Requiem for Cyberspace: The Effect of the European General Privacy Regulation on the Global Internet

*Steven P. Tapia**

INTRODUCTION

The dream of a perpetual, limitless, non-dimensional space is an idea that has transfixed clergy, philosophers, and poets for ages. Whether it is called "heaven," "the afterlife," "nirvana," or another linguistic stand-in, the dream of a dimension beyond the bounds of time, space, and the laws of nature seems as universal as any concept ever.

From its initial development in the 1970s (as a military, academic, and governmental experiment in creating a wholly alternative means of communication capable of surviving catastrophic failures of any parts of the communications conduits) until essentially now, the Internet seemed to be the closest incarnate approximation developed of a dimension beyond the bounds of time, space, and the laws of nature. It is no surprise, therefore, that for almost a quarter of a century, the fear of losing this seemingly limitless and boundless creation has been the primary metaphysical driver of policies and legislation worldwide. In short, for a long time, the governing entities in the world took a "hands-off" approach to regulating this universal construct called "the Internet."

That period of paradisal life for the Internet started to disappear when the People's Republic of China began perfecting its censorship and regulation of Internet content in the 1990s.[1] The disappearance of paradise accelerated with a key 2014 decision of the European Court of Justice.[2] Any hope of regaining paradise was further sealed away with the European Union's implementation of the European Union General Data Protection

* Distinguished Practitioner in Residence; Seattle University School of Law.

1. The very successful efforts of the Chinese government at taking control of the Internet for its citizens is beyond the scope of this piece. However, there have been several excellent surveys of their efforts, including ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING (Ronald Deibert et al. eds., 2008).

2. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R. 317.

Regulation (GDPR) beginning in 2017.[3] The dream and reality of a universal Internet is dead, replaced by what is currently three separate Internets—a European one, a Chinese one, and one for the rest of the universe.

I. THE EXCEPTIONAL INTERNET

The Internet—or, in its poetic guise, "cyberspace"—has been viewed as something unprecedented from its inception. In a world where the means of communication—books, newspapers, magazines, radio, television, phones—had been limited and controlled worldwide by corporations and governments, a set of software tools and computer network protocols we now call "the Internet" gave any individual the means to communicate anywhere in the world and with whomever desired. It was a civil libertarian dream come true: the ability to reach the entire world without censorship or gatekeeping fees.[4]

As a technical matter, the Internet is a network of networks.[5] It is a global system of interconnected computer networks using the Internet protocol suite (TCP/IP) to link devices worldwide.[6] It includes local and wide-area private, public, academic, business, commercial, and government networks, all interconnected by a huge menagerie of electronic, wireless, and optical networking technologies.[7]

Its poetic doppelgänger—cyberspace—comes from the literary world. William Gibson coined the term "cyberspace" in his short story *Burning Chrome*, first published in 1982 by *Omni* magazine and later anthologized in the collection *Burning Chrome*.[8] However, his use of the term in his 1984 science fiction novel *Neuromancer* caused its popularity as a synonym for the Internet. One passage of that work is often cited as the de facto definition of cyberspace:

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. . . . A graphic representation of data abstracted from banks of every computer in the human system.

3. Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

4. *See generally* Jack Goldsmith & Timothy Wu, *Digital Borders*, LEGAL AFF. (Jan.-Feb. 2006), http://www.legalaffairs.org/issues/January-February-2006/feature_goldsmith_janfeb06.msp [https://perma.cc/XXQ6-3G55].

5. JAMES GRIMMELMAN, INTERNET LAW: CASES AND PROBLEMS 27–35 (8th ed. 2018).

6. *See generally id.*

7. *Id.*

8. WILLIAM GIBSON, *Burning Chrome*, *in* BURNING CHROME 179 (Harper Voyager reprt. ed. 2003).

> Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding . . . .[9]

In 1990, John Perry Barlow, a storied Grateful Dead lyricist and early thinker on the metaphysics of the Internet, founded the Electronic Frontier Foundation (EFF) along with fellow digital-rights activists John Gilmore and Mitch Kapor.[10] In 1996, Barlow wrote and posted to the EFF website *A Declaration of the Independence of Cyberspace*,[11] which famously opens with a great summation of the poetic/philosophical view of the Internet:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.[12]

A few paragraphs later, Barlow writes:

> Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.
>
> We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.
>
> We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.
>
> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

---

9. WILLIAM GIBSON, NEUROMANCER 69 (Ace Books 2004) (1984).

10. *A History of Protecting Freedom Where Law and Technology Collide*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/about/history [https://perma.cc/9Y93-5R79].

11. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/2XVK-BKA3].

12. *Id.*

> Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.[13]

The strength of the effect of these metaphoric and poetic representations of the Internet on the imaginations of thought leaders and policy makers in the 1990s cannot be underestimated. The Internet's perception as an unprecedented but incipient historical development needing careful nurturing gave legislatures and regulators confronting the Internet at that time cause to fear regulating or limiting it in any way, or risk killing off the new technology. This fear led to an era of laissez-faire oversight called "Internet Exceptionalism."[14] Internet Exceptionalism primarily manifested itself in crafting Internet-specific laws that veered away sharply from the way telephone or broadcasting was regulated; instead, it immunized conduct that was seen to violate intellectual property or information torts.[15]

The Digital Millennium Copyright Act (DMCA), codified in relevant part in 17 U.S.C. § 512 in 1998, was the first major example of legislation in the Internet Exceptionalism era. The DMCA tried to solve the problem of who is liable for the distribution of copyrighted material via the Internet. The concept of secondary liability for copyright infringement—holding parties that facilitate or enable distribution of copyright infringing material liable—created a very real problem for businesses seeking to provide access and programs for consumers to use the Internet. A digital distribution system is agnostic to what flows through it. To the distribution system, it is all electronic bits, each like the one before and the one after. That the bits can be reassembled into digital copies of books, recorded music, movies, or other copyright material was not something that the providers of the distribution system could easily control. Anyone who had access to the system was virtually unmonitored to exchange not only thoughts but also essentially perfect digital copies of unlicensed copyrighted content. Technology businesses seeking to provide Internet access and services were faced with inconsistent judicial decisions as to

---

13. *Id.*

14. Eric Goldman, *The Third Wave of Internet Exceptionalism*, TECH. & MARKETING L. BLOG (Mar. 11, 2009), https://blog.ericgoldman.org/archives/2009/03/the_third_wave.htm [https://perma.cc/9FQF-XTF2].

15. *Id.*

whether they would be viewed identically to a "brick-and-mortar" store selling copyright infringing items.[16] The DMCA solved this problem by providing operators of Internet services immunity from copyright infringement for distribution of unlicensed content owned by third parties if they adopted a system where copyright holders could give the service notice of the presence of the content on their system and, once notice was received, the service removed the content within a reasonable time. The creation of these "notice and take down" systems created enough legal certainty that technology companies such as America Online, Yahoo!, Microsoft, and YouTube could provide Internet services broadly without fear of getting embroiled in massive numbers of copyright infringement suits. It is no surprise that Google, Facebook, and Twitter began to flourish and grow during this same period.[17]

Section 230[18]—the one piece of the Communications Decency Act left in place after judicial challenges—is another salient example of this "hands-off" approach. The statute immunizes online platforms like Facebook, Twitter, and Reddit from liability for publishing most types of third-party content. It was enacted—in substantial part—"to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[19] Section 230 is the prime example of Internet Exceptionalism because it so clearly insulates online platforms from liability for identical content that would otherwise fall on analog platforms like newspapers and magazines.

While more measured, the judicial system also viewed the Internet as something special. For example, in 1996, the trial court judge in the preeminent case challenging the Communication Decency Act[20] called the Internet "a unique and wholly new medium of worldwide human communication."[21]

While there have been several attempts at regulating the Internet under American law (preeminently, the Communications Decency Act and the Children Online Privacy Act[22]), these attempts have generally been

16. *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 907 F. Supp. 1361, 1381 (N.D. Cal. 1995) (means of digital distribution not liable); Playboy Enters. v. Frena, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993) (means of digital distribution liable).

17. For a summation of the interrelatedness of the DMCA and the growth of digital platforms like Google and Facebook, see JONATHAN TAPLIN, MOVE FAST AND BREAK THINGS: HOW FACEBOOK, GOOGLE, AND AMAZON CORNERED CULTURE AND UNDERMINED DEMOCRACY 97–102 (2017).

18. 47 U.S.C. § 230 (2012).

19. *Id.* § 230(b).

20. Formerly codified, in relevant part, at 47 U.S.C. § 151.

21. ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996).

22. 15 U.S.C. §§ 6501–6506 (2012).

set aside by the courts.[23] Similarly, individual lawsuits seeking closer Internet regulation have also generally failed.[24]

II. THE COMMERCIAL INTERNET

The light regulation of Internet businesses during the period of Internet Exceptionalism created an open field for innovation that gave birth to the companies and business models that came to dominate what we now think of as the Internet. Alphabet (the parent corporation of Google and YouTube), Amazon, Apple, Facebook, Microsoft, and Twitter became some of the most valuable corporations in the United States in large part because of the wide-scale usage of their digital platforms, curated user-generated content, and the finding tools they provide to locate content available on the Internet.[25] The net result of these business successes is that the poetic and metaphysic attributes and appeal of the Exceptional Internet started to recede and, instead, the Internet became the means of a small handful of American companies to control and profit from the content and services made available through the Internet worldwide.

III. THE EUROPEAN INTERNET

A. The Right to Be Forgotten

Whereas American courts and regulators have either not acted or only acted retrospectively to problems created by innovating American technology companies, their European equivalents have been actively—and, in some cases, proactively—seeking to maintain control on what technology companies can do with content and other information found on the Internet. Starting with the investigations of Microsoft in the late 1990s, Google in the 2010s, and now Facebook, European regulators have responded differently than their American counterparts to the dominance of American companies providing Internet services. Similarly, the European courts have not been reluctant to step in and dramatically alter the way technology companies handle information on the Internet.

With regard to regulating the Internet, the first major sign of this difference between the United States and Europe came with litigation that gave birth to a new personal right in Europe: the "right to be forgotten." In *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, the litigation resolved a case involving

23. *See* Ashcroft v. ACLU, 542 U.S. 656 (2004); Reno v. ACLU, 521 U.S. 844 (1997).

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

25. For a biographical survey of the founders of these companies and their successes, see generally WALTER ISAACSON, THE INNOVATORS (2014).

Costeja and changed the face of the Internet.[26] In 1998, *La Vanguardia*, a Spanish newspaper, printed two announcements about an auction of properties seized by the governmental authorities to satisfy social security debts.[27] A version of the edition was later made available on the web.[28] One of the properties described in the newspaper belonged to Mario Costeja González, who was named in the announcements.[29] In November 2009, Costeja contacted the *La Vanguardia* staff and complained that when his name was used as a Google search engine term, the announcements were prominently displayed.[30] He requested the announcements be removed from the web version of the newspaper, arguing that the forced sale had been concluded years before and was no longer relevant.[31] The newspaper responded that erasing Costeja's data was not appropriate because the announcements were on the order of a governmental authority.[32] Costeja next reached out to Google Spain in February 2010 and requested that the links to the announcements be removed.[33] Google Spain forwarded the request to its corporate parent at the time—Google Inc., in California—as Google Inc. maintained one universal search engine database used by all its regional subsidiaries.[34] Costeja then lodged a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos, AEPD) demanding both that the newspaper be required to remove the data and that Google Spain or Google Inc. be required to remove the links to the data.[35]

In July 2010, the director of AEPD rejected the complaint against the newspaper but upheld the complaint against Google Spain and Google Inc., requiring Google to remove the links referencing Costeja and make access to the data impossible.[36] As a result, Google Spain and Google Inc. brought separate actions against the AEPD's decision before the Audiencia Nacional (National High Court of Spain).[37] Several other European governments intervened in the litigation and it eventually found its way to the ECJ. The ECJ's decision concluded that:

---

26. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R. 317.

27. *Id.* ¶ 14.

28. *Id.*

29. *Id.*

30. *Id.* ¶ 15.

31. *Id.*

32. *Id.* ¶ 16.

33. *Id.* ¶ 17.

34. *See id.* ¶ 43.

35. *Id.* ¶ 15.

36. *Id.* ¶ 16–17.

37. *Id.* ¶ 18.

1. The "activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference" constituted the "'processing of personal data.'" As data "controllers," search engines are required to comply with the 1995 European Data Privacy Directive (95/46/EC).[38]
2. Google's maintenance of an advertising sales office in Spain meant that Google was processing the personal data found in its universal search database within the European Union and therefore was subject to European law.[39]
3. Google and other search engines must "remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person," even if (i) that information remains on the third-party website, and (ii) the third party lawfully published the information.[40]
4. This individual right to have search results removed "override[s] . . . not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name."[41]
5. Nevertheless, in certain cases the right to have search engine results removed can be outweighed by a "preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question," such as the person's role "in public life."[42]

The ECJ ruling directly contradicted the "hands-off" approach American courts had taken regarding search engine results holding, in essence, that search engines cannot be required to remove search results or be held liable for any such refusal.[43] The practical result is that the search engines currently available in the EU are separately operated and

38. *Id.* Ruling 1; *id.* ¶ 21.
39. *Id.* Ruling 2; *id.* ¶ 43.
40. *Id.* Ruling 3; *id.* ¶ 88.
41. *Id.* Ruling 4; *id.* ¶¶ 97–99.
42. *Id.*
43. *See, e.g.*, Zhang v. Baidu.com, Inc., 10 F. Supp. 3d 433 (S.D.N.Y. 2014); Murawski v. Pataki, 514 F. Supp. 2d 577 (S.D.N.Y. 2007); Langdon v. Google, Inc., 474 F. Supp. 2d 622 (D. Del. 2007); Search King, Inc. v. Google Tech., Inc., No. CIV-02-1457-M., 2003 WL 21464568 (W.D. Okla. May 27, 2003); Maughan v. Google Tech., Inc., 49 Cal. Rptr. 3d 861 (2006).

only include the subset of indexed entries not subject to an order in a "right to be forgotten" case.

B. The European Union's General Data Protection Regulation (GDPR)

In addition to codifying the holdings in the Google/Costeja case that established the "right to be forgotten" as regulation (now called "the right to rectification erasure"),[44] the implementation of the GDPR's provisions regarding data processing, privacy, and usage have had a dramatic effect on the global reach of the Internet.

The GDPR applies to anyone who "processes" personal data, defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means."[45] Under the Regulation, "personal data" is

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[46]

Despite the GDPR's attempts to distinguish personal data from nonpersonal data and make its terms applicable only to personal data, information used to make websites and online platforms function as a practical matter making even the basic data about a person—for example, logins, IP addresses, and geographic location are identifiable when combined with other readily available data. Therefore, a website operator—even one outside the EU—trying to decide if the GDPR applies to its operations must conclude that it does if the website is available to anyone in the EU. This is especially so given that the cost of making the wrong conclusion—deciding the GDPR does not apply and then having the regulators or courts in the EU decide otherwise—can result in fines and penalties up to €20 million, or four percent of the company's worldwide annual revenue of the prior financial year, whichever is higher.[47]

The GDPR prohibits the processing of personal data unless permitted by one of six enumerated bases, which includes "consumer consent."[48] However, the GDPR, unlike any counterpart elsewhere in the world,

---

44. GDPR, *supra* note 3, art. 17, at 43–44.
45. *Id.* art, 4(2), at 33.
46. *Id.* art. 4(1), at 33.
47. *Id.* art. 83, at 82–83.
48. *Id.* art. 6(1), at 36.

defines specific requirements for determining if effective consent has been obtained. For example, the GDPR requires that "an indication of consent must be unambiguous and involve a clear affirmative action (an opt-in)."[49] It specifically bans pre-selected opt-in boxes and directs that "[c]onsent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service."[50]

The GDPR applies to companies doing business in the EU regardless of whether data processing takes place inside or outside the EU or the data relates to EU residents.[51] This means that an American business with a physical presence in the EU, such as most of the technology companies (e.g., Google, Apple, Microsoft), will be subject to the Regulation both for consumer data from the EU and non-EU consumer data. The GDPR also applies to companies not established in the EU that process EU residents' data when it is (a) related to offering goods or services to EU residents, or (b) related to monitoring EU residents' behavior within the EU (for example, tracking their web usage via cookies or beacons).[52]

The effect of the Regulation is clear. The GDPR governs the processing of EU consumer data by companies that have no physical presence in the EU. So, rational risk management and legal analysis suggest that an American website or online platform globally available needs to comply with the GDPR (since it processes data relating to EU residents) unless the enterprise has no EU offices and never uses EU consumer data. In fact, in expectation of the implementation of the GDPR, several American online companies (such as the Chicago Tribune) have restructured their businesses, choosing to make them unavailable in the EU.[53]

The net result is that the GDPR's broad reach has effectively diminished what Internet content is available in the EU and has made a smaller, European-only Internet. As a direct consequence, the "cyberspace" ideal of a universal place where ideas can be freely exchanged without restriction is dead, and the migration of thoughts, ideas, and viewpoints from outside Europe faces a substantial barrier to entry.

In this way, an ostensibly well-intended attempt to force companies doing business in Europe to take good care of the personal data of

---

49. INFO. COMM'R'S OFFICE, GUIDE TO THE GENERAL DATA PROTECTION REGULATION (GDPR) (Mar. 22, 2018), https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf [https://perma.cc/7WYB-9QJF].

50. *Id.*

51. GDPR, *supra* note 3, Recital 22, at 4.

52. *Id.* Recitals 23–24, at 5.

53. Alyssa Newcomb, *Chicago Tribune, Los Angeles Times Block European Users Due to GDPR*, NBC NEWS (May 28, 2018), https://www.nbcnews.com/tech/tech-news/chicago-tribune-los-angeles-times-block-european-users-due-gdpr-n877591 [https://perma.cc/WZD7-284T].

European citizens serves as a requiem for the dream of a free, boundless, dimensionless cyberspace.