled in complexities and calling for novel thinking to make it relevant to our public and private lives. Its central thesis is that digital speech is ontologically different from offline speech and so calls for a more informed response to the harms it can inflict in order to determine whether legal or extra-legal mechanisms are most restorative. In spite of a wealth of international norms that address the value of personal reputation, they have had minimal influences on regional and domestic laws of the European Union and the United States, reflecting the deeply rooted cultural differences on each side of the Atlantic that shape laws of privacy and free speech. In conclusion, implications for future methods of addressing online reputational harm outside of traditional legal systems are discussed.

TABLE OF CONTENTS

[†] Ph.D. 2015, LL.M. 2006, Osgoode Hall Law School, York University in Toronto; JD University of Western Ontario; Associate Professor, Faculty of Business and Law, Deakin University in Melbourne AU. This paper was facilitated by a postdoctoral fellowship at the Nathanson Centre for Transnational Human Rights, Crime and Security at Osgoode Hall Law School. The author thanks Dr. Margaret Beare in addition to the editorial staff of this publication, with special thanks to Sara Townsend, as well as helpful commentators at the British & Irish Law, Education & Technology Association Annual Conference, Hertfordshire University, Hatfield UK, April 2016.

INTRODUCTION

Legend of early Indo-Europeans tells of the king of Phrygia tying his cart to a public post with an intricate knot of bark. After centuries of locals attempting to disentangle the knot, Alexander the Great devised a simple, but untried solution: he sliced it with his sword, thereby fulfilling Zeus' prophecy that the victor would become king of all Asia. Alexander was clearly thinking outside the box.

This paper likens the current state of reputation law to a Gordian knot, entangled in complexities and calling for novel thinking to make it relevant to both our public and private lives. Its central thesis is that digital speech, meaning communications on social media or other messaging platforms that are more amateurish, spontaneous and conversational than well researched speech aimed at a broader audience, is sufficiently different in kind from offline speech that it calls for a more informed response to the reputational harms it can inflict. Due to this ontological difference, rigorous, interdisciplinary research is needed to determine whether traditional legal responses or extra-legal solutions will be most restorative. Those harms are not to be underestimated in the emotional, financial and professional damage they can impose. They relate to the Internet's idiosyncrasies of memory, global distribution, telescoping of time, and the easy

acceptance of anonymity. Their sting can be felt through online invective and false stories or unauthorized exposure of personal data. In order to respond to free expression/privacy tensions, we need to understand the language, motivations and literacy of trolls, flamers, anarchists, militants, business competitors, jihadists and all those who aim to destroy our social, professional and financial identity as individuals.

This topic has universal importance because the social impact of lost reputation can be profound. We stand to lose our social and professional worth at the hands of vengeful ex-lovers, disgruntled employees or mean spirited trolls who work anonymously. Common law systems seem incapable of producing legal responses that can ease that suffering; the Internet, rather than utilizing its enhanced features of global dissemination and instantaneous response as steward of our reputational privacy, has served more as facilitator of harm.

The paper begins by noting that, although international law offers a wealth of legal norms for the protection of reputation through the lens of private and family life, those values have failed to inspire clearly stated laws or jurisprudence on the domestic level. The disappointing result has been the second tier status that jurists frequently allocate to reputational privacy in deference to free speech. While more recent privacy and data protection laws strive to right that imbalance, few are effective in rehabilitating one's dignity, honor and personality rights (as valued in the European tradition) or the American balancing of a right to be left alone and speech freedoms, as increasingly informed by the first amendment, section 230 of the *Communications Decency Act*,[1] and the more recent *SPEECH Act*.[2] That conflict of norms means that, when it comes to online social media messaging, addressing reputational damage calls for thinking outside the box.

This paper proceeds as follows: Part I examines international instruments for their influence on regional (EU) and domestic (US) law and details how those legal responses have produced quite discrete bodies of law on each side of the Atlantic, reflecting diverse

1. Communications Decency Act, 47 U.S.C. §230

2. Securing the Protection of our Enduring and Established Constitutional Heritage Act (SPEECH Act), P.L. 111-223, codified at 28 U.S.C. §§ 4101-4105, which bars U.S. courts, both state and federal, from recognizing or enforcing a foreign judgment for defamation unless certain requirements, including consistency with the U.S. Constitution and section 230 of the Communications Act of 1934 (47 U.S.C. § 230), are satisfied.

cultural values that shape them. Part II examines how reputational harm might be perpetrated and impediments to traditional legal responses. In Part III the ontological difference between online and offline speech is explored and extra-legal responses to reputational jeopardy are canvassed. The paper concludes with suggestions for future explication of reputational damage from digital speech and misuse of personal data.

I. INTERNATIONAL & DOMESTIC REPUTATION LAWS

Since the end of World War II, the international community has formulated a wealth of significant legal conventions that address reputation, primarily by framing those concerns broadly within values of privacy, family life, and personal dignity. Signatories acknowledge our entitlement to those protections as members of the human race. Although world wars have shrunk to more regional and asymmetric conflicts in the ensuing decades, the ambit of our interpersonal communications have gone the other way, expanding from localized gossip to instantaneous global dissemination of our secrets and stigma via Internet and social messaging.

We might anticipate, therefore, that the wide selection of international norms regarding privacy and reputation would provide a conceptual reference point and inspiration to domestic laws. Similarly, with the emergence of the Internet and social media as the dominant interpersonal messaging tools over the past decade, it would be reasonable to expect the evolution of digital-specific laws to protect our virtual presence from verbal attacks and data exposure that jeopardize our future opportunities of a social, professional and financial nature. Unfortunately for law reform, we see that those international values seldom seep down to domestic laws or jurisprudence.

A. Conventions & Declarations

1. UDHR & ICCPR

Two 20th century international instruments expressly address reputation as a basic human right, the first crafted by United Nations members as they emerged from the destruction and atrocities of the Second World War and the second, somewhat ironically, created in the midst of the Vietnam War of the mid-1960s. The *Universal*

Declaration of Human Rights[3] (UDHR) and the *International Covenant on Civil and Political Rights*[4] (ICCPR) use almost identical wording to stipulate that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and *reputation*" and that "everyone has the right to protection of the law against such interference or attacks."[5] The ICCPR only addresses interference and attacks that are "unlawful."[6]

The UDHR in article 19 also addresses a human right to free speech "through any medium and regardless of frontiers."[7] Reputation is treated as a right devolving from social and political life, and is significantly broader than the protections against violent and arbitrary treatment with which the UDHR begins. As one source explains, the UDHR leaves larger scope for variation in different social and political contexts, because "individuals everywhere have the right to be free of torture, but different countries may legitimately come to different conclusions about the conditions under which private property may be taken for public use."[8] Such differential treatment sets up the conditions for a hierarchy of rights in actual state practice.

The US and EU Member States have all signed both the UDHR and the ICCPR and ratified the former treaty.[9] Both treaties have enforcement bodies: for the UDHR several oversight mechanisms are provided.[10] The ICCPR is monitored by the UN Human Rights

---

3. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948), at Article 12. International law creates a hierarchy of instruments: a *convention* (synonymous with *treaty* and *covenant*) is binding between states. Conventions are stronger than *declarations* that constitute an agreement of standards without legal enforcement. Declarations frequently are products of UN Conferences and can be produced by government representatives or NGOs.

4.International Covenant on Civil and Political Rights, G.A. Res 2200A (XXI) A, U.N. Doc. A/RES/2200A(XXI) (Dec. 16, 1966), at art. 17 [hereinafter International Covenant].

5. *Id.* Those instruments, in combination with the International Covenant On Economic Social and Cultural Rights, comprise the International Bill of Human Rights.

6. *Id.* at art. 17(1).

7. "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948)

8. Mary Ann Glendon, *The Rule of Law in the Universal Declaration of Human Rights*, 2 NW. J. INT'L HUM. RTS. 1, 6 (2004).

9. The US signed on Oct. 5, 1977. EU Member States sign upon gaining EU membership.

10. Including the Committee on Economic, Social, and Cultural Rights, the Office of the UN High Commissioner on Human Rights, the Human Rights Council, and treaty-monitoring

Committee through regular reports from state parties on implementation of those rights. In practice enforcement for both treaties is more nominal than practical, however, with diplomatic pressure and other 'soft law' tools being preferred.

The UDHR is not legally binding as such; it carries no formal legal obligations but might carry moral obligations or attain the force of law as customary international law. Most of its rights had already received a significant degree of recognition by 1948 in the constitutions of many nations, if not in their practices.

In the case of the ICCPR, the US and all EU Member states that are parties to the Convention must respect the provisions of the treaty, subject to reservations, understandings and declarations (RUDs) requested by other signatories. One controversial RUD of considerable weight in foreign relations requested that the US Constitution prevail over any contested free speech issue involving the terms of the ICCPR. Another key RUD attached by the US Senate is a "non self-executing" Declaration, intended to limit the ability of litigants to sue in a US court for direct enforcement of the ICCPR. That Declaration effectively challenges any external enforcement mechanism.

Cases relating to reputation that expressly reference the UDHR and the ICCPR are very limited; one reason might be the strength of RUDs requested by the US. Another could be the comparatively low value allotted to reputational harm and privacy invasions on the international spectrum of human rights violations. Remedies, as discussed in the *UN Basic Principles and Guidelines on the Rights to Remedies*, seem restricted to "gross" violations of International Human Rights Law and "serious" violations of International Humanitarian Law, a bar that indignities and social stigma caused by reputational injury might not be able to hurdle.[11]

In a report to the ICCPR Human Rights Committee in 2014, the US was criticized for its surveillance activities on foreign and US citizens[12] that showed non-compliance with the privacy provisions in

---

bodies like the Committee on the Elimination of Discrimination against Women and the Committee on the Rights of the Child.

11. *See* Basic Principles and Guidelines on the Right to a Remedy and Reparation for the Victims of Gross Violations of International Human Rights Law and Serious Violations of the International Humanitarian Law, G.A. Res. 60/147, U.N. Doc. A/RES/60/147 (Dec. 16, 2005).

12. Specifically highlighted were NSA's bulk phone metadata surveillance program (§ 215 of the USA PATRIOT Act); surveillance under § 702 of the Foreign Intelligence Surveillance Act (FISA), conducted through PRISM (collection of communications content

the ICCPR's Article 17 and with international law principles of legality, proportionality and necessity.[13] Although reputation rights were not expressly addressed, the report recommended that any interference with the right to *privacy, family, home or correspondence* henceforth be authorized by laws that: 1) are publicly accessible; 2) are tailored to specific legitimate aims; 3) detail the precise circumstances of data collection and obtaining consent, and 4) provide for effective safeguards against abuse.[14] Also listed as excessive invasions of personal privacy are practices of third parties such as Internet Service Providers (ISPs) to retain personal data for state use.[15]

The Human Rights Committee monitoring state compliance with the ICCPR has interpreted the convention's free speech provisions as describing a much narrower right than that articulated in US constitutional laws. In any conflict between a US citizen's free speech rights and those of a non-US citizen subject to a non-US free speech law, the US position is likely to prevail due to its wider legal ambit. That is particularly the case with hate speech, where the US subscribes to a wide tolerance: only incitement that is intended to cause *imminent* violence justifies restricting fundamental speech rights.[16] Some EU states, however, such as Finland, Belgium, Iceland, and Denmark, oppose the term "hate speech" as potentially restricting democratic debate on religion and minorities.[17] Those speech protections are broader still than those in American law and can have injurious results for individual reputation.

The third pillar of an International Bill of Human Rights in concert with the UDHR and the ICCPR is the UN's *International Convention on Economic, Social and Cultural Rights* created in 1996. It does not expressly address reputation or privacy. Altogether the three treaties comprise a wide range of human rights that form an interrelated normative system.

---

from United States-based Internet companies) and UPSTREAM (collection of communications metadata and content by tapping fiber-optic cables carrying Internet traffic).

13. *Concluding Observations on the Fourth Periodic Report of the United States of America*, International Covenant on Civil and Political Rights, Human Rights Committee (Apr. 23, 2014), http://www.refworld.org/docid/5374afcd4.html.

14. *Id.* at § 20(b) (emphasis added).

15. *Id.* at § 20(c) and (d).

16. *See also Hate Speech*, ARTICLE19.ORG, https://www.article19.org/pages/en/hate-speech-more.html (last visited Apr. 7, 2016).

17. *Id.*

2. International Convention on Migrant Workers & Convention on the Rights of the Child

A more recent addition to international law is the *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families* that requires protection for "privacy, family, correspondence or other communications" against "unlawful attacks on his or her honour and reputation."[18] With that treaty, even temporary citizens are afforded a basic right to a good reputation, although subordinated to "respect for the rights and reputation of others."[19]

Other international instruments and initiatives that are relevant to reputation include the *UN Convention on the Rights of the Child* (prohibiting arbitrary or unlawful interference with a child's privacy, family, or correspondence, and unlawful attacks on his or her honor and reputation*);*[20] the *UN Convention on the Rights of Persons with Disabilities* (with similar provisions for the disabled, including protection from unlawful attacks on reputation and privacy rights for correspondence "and other types of communications"); [21] and the *UN Resolution on a Global Agenda for Dialogue among Civilizations* that urges full utilization of communication technologies including the Internet to further global dialogue and understanding.[22]

All of the above reveal international consensus on the importance of reputation protection as a legal norm. Although

---

18. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, G.A. Res. 45/158, U.N. Doc. A/RES/45/158 (Dec. 18, 1990), at art. 14.

19. *Id.* at art. 13(3)(a).

20. Convention on the Rights of the Child, G.A. Res 44/25, U.N. Doc. A/RES/44/25 (Nov. 20, 1989), at Art. 16. ("1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and *reputation*") (emphasis added).

21. Convention on the Rights of Persons with Disabilities, G.A. Res. 61/106, U.N. Doc. A/RES/61/106 (Dec. 13, 2006), at art. 22. ("1) No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence or other types of communication or to unlawful attacks on his or her honour and *reputation*. Persons with disabilities have the right to the protection of the law against such interference or attacks; 2) States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others") (emphasis added).

22. Global Agenda For Dialogue Among Civilizations, G.A. Res. 56/6, U.N. Doc. A/ RES/56/6 (Nov. 21, 2001), at art. 9 ("Utilization of communication technologies, including audio, video, printed press, multimedia and the *Internet*, to disseminate the message of dialogue and understanding throughout the globe and depict and publicize historical instances of constructive interaction among different civilizations.") (emphasis added).

repeated in regional instruments of the European Union (EU) reputation law does not trickle down to domestic (national) laws *per se*, but only obliquely through laws of defamation or privacy.

B. Regional Responses to Reputation Law

1. European Convention on Human Rights (ECHR)

In contrast to the wealth of international treaties that expressly address reputation, the *European Convention on Human Rights* (ECHR)[23] does not contain direct references to honor or reputation as a discrete *human right*; rather it makes the right of free expression subject to protection of "the reputation and rights of others."[24] The use of "reputation" as a qualification rather than a right seems deliberate, as appears from the preparatory work on Article 10 of the ECHR.[25] The text of the ECHR approaches reputational protection obliquely, then, as a contingency that would limit free expression, similar to such occurrences as threats to national security, public safety, the economic well-being of the state, the prevention of disorder or crime, the protection of health and morals, and the protection of the rights and freedoms of others." [26]

Recognition of reputation as a right of equal import to speech was slow to come in EU case law. In the first defamation case brought under article 10 of the ECHR, *Lingens v. Austria* in 1986,[27] the

---

23. Convention for the Protection of Human Rights and Fundamental Freedoms, Sept. 3, 1953, 213 U.N.T.S 222, (art. 10(2)) (ECHR), formulated by the Council of Europe after the Second World War ro provide for the first time human rights within Europe enforceable under international law and before a court independent of the nation states. Only states that belong to the Council of Europe can become parties to the ECHR. The ECHR is not an EU instrument, unlike the Charter of Fundamental Rights of the European Union that came into force in 2000 for all EU member states that assembled into one instrument human rights from several previous treaties, including the ECHR.

24. *Id.* at art. 10(2).

25. *See also European Commission of Human Rights Preparatory Work on Article 10 of the European Convention on Human Rights*, COUNCIL OF EUROPE, SECRETARIAT OF THE COMMISSION, Doc. No. DH (56) 15 Or. Fr. (Aug. 17, 1956) (noting the following proposals that were made but did not appear in the final document: a French proposal that free speech could be limited by the protection of "the reputation or rights of other persons" (Dec. E/1371, p. 21); a UN conference on freedom of information suggesting that free speech be restricted by expressions by other persons that "defame their reputations or are otherwise injurious to them without benefiting the public." (§ 2(g) and a similar proposal by the British Government (§ 8(3)(2)). Subsequent submissions to a Committee of Experts eliminated all references to "reputation.").

26. ECHR, *supra* note 21, at arts. 8, 10.

27. Lingens v. Austria 8 Eur. Ct. H.R. 407 (1986). Lingens published comments in a Vienna magazine characterizing behavior of the Austrian Chancellor as "basest opportunism,"

European Court of Human Rights (ECtHR) rejected the Government's argument that the case concerned a conflict between two equal Convention rights; the court held that a right to reputation only served as qualifier of the right to free expression. With the Article 10 case of *Chauvy and others v. France*[28] in 2004 and the article 8 case of *Pfeifer v. Austria*[29] in 2007, however, the right to protection of reputation was recognized as having full Convention status. The *Pfeifer* case decided "a person's right to protection of his or her reputation is encompassed by Article 8 as being part of the right to respect for private life".[30] With that case, European law had finally incorporated international legal norms expressed by the UDHR and ICCPR.

That development has its critics: Stijn Smet of the University of Ghent criticizes the European Court of Human Rights (ECtHR) for elevating reputation to convention rights status equal to its "strongest enemy."[31] Smet cites the ECtHR case of *Polanco-Torres* (where a judge's wife fought defamatory claims that she and her husband engaged in unlawful business transactions) as a judicial attempt to balance the human rights pendulum that had swung too far on the side of reputation with *Pfeifer*. In Smet's opinion the court wrongly set a high standard for proof of harm as one that "compromises personal integrity."[32] Smet is persuasive in arguing that, by creating the integrity standard, the ECtHR has created a situational right rather

---

"immoral" and "undignified." The Austrian criminal code provided the defense of truth but Lingens maintained they were value judgments and hence not within the four corners of that code. The ECtHR agreed and found a violation of Lingen's article 10 free speech rights without addressing reputational harm.

28. Chauvy and others v. France, 41 Eur. Ct. H.R. 29 (2005), regarding a book that suggested by innuendo that Jean Moulin, Resistance Leader in WW2 was betrayed and killed because of the actions of Raymond Aubrac who escaped. ("The book is little more than pure conjecture and constitutes a direct assault on the integrity and identity of Mr and Mrs Aubrac that robs them of their dignity. It is necessary to reaffirm respect for human dignity as one of the most important Convention values and one which historical works must also foster.")

29. Pfeifer v. Austria, 48 Eur. Ct. H.R. 175 (2007) (regarding an article alleging the Jews attacked Germany in 1933 and trivializing the actions of the Nazi regime and stating "A person's reputation, even if that person is criticised in the context of a public debate, forms part of his or her personal identity and psychological integrity and therefore also falls within the scope of his or her private life under Article 8.").

30. *See also* Stijn Smet, *The Right to Reputation Under the European Convention on Human Rights*, STRASBOURGOBSERVERS.COM (Nov. 1, 2010), http://strasbourgobservers.com/2010/11/01/the-right-to-reputation-under-the-european-convention-on-human-rights/.

31. *Id.* The European Court of Justice (ECJ) rules on European Union law while the European Court of Human Rights (ECtHR) rules on the European Convention on Human Rights which covers the 47 member states of the Council of Europe.

32. *Id.*

than balancing an existing right with a competing right of free speech using the traditional proportionality test. As a result, when applying the *Polanco* case "in some situations one enjoys a right to reputation and in others not."[33]

2. American Convention on Human Rights

Across the Atlantic, the *American Convention on Human Rights*, promoted by the Organization of American States (OAS) with state members in North, Central, and South America, sets out the right to privacy, honour and dignity.[34] It prohibits arbitrary interference with the "right to privacy or one's reputation" and stipulates that everyone has the right to protection of the law against attacks or interference with that right.[35] It further subjects the right of expression to a "respect for the rights or reputations of others."[36] The Convention also provides for a right of reply to individual complaints of reputational violations through the designation by every publisher (including online publishers) of a person without immunity to respond to such complaints.

The Convention was inspired by the *American Declaration of the Rights and Duties of Man* (the Declaration of the Americas) that marked the modern world's first general international human rights instrument, predating the Universal Declaration of Human Rights by one year.[37] The US and Cuba are the only parties not to have ratified the Convention, and a few states have actually attempted to rescind their ratification.[38] In practice, the OAS and the Convention are seen as "more Latin American than Inter-American" and there is strong pressure for the US to become a State Party to alternative OAS Inter-American treaties.[39]

---

33. Smet, *supra* note 30.

34. Organization of American States, American Convention on Human Rights, Nov. 22, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123, Article 11 ("1. Everyone has the right to have his honour respected and his dignity recognized; 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honour or *reputation*; 3. Everyone has the right to the protection of the law against such interference or attacks.") (emphasis added).

35. *Id.*

36. *Id.* at art. 13, § 2(a).

37. *American Declaration of the Rights and Duties of Man*, Inter Am. Comm'n H.R. (May 2, 1948).

38. Trinidad and Tobago has rescinded; Peru tried, but used the wrong procedure.

39. Monica Pinto, *The Role of the Inter-American Commission and the Court of Human Rights in the Protection of Human Rights: Achievements and Contemporary Challenges,* 20 HUM. RTS. BRIEF 2 (2013).

Although not well known outside of the legislative histories of the parties, the Declaration of the Americas has been referenced in the jurisprudence of both the Inter-American Court of Human Rights (IACHR), created by the OAS, and the work of the Inter-American Commission on Human Rights. The latter functions as a court of first instance and works at enforcement of the Declaration of the Americas in all OAS Member States.

Akin to its position regarding the ICCPR, the US holds that its own laws provide the same or stronger human rights protections than those of the Declaration of the Americas, in spite of its lack of a centralized data protection regime. As testament, the IACHR jurisprudence lacks any cases of US origin. Key objections in the US to OAS rights protections relate to issues of federalism, sovereignty, and incompatibility with US domestic laws, most prominently the US Constitution.[40] In political terms, US exceptionalism regarding OAS activities is heavily criticized by other members of the Convention that aim to exclude US participation.[41]

In addition, the US is signatory to many of the international conventions outlined above but on the domestic front, as we shall see, there is no direct mention in the US Constitution of "reputation" or "privacy" and data protection laws are formulated on an ad hoc and sectoral basis, producing a patchwork of protections across the country.

3. Data Protection in Europe

Reputational privacy can be adversely affected by the unauthorized disclosure of personal data, an act that occurs each time Internet users log on to search engines such as Google or the social networking site Facebook or other web service companies that transmit their personal identifying information across geopolitical borders. Companies such as Facebook, Google, Apple, LinkedIn, Dell

---

40. *Id.* at 21 (advising the US to ratify the American Convention to show international leadership regarding human rights).

41. The term "U.S. exceptionalism" is used here to indicate the belief that, unlike other states, the United States does not need to ratify international human rights treaties because its domestic legal system provides the same or better protections. *See* Stephen M. Walt, *The Myth of American Exceptionalism,* FOREIGNPOLICY.COM (Oct. 11, 2011), http://foreignpolicy.com/2011/10/11/the-myth-of-american-exceptionalism. *See also* Francisco J. Rivera Juaristi, *U.S. Exceptionalism and the Strengthening Process of the Inter-American Human Rights System,* AM. U. HUM. RTS. BRIEF (2012), http://www.wcl.american.edu/hrbrief/20/2juaristi.pdf (noting that US exceptionalism has left the Inter-American Human Rights System vulnerable to attacks on its legitimacy and credibility).

and Intel, for example, store their user data in Ireland, a corporate decision that translates into massive amounts of user information leaving countries of origin. As we shall see, data protection policies within the Council of Europe and European Union member states build on a long-held cultural respect for dignity of individuals by sheer virtue of their humanity. Policy makers in the US, by contrast, give innovative leadership and free speech pride of place in policy decisions and lawmaking. Those culturally entrenched and political relevant differences have wide ranging effects on international efforts to agree on an international technology policy as smart technologies, including digital communications, are introduced into more and more areas of society.

With respect to data protection law in Europe,[42] two international instruments are crucial to ongoing oversight of transborder data flow that could intrude on citizens' reputational privacy: the Council of Europe's *1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* (Convention 108),[43] and the *1980 Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data,* drafted by the Organization for Economic Cooperation and Development (OECD Guidelines).[44] Those rules were devised to deal specifically with personal information that crosses international borders, targeting the adequacy of protection afforded citizens in the exporting country. The former, Convention 108, was devised in pre-Internet days and has

42. *See generally* Meg (Ambrose) Jones, *A Right to a Human in the Loop: Legal Constructions of Computer Automation & Personhood from Data Banks to Algorithms*, SSRN (Aug. 1, 2016), http://dx.doi.org/10.2139/ssrn.2758160.

43. *European Treaty Series – No. 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, COUNCIL OF EUROPE, (Jan. 28, 1981) [hereinafter ETS No. 108]. The Convention has 53 signatories from Europe, Asia, South America and North Africa. *See also* Graham Greenleaf *'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?* 29 COMPUTER. L. & SEC. REV. 4 (2013) (documenting efforts to globalize Convention 108 to protect the transborder flow of data related to EU citizens and to enjoin non-European states in protection of their citizens within a globalized information flow and communications environment).

44. Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, ORGANISATION FOR ECONOMIC CO-OPERATION AND Development (July 11, 2013), http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. See also New Technologies and Their Impact on Regulation, ICT REGULATION TOOLKIT, http://www.ictregulationtoolkit.org/1.7 (last visited April 7, 2016) (discussing secondary use of data and enforcement of privacy guidelines); OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, OECD.ORG (2007), http://www.oecd.org/internet/ieconomy/38770483.pdf; Jennifer Stoddard, Thirty Years After The OECD Guidelines, OECD.ORG (2011), http://www.oecd.org/sti/ieconomy/49710223.pdf (discussing historical overview).

been described by the European Data Protection Supervisor as the only legally binding international treaty dealing with privacy and data protection.[45] It outlaws the processing of sensitive data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected. It applies to both private and public authorities, such as police organizations, but has been heavily criticized for lack of enforcement mechanisms and for its Euro-centered membership.[46]

Convention 108 places more emphasis on protection of human dignity and human rights through individual control of our data but does not expressly mention "reputation" or the personal cost of data misuse.[47] So too, the original OEDC Guidelines did not express concerns over individual reputation; revisions in 2013 mention reputation for the first time within the context of the "reputational impact" and "loss of trust or confidence" caused to individuals by organizations that experience a data breach, whether by inadvertence, negligence, or victimization at the hands of data thieves.[48] Both the 108 Convention and OEDC Guidelines are under continuous review but, despite those efforts, they have been criticized as ineffectual, as "burdensome to those whose motives are benign and ineffective towards those more malignly inclined."[49]

The *EU Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (95 Directive), inspired by Convention 108, was devised in the mid-1990s when personal computers were not widespread and

---

45. *Questions and Answers*, EUROPEAN DATA PROTECTION SUPERVISOR, https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA (last visited April 7, 2016).

46. Jorg Polakiewicz, *Convention 108 As a Global Privacy Standard?* INTERNATIONAL DATA PROTECTION CONFERENCE (June 17, 2011), http://www.coe.int/t/dghl/standardsetting/DataProtection/TPD_documents/Convention_108as_a_global_privacy_standards_June_2011.pdf.

47. ETS No. 108, *supra* 43, at preamble ("that it is necessary, given the diversification, intensification and globalisation of data processing and exchanges of personal data, to guarantee human dignity and the protection of human rights and fundamental freedoms of every person, in particular through the right to control one's personal data and the processing of such data.").

48. *Supplementary Explanatory Memorandum To The Revised OECD Privacy Guidelines*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT 26 (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

49. Sylvia Kierkegaard et al*., 30 Years On - The Review of the Council of Europe Data Protection Convention 108,* 23 COMPUTER. L. & SEC. REV. 223, 231 (2011).

data privacy regulation was viewed as "a niche activity".[50] Both instruments use technologically neutral language, as does the OEDC Guidelines, to avoid the dating of laws through reference to specific technologies that would be replaced over time. [51] What they provide are broad principles that serve as a template for the more technologically specific *General Data Protection Regulation* (GDPR) that was adopted at the EU level on April 14, 2016, after four years of drafting and negotiations; it is now officially EU law, replacing the 95 Directive and all national data protection legislation.[52]

While the 95 Directive did not expressly address the protection of "reputation," it set out the objective of protecting a "right to privacy, with respect to the processing of personal data."[53] The GDPR improves on that with two references to "reputation," but in the preamble rather than in the regulation proper:[54] the first recognizes risks to rights and freedoms, such as damage to reputation; the second reference includes reputational damage in a listing of general physical, material or non-material damage to natural persons arising from data misuse.[55] Interestingly there were eleven such references in the working draft.

Other, more innovative, provisions grant the right of access to data by the data subject[56] and the right to an effective remedy for misuse or leakage, some within a month of the transgression.[57] Those competent authorities have jurisdiction over online activities that fall within the scope of EU law only, that is, for activities of data processors located within the EU, whether or not processing is carried out in the EU.[58] Most notable for those who subscribe to a 'right to be

50. Council Directive 95/46, 1995 O.J. (L 281/31) (EC) [hereinafter 95 Directive].

51. Opinion of the Economic and Social Committee on the 'Proposal for a Council Recommendation Concerning the Protection of Minors and Human Dignity in Audiovisual and Information Services' (EC) No. 98/C 214/07 of 10 July 1998, 1998 O.J. (C 214) 25, § 3.2.5 (defining technologically neutral language: "Regulation should be 'technology-neutral': as few as possible new regulations, policies and procedures should be specific to the new services.").

52. *Regulation (EU) 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 or GDPR).

53. Counsel Directive 95/46, *supra* note 50, at art. 1.

54. Such references would provide interpretation guidelines, not law.

55. .GDPR, supra fn 52, Preamble paras. 75 and 85.

56. .*Id.*, at Section 2, particularly Art. 15.

57. .*Id.*, at art. 12.4, Art. 77 and Art. 79.

58. *Id.* at art. 3.1. It also applies to processing outside of the EU where goods or services are offered online to EU residents.

forgotten' as a reputational privacy mechanism for online content, and as suggested in preliminary proposals of the European Commission, the GDPR contains both a right of deletion of personal data and a right to restrict processing.[59] Conditions for granting a right of deletion include: where the personal data are no longer necessary for the purposes for which they were collected; the data subject withdraws the original consent for their use; or they were processed illegally. A right to restrict personal data processing arises where the accuracy of the personal data is contested by the data subject; or when further processing is unlawful or outside the scope of the original consent.

One concern about the new GDPR regime is the potential disparity between data collection laws from one member state to the next. While the GDPR applies uniformly to all EU member states by virtue of their membership, and legal uses of data are set out in Article 6, (by consent, to perform a contract, for legal obligations or public interest tasks of the controller,), there is some wiggle room under 6(2) for individual states to further define which activities are legally permissible within its borders; it remains to be seen how Internet services that transmit data across internal borders of the EU might get entangled in those legal differences from one country to the next.

Data transmission and storage have increased considerably with the new mobility of messaging and the novel features offered on cell phones and tablets. With such major shifts in the portability of data, and the unconstitutionality of the US-EU safe harbour arrangements as decided by the CJEU in the *Maximillian Schrems* case,[60] the EU-US Privacy Shield has come into effect. Its emergence and importance for reputational privacy will be discussed below.[61]

---

59. *Id.* at art. 17 and 18 respectively.

60. Maximillian Schrems v. Data Protection Comm'r, Case C-362/14, 6 October 2015 (Schrems I).

61. As early as 1999 the ARTICLE 29 Working Party, a group of European data protection officials, was of the opinion in 1999 that the "patchwork of narrowly focused sectoral laws and voluntary self regulation [of US data transmissions] cannot be relied upon to provide adequate protection in all cases for personal data transferred from the European Union." WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, Opinion 1/99 concerning the level of Data Protection in the United States and the Ongoing Discussion between the European Commission and the United States Government, at p. 4, DG MARKT DOC 5098, WP 15 (Jan. 26, 1999).

4. E-Privacy Protection in Europe

Two additional EU directives relate expressly to online information and aim at protecting personal reputation. *The Electronic Commerce Directive*, (e-Commerce Directive 2000)[62] provides legal certainty for EU businesses and consumers alike on issues such as information requirements for online service providers,[63] the execution of electronic contracts, and limitations of liability of ISPs.[64] Under the e-Commerce Directive, ISPs are subject to the law of the Member State in which the service provider is established. In turn, the Member State whose residents receive the service cannot arbitrarily restrict incoming services.[65]

The second directive influencing online personal data is the *Directive on the Retention of Data* (e-Privacy Directive)[66] that relates to publicly available electronic communications or public networks, such as mobile phone and texting data plan companies. The Directive requires those companies to store citizens' telecommunications data for a minimum of 6 months and a maximum of 24 months, to allow for official scrutiny by government agents if authorized by law, and is intended to curb data retention beyond an individual's original consent. The e-Privacy directive enables the police and security agencies to access details such as the IP address and time of use of every email, phone call and text message sent or received. A 2014 decision of the Court of Justice of the European Union (CJEU), *Digital Rights Ireland Ltd. v Ireland & Karntner Landesregierng & others*, ruled certain provisions of the e-Privacy Directive unconstitutional in that they are so broad as to permit mass surveillance by state authorities that challenge fundamental human rights.[67]

---

62. Directive on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce) (EC) No. 2000/31 of June 8, 2000, O.J. [hereinafter e-Commerce Directive].

63. For example, agents who receive tax information filed online.

64. *The EU Single Market: E-Commerce Directive,* EUROPEAN COMMISSION, http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm (last updated Mar. 20, 2014).

65. *Id.*

66. Directive on the Retention of Data Generated or Processed in Connection with the Provision of Publically Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC (EC) No. 2006/24 of 15 March 2006, O.J. [hereinafter ePrivacy Directive].

67. Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd. v Ireland & Karntner Landesregierng et al., 2014 E.C.R. (April 8, 2014) (seeking preliminary ruling on ePrivacy Directive (OJ 2006 L 105, p. 54) in the light of Articles 7, 9 and 11 of the CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION [Digital Rights Ireland]).

In conclusion, throughout the 20th century European efforts to protect reputation produced a centralized body of statutory law that, as we will see below, contrasted with developments in America.[68] The persistent influence over the ages of the Roman law of *ius natural* or natural justice can be seen as an enduring theme in harmonizing laws requisite for the formation of the EU. Today, Europeans continue to look to EU statute law to protect their fundamental interests in reputational privacy.

The rights status granted to reputation in several international conventions has not been readily reflected in the state laws or jurisprudence of individual EU Member States. One explanation might be that rights to privacy have historically been addressed through actions for civil and criminal defamation, breach of confidentiality and insult law, precedent that has undergone a particular uneven history in terms of its conceptual development, its location in public or private law, and the requisite evidentiary standards of proof for a claim in either civil or criminal law.

Gradually, the courts of the EU have acknowledged protection of reputation as a full status right. Most recently, the results of the *Schrems* and *Digital Rights Ireland* cases have signaled CJEU heightened concerns over data privacy during transatlantic transmission of data pertaining to EU citizens. That transmission has been accelerated by innovative technologies that have enabled wireless transmission, digital messaging and government data surveillance, all of which have implications for reputation rights.

C. Domestic Responses in the US Relative to European Nations

Concern for reputational privacy and data protection has moved in a very different direction in the US than in Europe.[69] There is no mention of "reputation" in the US Constitution, although freedom of speech figures prominently in the First Amendment and privacy in the Fourth. Neither is there is any federal data protection law, and individual privacy rights were not recognized in federal law until the *Privacy Act 1974,* despite a proposal for one by Warren and Louis

---

68. Paul M. Schwartz and Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?* 98 CALIF. L. REV. 1925, 1947 (2010).

69. The US Constitution is silent on reputation rights, although case law on free speech has obliquely created legal parameters for protection of personal reputation. *See further for historical perspective,* George C. Christie, *Injury to Reputation and the Constitution: Confusion And Conflicting Approaches,* 75 MICH. L. REV. 43 (1976).

Brandeis near the close of the 19th century.[70] State privacy laws have evolved to fill the legislative gap in a sector-specific and *ad hoc* fashion that creates doctrinal and procedural discrepancies between one state and another regarding, for instance, public laws in health, industry and insurance. In the absence of statutory guidelines, the common law has developed, albeit with uneven results. The development of data protection laws has followed a similar course.

For reputational damage perpetrated onto another, the common law offers defamation law, privacy law and, under the influence of UK practices, breach of confidentiality.[71] US causes of action tend to focus on loss of social esteem and goodwill or a loss of social capital in economic terms. In contrast, legal principles of continental Europe, reflected in the ECHR and other statutes, tend to link reputation to one's dignity or honor among peers. To defame that dignity is to challenge the positive public appraisal of the person; to damage another's honor is to mar the self-appraisal of his own public significance.[72]

In Harvard Dean William Prosser's estimate, the common law of defamation is full of "absurdities for which no legal writer ever has had a kind word."[73] Without going into detailed case analysis, the following principles indicate the intricacies and inconsistencies of defamation jurisprudence that bear out Prosser's assessment. In the US, truth is accepted as an absolute defense in some state jurisdictions, but not in others.[74] Truth is not accepted as a defense in privacy invasion cases that involve damages to reputation. A statement does not need to be literally true in order for this defense to

---

70. Privacy Act of 1974, 5 U.S.C. § 552a (Publ. L. No. 93-579), 88 Stat. 1896 (31 Dec. 1974); *see further,* Louis Brandeis & Samuel Warren, *The Right to Private Property*, 4 HARV. L. REV. 193 (1890).

71. A case for defamation should exhibit the following elements: the publication to third parties of a harmful statement about the plaintiff that causes her public embarrassment and/or professional and financial suffering, and is made without adequate research into the truthfulness of the statement. When those elements are present, and the plaintiff is reduced in the social estimation of her community as a result, a private case in defamation is usually made out at common law.

72. Defamation and Freedom of Expression, COUNCIL OF EUROPE, MEDIA DIVISION, DIRECTORATE GENERAL OF HUMAN RIGHTS (March 2003). In addition, the *French Press Act of 1881* remained faithful to the spirit of the 1789 *Declaration of the Rights of Man and of Citizens* that proclaimed the freedom of the press "save to respond to the abuse of this liberty, in the cases determined by the law", ie to defamatory statements (art. 11). *For American-European cultural differences in perceptions of privacy, see* James Q. Whitman, *The Two Western Cultures Of Privacy: Dignity Versus Liberty*, 113 YALE L. J., 1151 *passim* (2004).

73. WILLIAM PROSSER, HANDBOOK OF THE LAW OF TORTS, 737 (4ed. 1971).

74. *Cf.* a claim for invasion of privacy in the US where truth provides no defense.

be effective, just substantially true in the legal sense. This means that even if the defendant states some facts that are false, if the "gist" or "sting" of the communication is substantially true, then the defendant can prevail.[75] A plaintiff who is a public official or celebrity must prove both falsity and malice on the part of the defendant.[76] The US Supreme Court has held that private individuals can secure a remedy in defamation simply by proving negligence, as opposed to a higher standard of intent on the part of a media defendant.[77]

Similarly, a 2015 study of EU civil defamation laws regarding how helpful they are to journalists, concluded that most were unclear and confusing and that, when writing for publication, "vagueness is the name of the game" to escape civil liability.[78] Only Ireland, Macedonia and the UK were named as having passed legislation specific to defamation that reasonably conforms to international standards and that would assist journalists.[79]

Further confusion has been experienced in both Europe and the US over criminal defamation laws that use penal sanctions to respond to insults, criticism and defamatory behavior involving public officials and heads of state. Such laws are remarkably widespread: nearly 20 US states retain criminal defamation laws;[80] within the EU, 20 member states have retained criminal defamation laws on their books despite persistent pressure to repeal them.[81]

The development of privacy law in America in response to reputational injury was much more meticulous in its taxonomy due in

---

75. Gomba v. McLaughlin, 180 Colo. 232, 236 (Colo. 1972).

76. New York Times Co. v. Sullivan, 376 U.S. 254, 285-292 (1964). Sullivan did not prevail, as he could not establish that the statements were made with actual malice or that they related to him.

77. Gertz v. Welch Inc., 418 U.S. 323 (1974).

78. . Scott Griffen*, OUT OF BALANCE: Defamation Law in the European Union: A Comparative Overview for Journalists, Civil Society and Policymakers,* http://legaldb.freemedia.at/wp-content/uploads/2015/08/IPI-OutofBalance-Final-Jan2015.pdf (providing a comparison of defamation laws in EU states).

79. The study also notes that Austria, Croatia and Luxembourg have passed general media legislation that specifically addresses defamation and provides most relevant defenses.

80. David Pritchard, *Rethinking Criminal Libel: An Empirical Study,* 14 COMM. L. & POL'Y, 303 (2009) (listing Colorado, Florida, Idaho, Kansas, Louisiana, Michigan, Minnesota, Montana, New Hampshire, New Mexico, North Carolina, North Dakota, Oklahoma, Utah, Virginia, Washington, Wisconsin, Puerto Rico and the US Virgin Islands as having criminal defamation laws). Colorado repealed its criminal defamation laws in 2012.

81. *Defamation Laws in Europe - Media Laws Database,* INTERNATIONAL PRESS INSTITUTE, http://legaldb.freemedia.at/defamation-laws-in-europe (last visited April 8, 2016) (listing only Cyprus, Montenegro, the United Kingdom, Ireland, Romania, Macedonia and Estonia as having repealed criminal defamation laws).

large measure to William Prosser. He devised an intricate inventory of laws to address not only invasions into personal seclusion but such wrongs as appropriation of the name of another, public disclosure of private facts "not a matter of legitimate public concern", and disclosure of private facts that portray the victim in a false light.[82] The law of privacy in America thereby veered away from the European model, including the law of confidentiality, to create a new conception of privacy based on the individual's "inviolate personality."[83]

Prosser's work has been criticized as too regimental in its categorization. For victims of reputational exposure, his privacy torts present a confusing and often illogical combination of legal principles and practices. For example, they contain such arbitrary inclusions as the "right of publicity" (that protects a celebrity's intellectual property from misappropriation and hence financial deprivation) within the "appropriation" category (that protects the private person from the emotional harm of unwanted publicity). To some, such results produce contrivances that do not work well in practice.[84]

Most controversial are the uneven results played out in court. For example, false light claims are recognized in only about two-thirds of US states due to their doctrinal overlap with defamation actions. There are distinctions, however, that justify Prosser's inclusion of both torts. For instance, false light actions are not subject to limitation and retraction statutes unlike defamation actions. In terms of substantive differences, false light claims have no access to defenses available to the press in defamation actions: while truth is a complete defense to defamation, true statements are actionable under false light law.[85] Journalists must therefore be particularly wary of attracting false light claims because defendants can be successful even if the story is true in its entirety.[86]

---

82. William L. Prosser, *Privacy,* 48 CAL. L. REV. 383 (1960).

83. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy,* 98 CALIF. L. REV. 1887 *passim* (2010).

84. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality,* 96 GEO. L. J., 123, 125 (2007) (arguing that Warren and Brandeis did not invent the law of privacy from meager precedents of the common law but took it in a new direction).

85. Patricia Avidan, *Protecting the Media's First Amendment Rights in Florida: Making False Light Plaintiffs Play by Defamation Rules,* 35 STET. L. REV. 227 (2005).

86. *See, e.g.*, Gannett Co. v. Anderson, 947 So. 2d 1 (Fla. Dist. Ct. App. 2006) (where the owner of a road-paving company was awarded $18.28 million for a true report that he had shot his wife but that provided a statement that the authorities ruled the shooting accidental *two sentences after* the original mention of the shooting, thereby putting his name in a false light.

As well, false light requires the dissemination of offending content to a wide audience, whereas defamation claims can rest on the perceptions of a smaller number of recipients. The principal doctrinal difference rests in the interest the law seeks to protect: defamation protects the objective interest of reputation while false light protects the subjective interest of emotional injury causing personal embarrassment, helplessness or mere hurt feelings.[87] The conceptual vagueness of those terms has prompted journalists to complain about the tort's chilling effect on their First Amendment rights.[88]

Those transatlantic discrepancies in legal responses to reputational privacy threats exist within a broader nationalization trend that illustrates state authorities are beginning to take more notice of the risks of exporting their citizens' personal data. In Europe, for example, German's privacy federation has threatened to sue US-based Pokemon-Go developer Niantic Labs for over 15 violations of German privacy law;[89] and in France, the data protection regulator CNIL[90] fined Google for failure to conform on a global scale with the "right to be forgotten" as ruled by a 2014 ECJ judgment.[91]

In the US, libel chill has been addressed with passage of the SPEECH *Act*[92] that renders unenforceable any foreign defamation judgment against US journalists unless they are consistent with US laws and procedures, including the First Amendment, section 230 of the *Communications Decency Act*[93] and US standards of due process. In other words, foreign judgments must be "consistent with that which a US court would have reached on the facts, if the defamation

---

The decision was overturned on appeal in Anderson v. Gannett Co., 994 So. 2d 1048 (Fla. 2008)).

87. *Getting It Right, But in a "False Light,"* REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, http://www.rcfp.org/browse-media-law-resources/digital-journalists-legal-guide/getting-it-right-false-light-0 (pointing out that some states hold that false light claims can concern untrue *implications*, not directly false statements).

88. Thereby offending the constitutional standard that "Congress shall make no law . . . abridging *the freedom of speech, or of the press*; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." (emphasis added). U.S. Const. amend. I.

89. David Mayer, *Pokémon Go Maker Is Facing a Privacy Lawsuit Threat in Germany*, Fortune (July 20, 2016), http://fortune.com/2016/07/20/pokemon-go-germany-privacy/.

90. Commission Nationale de l'Informatique et des Libertes. Google argued it complied by scrubbing search results from its European subsidiaries (Google.fr and Google.de).

91. Kayla Haran, *France Fines Google Over Global Right to be Forgotten,* HARV.J. L. & TECH (Apr. 4, 2016), http://jolt.law.harvard.edu/digest/privacy/france-fines-google-over-global-right-to-be-forgotten.

92. *Supra,* note 2.

93. *Supra,* note 1.

had occurred in the United States."[94] Defamation is broadly defined in the SPEECH Act as "any action or other proceeding for defamation, libel, slander, or similar claim alleging that forms of speech are false, have caused damage to reputation or emotional distress, have presented any person in a false light, or have resulted in *criticism, dishonor, or condemnation* of any person."[95] The italicized inclusions harken to laws of insult in medieval Europe or present-day repressive regimes.[96]

Rules governing transatlantic export of personal data from EU countries by US Internet companies have changed considerably since the Schrems decision in 2015. With safe harbor agreements pronounced unconstitutional by the CJEU, the EU and US have had to build consensus regarding a workable balance between free speech and privacy rights for personal data transfers out of EU member states. The resulting self-certification Privacy Shield (IP/16/216) was signed in July of 2016 and governs all data flow of personal data from the EU to the US and particularly aims at commercial transactions between the two jurisdictions.[97] Salient provisions include notification to data subjects by commercial participants of the use being made of their data including third party use; mechanisms the data subject can use to access that data; and ways that the US Department of Commerce will cooperate with EU data protection authorities to facilitate claims of non-compliance by data subjects. The principles that frame the Privacy Shield mirror those of the GDPR regarding consent, notification, data retention guidelines, and publication of non-compliance actions by the appropriate authorities. As of this writing, the agreement is undergoing review by the Article 29 privacy advocacy group in Europe and privacy specialists in the US.

II. PRACTICAL HURDLES FOR PROSPECTIVE LITIGANTS

The Gordian knot metaphor suits the complex and often puzzling interplay of conceptual principles and practice outcomes in reputation

94. Emily C. Barbour, *The SPEECH Act: The Federal Response to 'Libel Tourism'*, CONGRESSIONAL RESEARCH SERVICE (Sept. 16, 2010), https://fas.org/sgp/crs/misc/R41417.pdf.

95. *Supra* note 2, at § 4101(1).

96. Ruth Walden, *Insult Laws: An Insult to Press Freedom,* WORLD PRESS FREEDOM COMMITTEE (2000), http://www.wpfc.org/site/docs/pdf/Insult%20Laws-Text.PDF.

97. Passage of the Judicial Redress Act H.R.1428 - 114th Congress (2015-2016) was a pre-condition to the agreement; it grants EU citizens the right to enforce data protection rights in the U.S. a key stipulation of the EC negotiators. *For details see* Welcome to the EU0US Privacy Shield, https://www.privacyshield.gov/welcome.

law. A layer of complexity is added to the mix by social media; it seems that features of the Internet that make it most attractive for every kind of informational exchange also contribute to a type of risk more permanent and severe than legacy journalism and what we used to call mass media. Those idiosyncrasies raise several legal and practical questions that call out for analysis. The following are key to reputational harm perpetrated online.

A. Gradients of Harm & Other Issues of Proof

> It is the remedy that bridges the gap between the ideal and the real, or, rather, between norms and fact.[98]

Tort law holds promise for reputational redress due to its focus on harm to the plaintiff rather than wrongdoing by the defendant: it looks to liability, not blame. Historically libel damages were presumed, in recognition of the reputational stigma that the written word could compel. Today, that presumption has narrowed to defamation -*per se* (obvious defamation) cases.[99] Beyond that, particularly in cases of innuendo or inducement, litigants must prove actual (or special) damages in order to recover.[100]

Innuendo can play a major part in social media defamation cases because the extrinsic facts it references add meaning to the truncated and fragmentary nature of tweets, emails or Facebook postings. That was illustrated in the 2013 London High Court case of Sally Bercow, wife of the current Speaker of the House of Commons in the United Kingdom who tweeted, "Why is Lord McAlpine trending? *innocent face,*" thereby implicating a former Conservative Member of Parliament. [101] The court found the contents were sufficient when combined with several other media accounts to link McAlpine to a child sex abuse scandal and so found for the plaintiff. The court

---

98. Helge Dedek, *From Norms to Facts: Realization of Rights in Common and Civil Private Law*, 56 MCGILL L. J. 77 (2010) (comparing the "lively" discourse in common law regarding converting rights to remedies to civil law jurisdictions where "the concept of remedy remains a mystery".)

99. *Per se* actions have historically been reserved for cases related to charges that a person has contracted a contagious or venereal disease; that a woman is of unchaste character; for other untrue statements that tend to injure a person in his profession, trade, or business; or accusations of crimes involving moral turpitude.

100. *See generally* UK Defamation Act 2013 (2013 UK Act), Chapter 26 that sets out to rebalance, rather than rewrite, the common law of defamation. It sets the requisite standard of harm at *serious* damage, thereby weeding out more trivial cases, but also doing away with the presumption of reputational harm.The defendant retains the defense of truth, but s/he must prove a statement is *substantially* true.

101. McAlpine v. Bercow [2013] EWHC 1342 (QB).

reasoned that Bercow's 56,000 Twitter followers, as well as a similar number of potential news subscribers, would comprehend the meaning of the "innocent face" (identified as a type of "stage direction or a emoticon" directing the reader to imagine that the expression on the tweeter's face is "one of innocence. . .[indicating] she does not know the answer to the question.")[102] Sufficient extrinsic value was found in the concurrent coverage of the child sex scandal by radio and print media to render Bercow's offending tweet as defamatory.

The *Bercow* case exemplifies a few novel issues of proof raised by social media cases. The High Court found that average readers of the tweet would find its tone "insincere and ironical", an observation that falls short of the traditional legal standard of falsehood of a defamatory statement but, in the instant case, contributed to evidence that found for the plaintiff.[103] Further, Bercow's reference to "trending" stories added to her liability by implicating her in several media reports produced at the same time. That finding assumes Twitter followers were necessarily aware of those news accounts and read them into Bercow's tweet, rather than dismissing the message as an "unfathomable, twitter 'in-joke'" as one source suggests.[104] An ancillary question is whether Bercow is necessarily rendered a public figure with a finding of malice added to the list of evidentiary requirements, due to the extensive readership the Twitter medium attracts.[105]

Courts exhibit reticence to acknowledge a legal expectation of privacy when dealing with social media speech as can be seen in the US where the mere creation of a Facebook account disqualified a user from such claims,[106] or a student's posting of his poem on a MySpace account convinced a school principal of his right to hand over the student's poem to the local newspaper for publication.[107]

Jurists and school personnel are not alone in their confusion over the privacy landscape for digital speech: users as well exhibit

---

102. *Id*. per Mr. Justice Tugendhat, at § 7.

103. *Id.* at § 84.

104. Hugh Tomlinson, *Case Law: McAlpine v Bercow (No.2), Sally Bercow's Tweet Was Defamatory,* INFORRM'S BLOG (May 24, 2013), https://inforrm.wordpress.com/2013/05/24/case-law-mcalpine-v-bercow-no-2-sally-bercows-tweet-was-defamatory-hugh-tomlinson-qc.

105. That question is posed with reference to US defamation law in Matthew Lafferman, *Do Facebook and Twitter make you a Public Figure? How to Apply the Gertz Public Figure Doctrine to Social Media,"* 29 SANTA CLARA HIGH TECH. L.J. 199 (2012).

106. *See, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S. 2d 650 (N.Y. Sup. Ct. 2010).

107. Moreno v. Hanford Sentinel Inc., 172 Cal.App.4th. 1125, 1130 (2009).

unfamiliarity with the scope of their audiences, as shown in US entertainer Courtney Love's insistence that she believed her offending tweet was sent directly to one recipient, not to Twitter readers at large,[108] or Sally Bercow's argument that her Twitter followers numbering in the tens of thousands should not be calculated as including those who read general news reports.

Another challenge is dealing with standards of proof for digital speech and wireless messaging tools with laws created for the era of wiretaps, radio and postcards.[109] In legal terms, jurists' cobbling of pre-Internet law onto digital speech cases has added to that confusion and led to more than a few awkward charges: for example, using trespass to chattels charges for email hacking,[110] assault by Internet,[111] and intentional infliction of emotional distress for overly expressive texts.[112] One of the most gymnastic applications of common law causes of action to social media is use of breach of confidential relationship where no prior close relationship ever existed. The practice is routinely used in the UK and exemplified in the Max Mosley case (discussed below).[113] It signals a need for better understanding of both technological capabilities of the medium and the ontological uniqueness of digital speech.

The view that novel media might require discrete legal solutions can be seen in arguments of the defense team of US entertainer Courtney Love, as discussed above. Love had tweeted to a very large fan base that Mafia members had placed illegal influence on her former lawyer. In America's first "twibel" case, the defense proposed that it is the nature of tweets to use "hyperbole and exaggeration" that are not to be scrutinized too carefully or taken as carrying deeper meaning.[114] In asking that claims made via Twitter not be held to the

---

108. Corina Knoll, Singer-actress Courtney Love wins landmark Twitter libel case, LA Times (Jan. 24, 2014), http://articles.latimes.com/2014/jan/24/local/la-me-love-libel-20140125.

109. For commentary on cultural differences regarding expectations of privacy for postcards, see also Steven D. Zansberg & Janna K, Fisscher, Privacy Expectations in Online Social Media - An Emerging Generational Divide?, Communications Lawyer (Nov. 20, 2011), http://www.lskslaw.com/documents/evolvingprivacyexpectations(00458267).pdf.

110. Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1347 (2003).

111. Marquez v. Reyes, Civil Action No. 10-cv-01281-BNB, 2010 U.S. Dist. LEXIS 65701 (D. Colo. June 10, 2010).

112. Clay Calvert, *Fighting Words in the Era of Texts, IMS and E-Mails: Can A Disparaged Doctrine Be Resuscitated to Punish Cyber-Bullies?*, 21 DEPAUL-LCA J. ART & ENT. L. & POL'Y 1, 23 (2010).

113. Mosley, *infra* at 122.

114. As referenced in Patrick H. Hunt, *Tortious Tweets: A Practical Guide to Applying Traditional Defamation Law to* Twibel *Claims,* 73 LA. L. REV. 559, 560 nn.13-14 (2013).

same legal standards as speech used by offline news organizations, Love's counsel were suggesting that the law of defamation shift to create a lesser category of speech with less stringent publishing standards when digital media are used, particularly given its unmediated status.[115]

Traditional remedies also provide a challenge in that they might prove impractical for digital speech cases where the majority of defendants are citizen journalists without deep pockets. In a pre-Internet study, the most sought-after defamation remedy was pecuniary,[116] even though plaintiffs admitted to its lack of effectiveness in meeting litigants' expectations.[117] The damage award for super model Naomi Campbell, for example, after several years of litigation in three levels of court and a widening circle of negative publicity, was a nominal £3,500.[118] By 2010, however, an Iowa study reported that the preferred solution was retractions, a possible reflection of social media users' realization that much wider audiences would access an online retraction or apology notice than when traditional media are used. Internet scholar David Ardia also points to the deterrence provided by the growing capricious nature of damage awards on both sides of the Atlantic.[119] Other recent remedies for defamation have included containment through injunctions[120] and erasure mechanisms contained in some US and EU laws promoting *le droit l'oubli,* a personal right to be forgotten.

---

115. *See* Hunt, *supra* note 114, 559 *passim* (arguing that Twitter is a revolutionary communications platform in that it enables, for the first time in modern communications, participation of the average citizen with celebrities, major news networks, and politicians).

116. Damage awards are customarily allocated in two categories, compensatory (or actual) damages and punitive damages (known as exemplary damages in Cyprus, England and Wales where they are extremely rare). There are other modifying terms placed in front of the word damages like "liquidated damages," (contractually established damages) and "nominal damages" (where the court sets a figure to reprimand the defendant, such as awards of one dollar).

117. Randall Bezanson, *Libel Law and the Realities of Litigation: Setting the Record Straight*, 71 IOWA L. REV. 226, 227 (1985).

118. Campbell v. MGN Ltd, [2004] UKHL 22, [14] (Eng.), 2 A.C. 457.

119. David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. CIV. RTS-CIV. LIB. L. REV. 261, 262 (2010). In the US, large damages continue to be awarded to a small number of plaintiffs.

120. David S. Ardia, *Freedom of Speech, Defamation, and Injunction*s, 55 WM. & MARY L. REV. 4 (2013) Note 15 (reporting that of fifty-six decisions involving injunctive relief in US defamation cases well over half were found to have been delivered since 2000 and over half by separate calculation, involved Internet speech. As well, the nature of injunctive relief awarded has been either disproportionate to the harm threatened or technologically infeasible).

The erasure remedy is highly controversial within the common law world as it represents a category of solutions that pose technological difficulties when dealing with online content. [121] In the Lord McAlpine case, above, the British peer sought damages against a number of "high profile Tweeters," identified as users with more than 500 followers, who retweeted Bercow's message, thereby enabling further third party dissemination of the original message. The anonymity of many citizen journalists would pose a further impediment to such remedies.

Calculating a gradient of harm for different ways to offend reputational privacy online is a complex undertaking: how does one prove damages given the *uber* accessibility, archiving capabilities and ongoing third party dissemination capabilities afforded by social media technologies? Nonetheless, some high profile figures have pursued litigation and have attempted to articulate damages and the further harm to reputation they or their families have suffered as a result of going to court. For example, wealthy lawyer and auto racing figure Max Mosley, the subject of online dissemination of images by News of the World in a fictitious media story of a Nazi-themed sex party,[122] spoke of "enormous and continuous damage"[123] that became "totally devastating" for his wife of 48 years and his sons for whom he could think of "nothing more undignified or humiliating."[124] Although successful in the originating jurisdiction, Mosley then faced mirror actions in 22 countries due to the replicative nature of online content, and at great personal cost.

Similar issues faced American single mother Lorraine Martin who sought enforcement of a Connecticut erasure law for arrest news of criminal charges against her that were ultimately withdrawn. She describes the nightmarish realities of job searching in the shadow of such headlines as "Mother and sons charged with drug offenses."[125] As well, plaintiff Gonzales in the *Google Spain* case, discussed further below, found employment and social opportunities were

---

121. Bill Keller, *Erasing History*, NEW YORK TIMES (Apr. 28, 2013), http://www.nytimes.com/2013/04/29/opinion/keller-erasing-history.html?_r=0.

122. Mosley v. News Group Newspapers Ltd. [2008] EWHC 687 (QB).

123. *Max Mosley Wins His Case Against Google in France*, COLLYERBRISTOW.COM (Nov. 6, 2013), http://www.collyerbristow.com/news/press-release-max-mosley-wins-his-case-against-google-in-france.

124. *Mosley Wins Court Case Over Orgy*, BBC NEWS (July 24, 2008), http://news.bbc.co.uk/2/hi/7523034.stm. Mosley also spoke of his elder son's suicide during proceedings.

125. Keller, *supra* note 121.

denied him due to persistent online accounts of his previous debt to social services authorities that cropped up each time he Googled his name.

One source cites the disparities in litigation outcomes as proof of need for a more contextual or nuanced approach: "common law courts attach extremely divergent legal consequences to impugned statements based on indefensibly broad generalizations about the degree of danger to personal reputation posed by the medium in which the statement was communicated."[126]

B. Jurisdiction & Choice of Law

Personality rights have been described as one of the most contentious areas of private international law[127] in that the instant personal data or defamatory content crosses national borders the issue of a multistate conflict of laws arises.[128] Such magnified exposure creates two immediate legal decisions for a plaintiff: where to sue and under which law. For those who find their privacy exposed by unauthorized use of their personal data, those questions are not easily answered. For EU victims, national data protection agencies are the first step, with subsequent judicial review provided by the CJEU; for US victims, the answer involves a sector-by-sector review of available legal remedies.[129]

Given the unique architecture of Internet communications, such reputational harm now crosses borders widely, instantaneously and far more frequently. That activity brings the non-European website operator within the four corners of two EU legal instruments: the

126. Robert Danay, *The Medium is not the Message: Reconciling Reputation and Free Expression in Cases of Internet Defamation*, 56:1 MCGILL L.J. 1, 1 (2010).

127. Csongor Istvan Nagy, *The Word is a Dangerous Weapon: Jurisdiction, Applicable Law and Personality Rights in EU Law – Missed and New Opportunities*, 8 J. PRIVATE INT'L. L., 251, 253 (2012).

128. *See also* Tamas Dezlo Czigler, *Choice of Law in the Internet Age: US and European Rules,* 53 HUNGARIAN J. LEGAL STUD. 193 (2012).

129. For example, the national Privacy Act, 1974 could be invoked for privacy breaches caused by federal civil servants; the Electronic Communications Privacy Act 1986 updates the Federal Wiretap Act of 1968, addressing concerns originating over wiretapping but now extended to protect wire, oral, and electronic communications; children's personal data exposure could involve the Children's Online Privacy Protection Act (COPPA); and the federal Department of Health and Human Services (HHS) addresses health data breaches by federal employees.

Brussels I Regulation[130] (Brussels I, governing the jurisdiction for hearing transborder civil matters) and the *Rome II Regulation*[131] (Rome II, addressing the choice of laws that will apply to non-contractual obligations). The third instrument, the *E-Commerce Directive*, is also involved in data transfer as it addresses publication of information on the Internet, particularly the issue of whether an ISP functions as a "mere conduit" or a controller of such information. What becomes important under Brussels I is not the location or domicile of the plaintiff but that of the defendant and, due to the variety of recognized exemptions, the geo-location where harm is experienced.[132]

With respect to reputational disputes, Rome II has been a most anticipated mechanism for clarifying "all matters relating to privacy and personality rights, including defamation."[133] It marks an effort by the EU to coordinate judicial decision-making regarding the import and export of online information of citizens within its member states. Such harmonization could reduce or eliminate forum shopping for plaintiffs.

Unfortunately for legal clarity and predictability, defamation law is not included in the provisions of Rome II at present, withdrawn at the eleventh hour due to a flood of protest from the publishing industry as well as a lack of consensus between the European Commission and the Council of Europe.[134] Negotiations continue.[135]

Brussels I, with provisions addressing non-contractual conflicts involving torts and including the media, holds that jurisdiction is to be

---

130. Council Regulation (EC) No. 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, O.J. (L 012) [hereinafter Brussels I].

131. Council Regulation (EC) No. 864/2007 of 11 July 2007 on the Law Applicable to Non-contractual Obligations, O.J. (L 199/40) [hereinafter Rome II].

132. For a more detailed analysis of Brussels I, *see The Brussels I Regulation (No 44/ 2001)*, Ch. 1, DUTCH CIVIL LAW, http://www.dutchcivillaw.com/content/brusselsone011.htm (last visited April 8, 2016).

133. On July 11, 2007 the European Parliament and the Council adopted the 'Rome II' Regulation on the law applicable to non-contractual obligations (OJ L 199, 31.7.2007, p. 40). Under Article 1(2)(g), 'non-contractual obligations arising out of violations of privacy and rights relating to personality, including' are excluded from the Regulation's scope.

134. Symeon C. Symeonides, *Rome II and Tort Conflicts: Missed Opportunities,* 56 AM. J. COMP. L. 173 (2008).

135. Jan-Jaap Kuipers, *Towards a European Approach in the Cross-Border Infringement of Personality Rights*, 12 GERM. L. J. 1681, 1697 (2011), (describing thirteen options for violations of privacy and personality rights discussed in preparatory meetings of the Rome II committee).

exercised by the EU country in which the defendant is domiciled, regardless of his/her nationality.[136] In the case of legal persons, domicile is the country where they have their central administration or principal place of business. For Google Inc., for example, domicile could be Mountain View, California but if the suit involves an individual plaintiff domiciled in France, the matter could involve Google France and hence a French court. Brussels I also provides that jurisdiction can be determined by the "place where the harmful event occurred."[137] That provision complicates the issue by creating a number of possibilities along the chain of causation. In the German case of *Bier BV v Mines de Potasse d'Alsace*, the CJEU interpreted that clause to mean either the domicile of the defendant who posted the defamatory content or the domicile of the plaintiff who suffered the resulting publicity.[138] That interpretation was made in pre-Internet days, however, when points along the causal chain were more easily identified.[139]

More recently, the CJEU took the opportunity to address the "Gordian knot" that the jurisdiction and choice of law issues have become in defamation and invasion of privacy cases with the enjoined Internet cases *eDate Advertising* and *Oliver Martinez*.[140] The claimants alleged that their personality rights had been infringed as a result of online publications on websites that were based in different EU Member States than those in which they lived. In *eDate Advertising,* the plaintiff was a German national and resident that had been convicted of murdering a well-known actor in 1993 and released on parole in 2008.[141] He complained that the Austrian website publisher *eDate Advertising*, infringed his personality rights by reporting his full name, conviction for murder, and the fact that he

136. Brussels I, *supra* note 132, at art. 2.

137. *Id.* at art. 5(3) for all torts (non-contractual matters).

138. Case 21/76, Bier BV v. Mines de Potasse d'Alsace, 1976 E.C.R. 1735 [BIER]. *See generally* Nagy, *supra* note 127.

139. The *Bier* issues were revisited in 1996 CJEU cases of *Shevill v Presse Alliance SA*. *See* Case C-68/93, Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v. Presse Alliance SA, 1995 E.C.R. I-415 (determining that harm occurs where the defamatory material is accessed or read (offline newspapers in this case), not where the publisher is headquartered or where the plaintiff is located when discovering the offending content).

140. Joined Cases C-509/09 & C-161/10, eDate Advertising v. X and Olivier Martinez & Robert Martinez v. MGN Limited, 2011 E.C.R. I-10269.

141. *Id.*

was appealing his conviction.[142] The Bundesgerichtshof or Federal Court of Justice for Germany asked the CJEU for a preliminary ruling on the applicability of Brussels I regarding jurisdiction and the enforcement of judgments in civil and commercial matters[143] as well as the e-Commerce Directive relating to matters of tort published on the Internet.[144]

In the companion case *Martinez,* the French actor Olivier Martinez complained of an infringement of his privacy and of the right to his image by the UK-based Sunday Mirror website in an article entitled"Kylie Minogue back with Olivier Martinez." The online coverage used a dated photograph to erroneously suggest Martinez had reunited with a former girlfriend.[145] Domestic courts faced arguments from the commercial defendants that the court did not possess authority to make orders restricting publication outside their jurisdictions.

The CJEU confirmed for both cases that infringement of personality rights by Internet can be litigated either in the EU Member State where the publisher is established or where the plaintiff's "centre of interests" is based, a finding that did not bring clarity to existing law.[146] The decision acknowledged that the law of conflict might not be of much assistance within the unique context of Internet communications because Internet distribution is "universal," "intended. . .to ensure the ubiquity of that content," and calls into question the whole "centre of interests" concept.[147]

The decision in *eDate Advertising* and *Oliver Martinez* acknowledges the borderless nature of the Internet but does little to simplify the law for its extraterritorial transmission of data; it underscores the need for innovative thinking when it comes to online behavior.

C. The Half Life Debate

Much literature addressing new media communications has us believing that reputation-damaging postings are permanent or at least

142. Nagy, *supra* note 127, at 252-253 (acknowledging that personality rights and privacy are much broader concepts than libel and defamation and might cover, for example, the right to human dignity, bodily integrity, and private communications).

143. *Id.* at note 43.

144. *Id.* at note 28.

145. eDate Advertising, *supra* note 140.

146. *Id.* at § 48.

147. *Id.*

highly persistent and accessible.[148] The "right to be forgotten" raised by the European Commission in the context of both extant and pending data protection legislation advocates recognition of a human right to delete personally damning content and past social mistakes that pervade online spaces with an "iron memory."[149] The concept can be seen as both "intuitive and widely appreciated" in European thinking and lawmaking;[150] so too in America, given the ethos of second chances from which the new nation was forged.[151] Hence there is potential for deeper and more enduring harm than with offline defamatory statements because of protracted access to personal data by an expanded audience. Internet users, particularly young ones, receive ample warnings of the permanence of online memory from industry, educators, and family.[152] Bert-Jaap Koops warns of apprehension or that "distinct feeling of unease" provoked when suddenly data from the past re-emerges in unexpected contexts.[153]

In contrast, several digital-savvy scholars maintain that online content is short-lived. They speak of the evanescence of texting and SNS communications, a concept that "eases the force of a blow" of defamation.[154] Among proponents of the half-life debate is Harvard history scholar Jill Lepore who assesses the Web as ethereal, unstable and unreliable. She cites two studies that offer empirical proof of the transience of online academic sources. In the first, a 2013 survey of legal policy-related journals identified a near-fifty percent loss in workable URLs over six years.[155] The second study, at Harvard Law School, found over 70% loss of URLs cited in the *Harvard Law Review* and other journal articles, as well as a 50% attrition of URLs within US Supreme court opinions. Lepore notes the frequency with which the error message "Page not Found" is the result of our online search efforts and concludes, "[s]ocial media, public records, junk: in

148. *See also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 8 (2004).

149. Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice'* 8 SCRIPTed 1 (2011).

150. *Id.* at 2.

151. LAWRENCE FRIEDMAN, GUARDING LIFE'S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY *passim* (2007).

152. Mike Lata, *Snapchat Tells FTC That Your Private Photos Never Actually Got Deleted,* TECHTIMES (May 12, 2014), http://www.techtimes.com/articles/6853/20140512/snapchat-image-sharing-images-photos-videos-fcc-privacy-online-privacy.htm.

153. Koops *supra*, note 149, at 2.

154. Anita Bernstein, *Real Remedies for Virtual Injuries*, 90 N.C. L. REV. 1457 (2012).

155. Jill Lepore, *The Cobweb: Can the Internet Be Archived?* THE NEW YORKER (Jan. 26, 2015), http://www.newyorker.com/magazine/2015/01/26/cobweb.

the end, everything goes."[156] Both of those studies relate half-life to the amount of time that content remains accessible and functionally useful while online.

Also promoting an evaporation theory are computer engineers Daniel Gomes and Maroi Silvia. Their 2006 study suggests that, in that year, just over half (55%) of content remained online after one day, 41% after a week, 23% after 100 days, and 15% after a year.[157] Meg Angelo of Georgetown University in turn suggests that "information is not permanent, no matter the medium" and calls for principled information storage practices.[158] She attributes disappearing content more to technological malfunctions such as media and hardware errors, software failures, network service failures, component obsolescence, operator errors, natural disasters, internal and external attacks, and organizational failures.[159] In the end, the half-life debate is of little comfort to reputational privacy victims whose exposure endures long after their usefulness or authorization has expired.[160]

D. The Attribution Problem

Attribution can be defined as the identification of users or data subjects through their online data. Anonymity defeats attribution attempts. Identifying who comprises the plaintiff's online community is algorithmically challenging with the use of widespread anonymity and third party dissemination.[161] Messages and images are accessed by persons who never have, or probably never will, meet the plaintiff or speak the same language. That open availability of content is assisted by permanent archiving capabilities and low entry costs of the medium.

Anonymity is used for two principal reasons, to protect the privacy of the data subject and to avoid responsibility for one's online behavior. Our vulnerability to invasive technology at the hands of the

---

156. *Id.*

157. Daniel Gomes & Mario J. Silvia, *Modeling Information Persistence on the Web*, PROCEEDINGS OF THE VI INTERNATIONAL CONFERENCE ON WEB ENGINEERING, 1 (2006).

158. Megan Angelo, *You Are What Google Says You Are,* WIRED (November 2, 2009), http://www.wired.com/business/2009/02/you-are-what-go/.

159. *Id.*

160. Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, 2014 E.C.R. 317 [hereinafter Google Spain] (reporting the offending news account remained online for 16 years before the CJEU ordered it removed).

161. *See generally* Amy Kristin Sanders, *Defining Defamation: Community in the Age of the Internet,* 53 COMM. L. & POL'Y 231 (2010).

state is accelerating at an alarming pace in the digital era. Through use of deanonymizing technology and the combination of seemingly discrete bits of information,[162] data analysts can pierce the public/ private divide we believe we enjoy as citizens of a democratic state. For example, we have been told that our gender and sexual preferences can now be ascertained from a mere examination of our use of the "like" function on Facebook.[163] Similarly we have been alerted that we are only four mobile phone conversations away from government identification.[164]

In addition to increasing surveillance capabilities of many governments, we are learning that much personal data sold to commercial advertisers is not anonymized before being sold.[165] The degree of anonymizing becomes a critical factor in determining what is "personal data," "personally identified information," or "personally identifiable information" when constructing privacy or data protection legislation.[166] Those definitions, and hence the type of data that is regulated, differ from one country to the next, making consensus on privacy standards and anonymity a complex objective.

E. Legal Immunity of ISPs

1. The Communications Decency Act Meets Google Spain

Legislative and judicial treatment differs on each side of the Atlantic regarding the legal accountability of ISPs for harmful content they distribute or invasive data retention practices they employ.[167] In

---

162. Daniel Solove, *Justice Scalia's Dossier: Interesting Issues About Privacy and Ethics*, CONCURRING OPINIONS (April 29, 2009), http://www.concurringopinions.com/archives/2009/04/justice_scalias_2.html.

163. Rebecca J. Rosen, *Armed with Facebook 'Likes" Alone, Researchers Can Tell Your Race Gender and Sexual Orientation*, THE ATLANTIC (March 12, 2013), http://www.theAtlantic.com/technology/archive/2013/03/armed-with-facebook-likes-alone-researchers-can-tell-your-race-gender-and-sexual-orientation/273963/.

164. Matt Warman, *Online Anonymity: Impossible After Four Phone Calls*, THE TELEGRAPH (Mar. 25, 2013), http://www.telegraph.co.uk/technology/news/9952841/Online-anonymity-impossible-after-four-phone-calls.html.

165. *See also* Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011) (holding that a Vermont statute that restricted the sale, disclosure, and use of records that revealed the prescribing practices of individual doctors violated the First Amendment).

166. Paul M. Schwartz & Daniel L. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information,* 85 N.Y.U. L. REV. 1814 (2011).

167. This area of law is in flux in both the US and EU, generating a large body of litigation for the courts and government watchdogs such as the Federal Communications Committee in America and the International Telecommunications Union in Europe. US Internet service providers maintain either that their role is as intermediary between those who post the content

Europe, the ECHR provides the doctrinal basis for protection of personal privacy and the sanctity of family life; human rights case law applies those principles as adjudicated by the ECtHR. EU data privacy regulation and policies, such as detailed in GDPR, require data controllers to provide data subjects with unambiguous notice of what information is being collected, why it is gathered, and who will be able to access it. Those laws inform domestic law in each EU Member State, although front line decisions regarding ISPs rest in the hands of national data protection agencies.

The European formal position, then, is that operations of Internet companies that involve their citizens be subject to rigorous laws of anti-competition, data protection, and content liability. The *Google Spain* decision identified ISPs and Internet content hosts as controllers of content with legal liability and pro-active responsibilities regarding privacy-sensitive content.

US judges are far less likely than their European counterparts to find Internet companies or ISPs liable for the hosting and distribution of defamatory content due to First Amendment protections and the sweeping immunity afforded by the *Communications Decency Act.* Section 230 of that law provides that "[n]o provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider."[168]

Such wording broadly exempts from liability any linking or other exchange of online content between service providers, leaving the regulation of online privacy to individual users through "click-wrap agreements."[169] Those contracts, unwieldy in length and complexity, grant individual access to websites and applications and hence various Internet content. Their terms are non-negotiable from

---

(publisher) and the subject of the content (individual user), or that they are data processors under an agency arrangement with the publisher. EU data regulations define a processor as a "separate legal entity with respect to the controller who process [sic] personal data on his behalf" while a controller is any body that "determines the purposes and means of the processing of personal data." Opinion 1/2010 on the Concepts of "Controller" and "Processor," Working Party Document 169, ARTICLE 29, DATA PROTECTION WORKING PARTY (Feb. 16, 2010), *available at* http://ec.europa.eu/justice/data-protection/index_en.htm.

168. *Supra* note 1.

169. The compulsory clicking of "I agree" to terms of service in order to access a particular site or service. *See also* Ryan J. Casamiquela, *Contractual Assent and Enforceability: Cyberspace*, 17 BERKELEY TECH. L.J. 475, 475–76 (2002) (detailing numerous contract court decisions from the 1990s and early 2000s). *See* Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Layers of Big Data*, 31 SANTA CLARA HIGH TECH. L.J. 483 *passim* (2015).

the user's perspective. Unacceptable terms can be dealt with by non-participation in the service or registering complaints with the Federal Trade Commission (FTC) about deceptive practices. Although the Federal Communications Commission (FCC), the other major US agency involved in the regulation of online activities, embarked upon a strategy in 2015 to centralize requirements for ISPs regarding Do Not Track mechanisms, industry response has been uneven and self-regulation remains the business practice for now.[170]

More broadly, US privacy law is regulated through sector-specific federal and state laws. Consequently, a consent-based regime links users to primary parties but does little to reveal subsequent use of their data and what that consent truly entails.[171] The Matthew Drudge case illustrates that even active participation by an ISP can garner protection within US jurisprudence.

Matthew Drudge is an Internet gossip columnist,[172] most noted for breaking the President Clinton-Monica Lewinski story. He was contracted to America On-Line (AOL) for a series of news stories he posted on an AOL enabled website that were distributed by email to subscribers. The Drudge Report promoted itself as a particular species of new media: a US-based "news aggregator."[173] The AOL, as ISP for those columns, had the right to remove content under its standard terms of service, and arguably could be considered an editor or controller of content for its active involvement in the selection of material to publish. Drudge posted the gossipy content, which provided links to other articles and sources of news. In one such story Drudge reported domestic abuse by Sidney Blumenthal, a prominent member of President Clinton's administration.[174] Blumenthal sued both Drudge and AOL for defamation. By invoking section 230 of the *Communications Decency Act* and disavowing any activities as

170. In general, the FCC oversees Internet infrastructure while the FTC regulates content. There is some confusion of roles when dealing with net neutrality.

171. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM L. REV. 583, 587 (2014).

172. The Drudge Report provided links to upcoming political and entertainment stories and "predicted" various public sector scandals.

173. Kaley Leetaru, *New Media vs. Old Media: A Portrait of The Drudge Report 2002-2008*, FIRST MONDAY (July 6, 2009), http://journals.uic.edu/ojs/index.php/fm/article/view/2500/2235 (arguing that the *Drudge Report* relied heavily on wire services and obscure news outlets to find small stories that would break large in future days, making it highly dependent on mainstream "old media" sites).

174. Blumenthal v. Drudge, 992 F. Supp. 44 (D.C.C. 1998).

publisher, AOL was successfully removed as a defendant, despite its input to content and the editorial oversight it provided.

While the appellate court questioned the *carte blanche* extended to ISPs under the *Communications Decency Act* and berated their freedom to "flaunt a rumormonger's ability to make rumors instantly accessible to its subscribers and then claim immunity," the court upheld the originating court's decision all the same.[175]

The *Communications Decency Act* was originally introduced to combat youth-directed pornographic content on the Internet.[176] Criticism of the generous ambit of section 230 grows with the wide berth it affords ISPs.[177] Free speech proponents continue, however, to praise the legislation as the vanguard of Internet liberalism and non-curated content, such as that produced by citizen journalists.[178]

EU law has generally taken a stricter view of liability for ISPs than that of the US. Under the *Technical Standards Directive*, a "service provider" for purposes of establishing liability is defined as any person or entity providing an "information society service" which means any services offered for remuneration at a distance by electronic means.[179] Similarly, the *eCommerce Directive* affords an ISP immunity from liability only when it serves as a "mere conduit"[180] or provides "temporary caching"[181] for the sole purpose of making the transmission of content more efficient. The Directive is

---

175. *Id.* at 51.

176. Nebraska Senator Exon proposed the original draft of the CDA in the mid-1990s. *See* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51 (1996).

177. *See also* JOEL R. REIDENBERG ET AL., SECTION 230 OF THE COMMUNICATIONS DECENCY ACT: A SURVEY OF THE LEGAL LITERATURE AND REFORM PROPOSALS, CENTER ON LAW AND INFORMATION POLICY REPORT (CLIP) FORDHAM UNIVERSITY (Apr. 25, 2012); Ryan Dyer, *The Communication Decency Act Gone Wild: A Case for Renewing the Presumption Against Preemption,* 37 SEATTLE U. L. REV. 837 (2014); Sheri Wardwell, *Communications Decency Act Provides No Safe Harbor Against Antifraud Liability for Hyperlinks to Third Party Content Under the Securities And Exchange Act,* 6 WASH J.L. TECH. & ARTS 49 (2010).

178. *See, e.g., Section 230 of the Communications Decency Act: The Most Important Law Protecting Internet Speech*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/cda230 (promoting § 230 as sound legal policy allowing for "YouTube and Vimeo users to upload their own videos, Amazon and Yelp to offer countless user reviews, craigslist to host classified ads, and Facebook and Twitter to offer social networking to hundreds of millions of Internet users").

179. Directive Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations (EC) No. 98/34 of 22 June 1998, art. 1(2), 1998 O.J. (L 204).

180. e-Commerce Directive, *supra* note 64, art. 12.

181. *Id.* at art. 3.

used in cases of copyright infringement, defamation, and invasion of privacy. Immunity is also provided if the ISP service is of a mere technical, automatic and passive nature, and where the ISP has no actual knowledge or control over the content being transmitted or stored.[182]

Personal data retention by *telecom* service providers is regulated under a separate ePrivacy Directive.[183] Such laws requiring the retention for government purposes of location and traffic data of individual users were found to violate the ECHR in 2014.[184] As a result, service providers now have a legal basis on which to refuse compliance with national data retention obligations, although the decision is unclear as to which remedies are available to individual users whose personal data is disclosed. It is difficult to imagine such restriction on government surveillance practices in America.

The individual right to seek takedown requests from ISPs, and to have them give serious consideration to those requests, is of particular interest to courts in Europe.[185] An often-cited example involves the conviction for invasion of privacy and defamation of three Google executives at the hands of a Milan court of first instance in 2010. Residents of a small Italian town complained that a YouTube video of schoolmates taunting an autistic student lingered online for a couple of weeks before Google administration removed it.[186] The Milan court found that that period of time allowed extensive access by countless online viewers. Google argued a guilty verdict might require it to filter content on all YouTube videos before they was posted, which it claimed would be incompatible with the spirit of an open Internet as well as the tenor of several European directives and guidelines. The executives were given a suspended sentence and fine.[187] On appeal the "mere conduit" defense of the Google executives was accepted and the convictions overturned.[188]

---

182. *Id.* at art. 42. As affirmed in the CJEU decision of Case C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), 2012 E.C.R. 4.

183. Eprivacy Directive, *supra* note 66.

184. Digital Rights Ireland, *supra* note 67.

185. As reflected in the "right to be forgotten" proposed by the GDPR and detailed in the CJEU reference decision, *supra* note 160.

186. Loek Essers, *Google Video Trial to Continue to Italian Supreme Court*, PCWORLD (April 17, 2013), http://www.pcworld.com/article/2035387/google-video-trial-to-continue-to-italian-supreme-court.html. Google Inc. purchased YouTube on Nov. 13, 2006.

187. Privacy actions are addressed through the criminal law in Italy.

188. Bogdan, *Italian Supreme Court: Google's YouTube is just a hosting provider,* EDRI (Feb. 12, 2014), https://edri.org/italian-supreme-court-search-engines-just-hosting-providers/.

The more clear-cut intercontinental differences between European and American legal treatment of ISPs are beginning to blur. With the long-awaited *Google Spain* decision*,* the CJEU advanced the autonomy of users and data subjects in two significant ways: it judged Internet companies to be "controllers" of data information involving EU citizens; and it granted those citizens unprecedented autonomy regarding the collection, processing, leakage, and mobility of that information. Prior take-down requests had been limited to information deemed illegal by a court, such as in defamation, privacy or breach of confidentiality cases, pirated content, malware, child sexual abuse imagery and other content prohibited by local law such as material that glorifiesNazism in France.[189]

Control of the individual over her personal information was limited in other ways before *Google Spain.* People were not notified of which data identifying them was being collected, profiled, or shared with other institutional or commercial third parties. Such activities increased individual risk of hacking, loss, negligent handling, or other activities that jeopardized their privacy. If leaks, exposure or loss occurred, there was little legal compensation offered the data subject. That lack of transparency hid the extent and acceleration of the exposure problem: an IBM study in 2013 revealed that globally "more than half a billion records of personally identifiable information—including names, emails, credit card numbers and passwords—were stolen."[190]

2. Terms Of Service Meet *Schrems v Facebook*

The 2014 reference case of *Maximillian Schrems v. Data Protection Commissioner of Ireland* involved a challenge to routine exportation of the Austrian law student's Facebook data from Ireland (where subscriber data of many Internet companies resides) to the US (the corporate headquarters of such technology giants). Many postings were of a very personal nature.[191] The CJEU ruled as

189. David Drummond, *We Need to Talk About the Right to be Forgotten,* THE GUARDIAN (July 10, 2014), http://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate (setting out formal criteria according to the UK Google head).

190. IBM Security Services 2014 Cyber Security Intelligence Index (June 2014, https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.

191. "[E]very 'poke', friend request and invitation (and response) he had sent since setting up an account in 2008" according to Robert Levine, *Behind the European Privacy Ruling that's confounding Silicon Valley,* N.Y. TIMES (Oct. 9, 2015), http://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html?_r=0.

unconstitutional the EU-US Safe Harbor agreement enabling cross-border transfer of EU citizens' data as it did not meet privacy protection as required by EU fundamental rights legislation.[192] Schrems pointed as proof to the 2013 revelations of Edward Snowden concerning the surveillance activities of the US intelligence services focusing on EU citizens.

On the American side of the Atlantic, such activities might be scrutinized for First Amendment violations but otherwise are considered a matter of individual freedom of contract and self-regulation through subscribers' privacy settings. Facebook defended its broadly based terms of service that license the social media company to use subscribers' content in any way it sees fit: for example, Facebook can transfer or sub-license its rights over a user's content to another company or organization and all such uses continue after the deactivation or deletion of a user's account. Facebook loses this license only once all other users that have interacted with the content have also deactivated their accounts.

The case highlights the heightening tension between the libertarian values promoted by Silicon Valley entrepreneurs and EU regulators who focus on the regulation of privacy as a human right. In the wake of the CJEU reference case, Schrems suggests three options for Facebook, Google and other implicated US companies: "moving data to Europe, encrypting data that is stored in the United States or reviewing the corporate structure."[193]

III. TREATING DIGITAL SPEECH DIFFERENTLY

Of increasing promise for addressing reputational protections are extra-legal activities such as the *ad hoc* assemblage of online communities to lobby for user interests whenever unilateral actions by companies or governments threaten online privacy. Another emerging practice is that of online review and ranking systems where positive accomplishments or services of individuals can be promoted and false claims can be unearthed. This section briefly canvasses both a more formal adjudicatory two-tiered system addressing social media harms to reputation and extra-legal suggestions.

---

192. Schrems, *supra* note 60.

193. *Data Protection Authorities in Ireland, Belgium and Germany requested to review and suspend Facebook's data transfers over US spy programs*, EUROPE V. FACEBOOK (Dec. 2, 2015), http://www.europe-v-facebook.org/prism2_en.pdf.

A. The Speech Conundrum & A Separate Space

The democratization of online communications has produced spontaneous, a-contextual and unmediated speech – environmental factors that some argue merit less weight and meaning in legal terms.[194] That debate raises the judicial practice of discerning "high" from "low" speech.[195] Discussions of high level speech that is well researched and aimed at a broad audience, as distinguished from low level speech that is more amateurish, spontaneous and conversational, suggest a value-laden gradient of social good. If we were to debate the value of messages via new media such as video blogging, podcasts, or texting where content can be more off the cuff, fragmented or emotional, we might argue the content has less social currency because it is of little public interest.[196] We could suggest that fewer constitutional protections would be justified regarding such speech because it comprises the daily back-and-forth of minutiae, humor, hyperbole and commentary. We could leave the more egregious, hurtful or inflammatory examples for penal treatment under the criminal law, with its elevated standards of proof. Rowbottom suggests it is only with the "persistence and searchability of digital messaging" that the scrutiny of prosecutors and litigators becomes involved.[197] He concludes, however, that such amateur and casual speech merits some legal response and in proportion to the harm inflicted.

Internet scholar Yuval Karniel supports a different view: that a rumor or other offhand comment does not have elevated status just because it is online: its reliability is still "restrained and incomplete."[198] The credibility of sources, so critical to public acceptance of traditional media accounts, is often suppressed or absent in online accounts. Cues about authority and status of either the writer or sources are often hidden or absent. As one psychological study of Internet behavior points out, in cyberspace what mostly

194. Yuval Karniel, *Defamation on the Internet: A New Approach to Libel in Cyberspace*, 2 J. INT'L MED. & ENT. L. 215, 219 (2009).

195. *See further,* Jacob Rowbottom, *To Rant, Vent and Converse: Protecting Low Level Digital Speech* 71 CAMBRIDGE L. J. 355, 367 (2012) (for a UK perspective).

196. That is the approach of European courts in cases involving freedom of expression under Article 10 of the ECHR.

197. Rowbottom, *supra* note 195, at 366.

198. Karniel, *supra* note 194, at 231.

influences listeners is the speaker's skill in communicating coupled with "persistence, creative ideas and technical know-how."[199]

David Mangan suggests digital speech should be a qualified social good, dependent on our responsible participation in the digital conversation.[200] We already allot different values to various kinds of speech, such as the positive contributions of political speech and speech appearing in legacy journalism. He urges us to rein in the expansive berth that defamation law has allotted to free speech now that social media speech is challenging the status quo.

Criminal and civil court remedies involve so many features that argue against using traditional litigation for online speech: cost, delays, uncertainty of outcome, mandatory criminal sanctions. It would be worthwhile, then, to consider starting with the premise that, outside of egregious threats of harm warranting immediate police attention, digital speech has no social value at all, save those of venting or conveying subjective impressions, banal messages, opinions, gossip or innuendo.

Legal actors struggle with how to define and measure the effects of digital speech on others. Internet defamation researcher Lyrissa Lidsky notes it occurs in a space where hyperbole and exaggeration are routine and venting is as commonplace as careful and considered argumentation.[201] She concludes it is the side-by-side existence of both styles of speech in online communications reporting that creates uncertainty about the verifiability of digital speech.[202]

One argument for treating digital speech as a discrete species of communication is that Internet content is "located in another time and zone," more anecdotal and immediate, and so should not be subjected to the investigative rigors of traditional journalism or the legal standards of proof for defamation.[203] In the Oregon case of *Obsidian Financial Group. LLC v. Cox*, a blogger Courtney Cox posted allegations of fraud, corruption and money laundering involving the plaintiff, a bankruptcy consultation business. Cox liberally injected her posts with hyperbolic terms such as "immoral," "thugs," and "evil

199. John Suler, *The Online Disinhibition Effect*, 7 CYBERPSY. & BEH. 321, 324 (2004).

200. David Mangan, *Regulating for Responsibility: reputation and social media,* International Review of Law, Computers & Technology DOI: 10.1080/13600869.2015.1008960 (2015).

201. Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace* 49 DUKE L.J. 855, 863 (2000).

202. *Id.*

203. Karniel, *supra* note 194, at 218.

doers."[204] The US 9th Circuit Appellate Court applied its test in *Unelko Corp. v. Rooney*[205] to find that the very tenor of blog language used by Cox "negates the impression that [she was] asserting objective facts."[206] The statements were posted on obsidianfinancesucks.com, a URL indicating that any reader would be predisposed to view them with a certain amount of scepticism and an understanding that they likely presented one-sided viewpoints rather than assertions of provable facts.

Karniel argues that the role of blogs, tweets, and other citizen journalism is to serve as a vetting function, providing preliminary flagging of issues that the mainstream offline press can review for stories worthy of further investigation, sober thought and publication. Regarding the role of law in addressing defamatory remarks online, Karniel makes two proposals: either create a sub-category of law for virtual speech with more lenient levels of proof or remove it altogether from judicial scrutiny.[207]

Others have observed the legal predisposition to treat social media messaging as a less important form of speech garnering fewer constitutional protections.[208] That distinction is particularly noted within the employment context.[209] Much of social media language already evades traditional causes of action because it comprises gossip, opinion, insult, vitriol, hyperbole and creepiness.[210]

B. Moving Beyond The Slander-Libel Distinction

Distinguishing between the written and spoke word for litigation purposes made some sense in pre-Internet days when text was considered more damning because it endured over time, whereas the spoken word was ephemeral and, unless recorded, was unavailable at

---

204. Obsidian Fin. Grp., LLC v. Cox, 812 F. Supp. 2d 1220, 1233 (D. Or. 2011).

205. Unelko Corp. v. Rooney, 912 F.2d 1049, 1053 (9th Cir. 1990).

206. Obsidian Fin. Grp., LLC v. Cox, 740 F.3d 1284, 1294 (9th Cir. 2014).

207. Karniel, *supra* note 194, at 231 (rationalizing that most of us do not believe what we read online in any event).

208. Richard Sanvenero, *Social Media and our Misconceptions of the Realities,* 22 INF. & COMM. TECH. L., 89 (2013) (referring to social media, not as an absolute social good, but a "disease").

209. David Mangan, *A Platform for Discipline: Social Media Speech and the Workplace*, Osgoode Legal Studies Research Paper 85 (2015), http://digitalcommons.osgoode.yorku.ca/olsrps/85 (observing speech in traditional media in Canada and England is better protected than that of workers using virtual social platforms as it affects corporate reputation).

210. For an analysis of the latter *see* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 35116 Y. J. L. & Tech 59, 61 (2013).

a later time. Such distinctions have lost relevance as our communications have migrated online. [211]

It is a complex task to determine which cause of action best serves the non-traditional nature of online communications. For example, is a YouTube video actionable as libel or slander? What of podcasts? Chats? Facebook Befriending? Twitter messaging? What about consumer commentary displayed below a video? Is texting an abbreviated form of writing or speaking? What of gestures in videos? Further research into the nature of social media speech could address those uncertainties.

The Internet has several idiosyncrasies that confound traditional categories of offending speech. New media communications can be, for example, truncated into digital semaphore;[212] non-curated; internationally accessible; consensually anonymous and interactive;[213] sent with impetuosity and archived in perpetuity with low entry costs.[214] Posted or texted content can inform, alert, persuade, or convert, but it can also confound the recipient or judge who needs some method of translation to decode the cryptic terms, fragmentary style and emotional overtones. In the extreme, it is its own language and context.

Linguist John McWhorter of Columbia University still works within the traditional distinctions when he suggests digital messaging is more speaking than writing. "Texting isn't written language," he claims, "[i]t much more closely resembles the kind of language we've had for so many more years: spoken language."[215] Texting is patterned after speaking, McWhorter proposes, — looser, telegraphic, and less reflective. We lack tools, however, to make a complete conversion: pencils, typewriters, even computers have historically proven too slow to keep up with the pace of human speech. The speed and convenience of texting on our mobile phones or tablets just might achieve that.

---

211. Leslie Yalof Garfield, *The Death of Slander,* SSRN, *available at* http://ssrn.com/abstract=1916212.

212. Employing terms such as "btw" or lmao that need context and cultural cues to determine intent.

213. Karniel, *supra* note 194, at 220 (confirming anonymity is well accepted by cyber culture).

214. Rowbottom*, supra* note 195, at 356 (noting that "Words typed in seconds followed by hitting the enter key can lead to a criminal record or costly civil litigation.").

215. Michael V. Copeland, *Texting isn't Writing; it's Fingered Speech',* WIRED (Mar. 1, 2013), http://www.wired.com/2013/03/texting-isnt-writing-its-fingered-speech/.

In terms of style dictating meaning, "fingered speech" is developing its own form and vocabulary; it does not measure a decline in written speech but an evolution into a new genre of communication, according to McWhorter, who gives as example the changing nuances of the acronym "lol." With usage, McWhorter sees those three characters becoming something far subtler than "laughing out loud" or "loving you lots." "It's a marker of empathy," he advises, "of accommodation," what linguists call a "pragmatic particle," like the word "yo."[216] Another example is the recently minted acronym "TLDR" which serves as disclaimer - "too long, didn't read" or the use of a forward slash (/) to indicate the author is changing topic. In some ways, texting resembles Pitman shorthand, an American transcribing system from the 1950s that few would argue should be taken for a complete language of communication. It was semaphoric in style, personal, and economic in its abbreviation of words through symbols. For legal actors to be tasked with finding criminal intent or the civil standard of liability in such fragments would be akin to deciphering a complete unique code or language from linguistic bits and pieces. In addition, *cultural* coding must be taken into consideration that shapes speech to local experiences.

C. Keeping up with Technological Capabilities

By putting our reliance in the court system we expose our private selves to judiciaries who, often by self-admission, experience confusion over the complexities of digital communications. Examples abound: in the 2010 case *City of Ontario v. Quon,* involving the issue of constitutional protection of California police communications sent by a paging system, US Supreme Court Chief Justice John Roberts asked in oral argument, "What's the difference between email and a pager?"[217] Justice Anthony Kennedy asked how a text message could be sent to an officer at the same time he was sending one. Former Justice Scalia asked, "Could Quon print these spicy little conversations and send them to his buddies?"[218] In one journalist's opinion, the implications are profound in that "speech, expression, and living have become intertwined in technology" so that "[i]f we're ever to have a case involving Snapchat selfies and eDiscovery [argued

---

216. *Id.*

217. City of Ontario v. Quon, 560 U.S. 746 (2010).

218. Kimberly Atkins, *Technical difficulties at the Supreme Court*, LAWYERS USA (Apr. 19, 2010), http://lawyersusaonline.com/dcdicta/2010/04/19/technical-difficulties-at-the-supreme-court-2/.

before the US Supreme Court], we could be in trouble."[219] It provides small comfort to litigants that US Justice Scalia publicly admitted to being "Mr. Clueless" when it comes to communications technology.[220] Justice Elena Kagan has acknowledged that the court hasn't "gotten to" e-mail yet—reportedly preferring internal communication by hand-written memos printed on ivory paper.[221] As cyberlaw scholar Michael Geist commented when Internet cases were beginning to appear on court dockets: "The technology involved in Internet publication is not a matter of judicial notice of knowledge. Many of the words used to describe what appears to be happening on the screen. . . are quite obviously metaphors and the Court cannot assume that they accurately describe what is actually taking place."[222] Hence they struggle to use technologically neutral language to avoid dating or over-particularizing their decisions. [223]

Technological confusion was also indicated in 2014 when US Supreme Court Justice Sonia Sotomayor asked a lawyer to compare the services of his corporate client to "iDrop in the cloud," a non-existent data storage system.[224] She further asked about the video streaming service "Netflick" although, despite such gaffes, Justice Sotomayor is credited for venturing into unfamiliar technological terrain.[225] Also struggling with counsel submissions during the *Aereo* argument was Justice Stephen Breyer who said, "I've read the briefs

---

219. *See further,* Mark Grabowski, *Are Technical Difficulties At The Supreme Court Causing A 'Disregard Of Duty?'* 3 J. L. TECH. & INTERNET 1, 1 (2011).

220. Jordan Fabian, *Chairman to Justices: "Have Either of Y'all Ever Considered Tweeting or Twitting?"* HILLICON VALLEY: THE HILL'S TECH. BLOG (May 21, 2010), http://thehill.com/policy/technology/99209-chairman-to-justices-have-either-of-yall-ever-considering-tweeting-or-twitting- (quoting Justice Scalia's testimony at a House judiciary subcommittee hearing).

221. Joe Silver, *Supreme Court struggles with e-mail but will shape technology's future,* ARS TECHNICA (May 6, 2014), http://arstechnica.com/tech-policy/2014/05/supreme-court-struggles-with-e-mail-but-will-shape-technologys-future/.

222. Michael Geist, *Cyberlaw shows its true colours,* Blog (Sept. 6, 2001), http://www.michaelgeist.ca/resc/html_bkup/sept62001.html (citing the judge in the Federal Court of Canada case of Guillot v Istek *Corp*. [2001] F.C.J. No. 1165).

223. Rajab Ali, *Technological Neutrality,* 14 LEX ELECT. (Rev. du Centre de recherché en droit public) (Fall 2009).

224. *.ABC, Inc. v. Aereo, Inc*., OYEZ (Apr. 22, 2014), https://www.oyez.org/cases/2013/13-461. *See further* Timothy B. Lee, *The Supreme Court's technical cluelessness makes them better justices,* VOX (Oct. 15, 2014), http://www.vox.com/2014/4/23/5644154/the-supreme-courts-technical-cluelessness-makes-them-better-justices (suggesting that US Supreme Court Justice Sonia Sotomayor confused the technologies of iCloud and Dropbox).

225. Lawrence Hurley, *In U.S., when high-tech meets high court, high jinks ensue,* REUTERS (May 9, 2014), http://www.reuters.com/article/2014/05/09/us-usa-court-tech-idUSBREA480N420140509.

fairly carefully. . . and I'm still uncertain that I understand it well enough."[226] His struggles were evident when he suggested that the tiny broadcast antennas that Aereo sets up in a city could "pick up every television signal in the world and send it. . . into a person's computer."[227]

Lawyers also reveal gaps in digital knowledge. For example, in a 2011 class action against Google regarding its Street View geo-location service, the plaintiffs claimed privacy invasion under the *Electronic Communications Privacy Act*.[228] The information collected, however, was from open Wi-Fi networks, requiring no special equipment. It was unencrypted information broadcast into public airspace.

Similar concerns are expressed within the EU: a report from the Council of Europe states, that "*in most cases,* judges and prosecutors encounter difficulties in coping with the new realities of the cyber world."[229] As early as 2007 a study of European judges and litigation lawyers revealed significant discrepancies in their understanding of the technological basics of electronic evidence. Judges were found to hold subjective perspectives that created "multiple contradictions"; they were often divided in their opinions regarding the admissibility of electronic evidence even when provided with expert testimony.[230] Other studies have acknowledged the uneven understanding by criminal jurists and prosecutors of information and communication technologies across EU jurisdictions.[231]

---

226. As reported in Jordan Graham, *Supreme Court weighs ripple effect of Aereo TV case* (April 23, 2014), http://www.bostonherald.com/business/media_marketing/2014/04/supreme_court_weighs_ripple_effect_of_aereo_tv_case.

227. Silver, *supra* note 221.

228. Complaint, In re Google Inc. Street ViewElectronic Communications Litigation, 794 F.Supp.2d.1067 (N.D. Cal. 2012); *see also* Mike Masnick, *Judge Who Doesn't Understand Technology Says Wi-Fi is Not Radio Communication,"* TECHDIRT (July 1, 2011), https://www.techdirt.com/blog/wireless/articles/20110701/12225114934/judge-who-doesnt-understand-technology-says-Wi-Fi-is-not-radio-communication.shtml.

229. *Cybercrime training for judges and prosecutor: a concept*, COUNCIL OF EUROPE PROJECT ON CYBERCRIME AND THE LISBON NETWORK (Oct. 8, 2009), http://www.coe.int/t/DGHL/cooperation/LisbonNetwork/meetings/Autre/2079_train_concept_4_provisional_8oct09_en.pdfhttp.

230. Fredesvinda Insa, *The Admissibility of* Electronic *Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study*, 1 J. DIG. FOR. PRACT., 285-289 (2007), http://www.tandfonline.com/doi/pdf/10.1080/15567280701418049.

231. *See further,* Lorena Bachmaier Winter, *Section III – Criminal Procedure Information Society And Penal Law*, GENERAL REPORT TO XIX INTERNATIONAL CONGRESS OF PENAL LAW, Rio de Janeiro (Sept. 6, 2014).

CONCLUSION

Reputation, privacy and memory comprise a tricolor badge of personal identity. While all three can be damaged by the untruthful expressions and data collection practices of others, we can maintain some command over their function if we are prepared to call on international legal norms to which western democracies have already committed in principle. This paper has described that rich inventory of laws, as well as current local responses within the US and EU that, to date, have had limited value in lowering our online reputational risk. The Internet is idiosyncratically over-accommodating in that regard in its speed, reach, replication, archiving capabilities, and anonymity – technological features that challenge lawmakers, in whatever jurisdiction, to acknowledge we are spending increasing amounts of our daily lives in a shared space much more powerful in its reputational risk potential than what we used to call mass media.

If we are to rely on extant legal systems, we need a back-to-basics explication of online communications so we can gain a more informed understanding of the nature of digital speech and structure gradients of harm for law reform. Much work is needed to understand the ontological difference of digital speech and evolving forms of human communication.[232] Tapping the wealth of multi-disciplinarity is key. Superior court judiciaries might want to take leadership in this by re-examining their oaths of office to ensure they provide wisdom and guidance to those who struggle to understand law's relevance to digital communications. Judges are often tasked with accommodating new realities while "proclaiming fidelity to the past."[233] Unlike Internet technology itself, developments in the law must be seen as continuous, not disruptive.[234] Judges, in turn, have been critical of attorneys' poor comprehension of digital technologies, in one case expressing concern that lawyers unquestioningly accept information from the Internet and often do not know when they should object to digital evidence.[235]

EU lawmakers as well need to continue calling to account industry practices that facilitate personal profiling and extreme speech that can

---

232. Austin Sarat, Lawrence Douglas & Martha Merrill Umphrey eds, IMAGINING NEW LEGALITIES: PRIVACY AND ITS POSSIBILITIES IN THE 21ST CENTURY, Introduction, 2 (2012).

233. *Id.* (suggesting law be an instrument of both continuity and change, all the while appearing unsettled, not reassured, by such change.)

234. *Id.*

235. Gary Craig Kessler, *Judges' Awareness, Understanding, and Application of Digital Evidence*, PHD DISSERTATION IN COMPUTING TECHNOLOGY IN EDUCATION, NOVA SOUTHEASTERN UNIVERSITY (2010), http://www.garykessler.net/library/kessler_judges&de.pdf.

ruin the social worth and dignity of its citizens.

Extra-legal responses include assuming individual responsibility for the shape of our personal identities. We can still maintain much control by exercising prudence in our postings and educating each other about their indelibility and potential for misguided manipulation. Microsoft announced it has commissioned research in Canada, Germany, Ireland, Spain, and the United States that found that a notable 91 percent of people have made attempts to manage their online profile at some point but only 44 percent of adults actively think about the long-term consequences of their online activities.[236] That gap must close if we are to assume reputational control and use social media responsibly. Curative suggestions include signing up for personal alerts of others posting our names online, taking a more aggressive role in shaping our online presence, using separate accounts for personal and professional profiles and lobbying the Internet and social media industries to rethink arbitrary terms of service in favor of user input on the limits of exposure we are prepared to endure. Within legal systems, lawmakers are encouraged to think more knowledgably about the changing semantic, social and cultural contours of language.

As we come to know, click by click, the privacy costs of our social and digital engagement, and as calls increase for recognition of Internet access as a human right, we are urged to consider our important role in untying the Gordian knot.

236. *Take charge of your online reputation,* MICROSOFT SAFETY & SECURITY CENTER, https://www.microsoft.com/security/online-privacy/reputation.aspx (no data provided on sample size or methodology).