PRIVACY LAW THAT DOES NOT PROTECT PRIVACY, FORGETTING THE RIGHT TO BE FORGOTTEN

MCKAY CUNNINGHAM*

I. Birth of a New Right

Mario Costeja, a Spanish lawyer, could not pay his debts.[1] His home was repossessed and a local newspaper, *La Vanguardia*, published a 36-word notice

* Associate Professor, Concordia University School of Law

1 *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, Mario Costeja González (May 13, 2014), *available at* http:// curia.europa.eu; *Factsheet on the "Right to be Forgotten" Ruling (c-131/12),* EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [hereinafter European Commission Factsheet]; Daniel Lyons, *Assessing the Right to be Forgotten*, 59 FALL B. B.J. 26, 26—28 (2015).

Electronic copy available at: https://ssrn.com/abstract=2933634

of the debt.[2] The short notice was published only once by the newspaper in 1998, but it followed Costeja every year thereafter.[3] Google searches under his name consistently retrieved the 36-word notice of his old debt – even fifteen years after the original 1998 publication.[4] Costeja sued, asking a Spanish court to delete the record of the debt as to both *La Vanguardia's* publication and Google's links to it.[5]

Costeja claimed a right to be forgotten, that the old debt was no longer relevant, and that both Google and *La Vanguardia* must forever erase the 36-word notice and all reference to it.[6] Because the case turned on law promulgated by the European Commission, the Spanish court referred the case to the Court of Justice of the European Union (CJEU), which exercises jurisdiction in some instances over twenty-eight European Member States. The CJEU directly addressed the certified question of "whether an individual has a right to request that his or her personal data be removed from accessibility via a search engine (the 'right to be forgotten')."[7] The Court ruled that the debt notice could remain on *La Vanguardia's* website, but that Google must delete any link connecting Costeja to it.[8]

The high court ruling was instantly controversial.[9] It set a broad precedent, conferring a new legal right to force erasure of links to data on the Internet. The right requires that Google and similar data "controllers" delete access to information deemed "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in light of the time that had elapsed."[10] The Court offered little guidance in determining when

---

2 *Id.*

3 *Id.*

4 *Id.*

5 Jeffrey Toobin, *The Solace of Oblivion*, THE NEW YORKER (Sep. 29, 2014), http://www.newyorker.com/magazine/2014/09/29/solace-oblivion.

6 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, Mario Costeja González (May 13, 2014), *available at* http:// curia.europa.eu; *see also,* Dave Lee, *What Is the "Right To Be Forgotten"?,* BBC (May 13, 2014), http://www.bbc.com/news/technology-27394751.

7 *Google Spain SL*, Case C-131/12; *see also* European Commission Factsheet*, supra* note 1.

8 *Id.*

9 *See* Dan Jerker B. Svantesson, *Delineating the Reach of Internet Intermediaries' Content Blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach?"*, 11 SCRIPTED 153, 155 (2014), http://script-ed.org/wp-content/uploads/2014/10/svantesson.pdf; Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, PETER FLEISCHER: PRIVACY (Mar. 9, 2011), http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html; Meg L. Ambrose, *A Digital Dark Age and the Right to Be Forgotten*, 17 J. INTERNET L. 1 (2013); Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1533—34 (2012).

10 *Google Spain SL*, Case C-131/12; *see also* European Commission Factsheet*, supra* note 1.

Electronic copy available at: https://ssrn.com/abstract=2933634

personal information is subject to mandatory erasure due to "irrelevance" or "inadequacy."[11]

The Court did not identify or characterize how the new right to delete information comports with countervailing rights related to free expression, media publications, and political speech. What if a European politician demands that Google, Yahoo, and Microsoft delete all links to past indiscretions? Can those convicted of child molestation erase public notice of those convictions through the right to be forgotten? What about those who provide or publish information? One reporter claimed he was "cast into oblivion" when his blog was delisted from Google searches?[12] Do bloggers, owners of websites, digital news outlets, and others get an opportunity to object before their content is blotted out by the right to be forgotten? Do they even get notice? The CJEU ruling provided little insight to such questions and allowed little time to consider them.[13]

Indeed, Google promptly complied with the CJEU ruling by creating and publishing a deletion request form.[14] On the first day of the form's publication, Europeans submitted 12,000 requests to delete data.[15] Within four days, it had grown to 41,000 requests.[16] As of January 2017, Europeans had submitted over 645,000 requests to deactivate 1.7 million URLs. Google has deleted over 43% of those, approximately 657,000 links.[17] Early reports suggested that a large percentage of deleted content involved accusations of fraud, child pornography, and other serious crimes.[18] One reporter revealed deletion requests made by "a British politician who's trying to make a comeback, someone convicted of possessing child abuse images and a doctor who doesn't want negative reviews from patients to be searchable."[19] After Google inadvertently revealed information

---

11 *Google Spain SL*, Case C-131/12.

12 Robert Peston, *Why has Google Cast me into Oblivion?* BBC NEWS (July 2, 2014), http://www.bbc.com/news/business-28130581.

13 *Google Spain SL*, Case C-131/12.

14 *See* Caitlin Dewey, *Want to Remove Your Personal Search Results from Google? Here's How the Request Form Works,* THE WASHINGTON POST (May 30, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/05/30/want-to-remove-your-personal-search-results-from-google-heres-how-the-request-form-works/.

15 *See* Caroline Preece & Rosie Clarke, *Google "Right to be Forgotten": Everything You Need to Know*, ITPro (Feb. 9, 2015), http://www.itpro.co.uk/security/22378/google-right-to-be-forgotten-everything-you-need-to-know.

16 *See id.*

17 *Transparency Report, European Privacy Requests for Search Removals,* GOOGLE, http://www.google.com/transparencyreport/removals/europeprivacy/ (last visited, January 1, 2017).

18 Leslie D'Monte, *Right to be Forgotten Poses a Legal Dilemma in India*, LIVE MINT (June 6, 2014), http://www.livemint.com/Industry/5jmbcpuHqO7UwX3IBsiGCM/Right-to-be-forgotten-poses-a-legal-dilemma-in-India.html.; See Caroline Preece et al., *Google "Right to be Forgotten": Everything You Need to Know*, IT PRO (Feb. 9, 2015), http://www.itpro.co.uk/security/22378/google-right-to-be-forgotten-everything-you-need-to-know [https://perma.cc/WW5S-PQM3].

19 See David Mitchell, *The Right To Be Forgotten Will Turn the Internet into a Work of Fiction*, OBSERVER (July 5, 2014), http://

about those requesting data deletion, it appeared that 95% of the erasure requests derive from "ordinary members of the public."[20] Regardless, it remains difficult to know who is requesting content deletion and why.[21]

Commentators from diverse socio-political backgrounds but particularly from the United States decry the right to be forgotten as antithetical to free expression and as distorting the benefits attending unfiltered access to information.[22] One law professor claims "the right to be forgotten will lead to censorship of the Internet because data subjects can force search engines or websites to erase personal data, which may rewrite history."[23] If content becomes less searchable, others assert it will "derogate[] the role of counterspeech."[24]

Wikipedia's founder portrayed the right to be forgotten as "completely insane," maintaining that "in the case of truthful, non-defamatory information obtained legally, I think there is no possibility of any defensible 'right' to censor what other people are saying. You do not have the right to use the law to prevent Wikipedia editors from writing truthful information, nor do you have a right to prevent Google from publishing truthful information."[25] Admittedly, the author of this paper agreed, writing that "European filtering of Internet content worldwide through the right to be forgotten…effectuates international censorship in the guise of privacy."[26]

This Article confronts these predictions. Are these censorship consequences manifesting? Will they? Start with "patient zero," the first person granted anonymity under the right to be forgotten. Mario Costeja sought to erase any

---

www.theguardian.com/commentisfree/2014/jul/06/right-to-be-forgotten-internet-work-of-fiction-david-mitchell-eu-google.

20 *See* Sylvia Tippmann and Julia Powles, *Google accidentally reveals data on 'right to be forgotten' requests*, THE GUARDIAN (July 14, 2015), https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests ("Less than 5% of nearly 220,000 individual requests made to Google to selectively remove links to online information concern criminals, politicians and high-profile public figures, the Guardian has learned, with more than 95% of requests coming from everyday members of the public.").

21 *See* Ravi Antani, *The Resistance of Memory: Could the European Union's Right to be Forgotten Exist in the United States?* 30 BERKELEY TECH. L.J. 1173, 1199—1204 (2015).

22 Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 354 (2015) ("In this Article, we compare the EU and U.S. privacy regimes and explain how the EU's right to be forgotten, as currently framed, is antithetical to the First Amendment of the U.S. Constitution.").

23 Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH. 349, 373 (2015).

24 Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right To Be Forgotten Are Incompatible with Free Speech*, 18 COMM. L. & POL'Y 91, 114 (2013).

25 Preece, *supra* note 15.

26 McKay Cunningham, *Free Expression, Privacy, and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship*, 69 ARK. L. REV. 71, 114 (2016).

report of his 1998 debt, and yet in a single day in 2014 "840 articles in the world's largest media outlets were published in reference to his case, including in countries where his name would otherwise never have been heard, and where the [CJEU's] ruling will never reach."[27] Today, a Google search under Costeja's name generates thousands of articles, linking him to the right to be forgotten, and ultimately to his 1998 debt. Costeja's attempt to suppress information only amplified it.

But perhaps Costeja's case is unique. As the first to exercise the right, his request was the most public and controversial.[28] Certainly others seeking data erasure succeeded in withdrawing their personal information from the public eye? A close look, however, indicates that these less polemical erasure requests faced similar barriers, revealing the difficulty inherent in erasing digital data.[29]

An assortment of unaffiliated entities purposely undermine efforts to delete links under the right to be forgotten.[30] Soon after Google began delisting links, the website "Hidden from Google" began tracking the very content targeted for deletion, memorializing the delisted links on the website as well as the relevant search term and the source that hosted the content.[31] Links to information involving a shoplifting incident, a financial scandal, and an alleged sexual predator disappeared from Google search results only to reappear on the "Hidden from Google" webpage.[32] News media increasingly do the same, particularly for stories they publish and that Google delists. The British Broadcasting Corporation (BBC) re-publishes the stories it generates and Google delists,[33] and others like Wikimedia and Reddit maintain logs that track the content from each link that Google truncates.[34]

---

27 James Ball, *Costeja González and a Memorable Fight for the 'Right to be Forgotten'*, THE GUARDIAN (May 14, 2014), http://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten.

28 *See* Ravi Antani, *The Resistance of Memory: Could the European Union's Right to be Forgotten Exist in the United States?* 30 BERKELEY TECH. L.J. 1173, 1174—77 (2015).

29 See *infra*, Part V.

30 See *infra*, Part V(b).

31 *See* Hidden from Google, http://hiddenfromgoogle.afaqtariq.com/ (last visited May 6, 2016).

32 See Jeff John Roberts, *"Hidden from Google" Shows Sites Censored Under EU's Right-to-be-Forgotten Law*, GIGAOM (July 16, 2014), https://gigaom.com/2014/07/16/hidden-from-google-shows-sites-censored-under-eus-right-to-be-forgotten-law/.

33 Neel McIntosh, *List of BBC Web Pages Which have been Removed from Google's search results*, BBC INTERNET BLOG (June 25, 2015), http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379.

34 *Notices Received from Search Engines*, WIKIPEDIA, https://wikimediafoundation.org/wiki/Notices_received_from_search_engines (last visited July 11, 2016); Subreddit, *Things That Were Not Meant to be Forgotten*, available at https://www.reddit.com/r/nevertoforget/? (described as a "forum to post articles that have been removed by Google from search results as a consequence of the righto to be forgotten); *see also* Geoff Brigham & Michelle Paulson, *Wikipedia Pages Censored in European Search Results*, WIKIMEDIA BLOG (Aug. 6, 2014),

These accumulated efforts undermine the right to be forgotten and presage its failure. As soon as European law strips content from Google searches, that content is added back into the cyber commons through alternative avenues.[35] The best-case scenario for proponents of the right to be forgotten, is that "deleted" content becomes more difficult to find.[36] As long as the search engine industry is dominated by one or two providers, this best-case scenario is not so bad.

Google currently monopolizes the search engine market and has been likened to the "card catalogue" of the Internet library.[37] But if it continues to delete links in compliance with the right to be forgotten, that status may very well falter. The more content Google scrubs, the less attractive its service, opening a market for smaller, perhaps regional search engines that do not have assets or market-share in Europe and are not subject to the right to be forgotten.[38] This is already taking place; Google's market share fell from in 82.5% in 2011 to 66.41% in 2015,[39] with some prognosticating that Google's market share "is now likely in permanent decline."[40]

In the long term, the right to be forgotten will not realize the goal of ensuring privacy to Europeans who seek to remove their personal information from public access. It may, however, dilute Google's primacy as search engine juggernaut – a perhaps unsurprising secondary effect, given the European Commission's ongoing efforts to diminish Google's dominance in Europe.[41] The EU's failure to effectuate privacy goals through the right to be forgotten is emblematic of EU privacy

---

https://blog.wikimedia.org/2014/08/06/wikipedia-pages-censored-in-european-search-results.

35 *Notices Received from Search Engines*, WIKIPEDIA, https://wikimediafoundation.org/wiki/Notices_received_from_search_engines (last visited July 11, 2016); Subreddit, *Things That Were Not Meant to be Forgotten*, available at https://www.reddit.com/r/nevertoforget/? (described as a "forum to post articles that have been removed by Google from search results as a consequence of the righto to be forgotten); *see also* Geoff Brigham & Michelle Paulson, *Wikipedia Pages Censored in European Search Results*, WIKIMEDIA BLOG (Aug. 6, 2014), https://blog.wikimedia.org/2014/08/06/wikipedia-pages-censored-in-european-search-results

36 See Jeff John Roberts, *"Hidden from Google" Shows Sites Censored Under EU's Right-to-be-Forgotten Law*, GIGAOM (July 16, 2014), https://gigaom.com/2014/07/16/hidden-from-google-shows-sites-censored-under-eus-right-to-be-forgotten-law/.

37 Jeff John Roberts, *The Right to Be Forgotten From Google? Forget It, Says U.S. Crowd,* FORTUNE.COM (Mar. 12, 2015), http://fortune.com/2015/03/12/the-right-to-be-forgotten-from-google-forget-it-says-u-s-crowd/.

38 Laurie Sullivan, *Search Engines Struggle To Keep Web Traffic*, MEDIA POST (Dec. 18, 2015), http://www.mediapost.com/publications/article/265120/search-engines-struggle-to-keep-web-traffic.html.

39 *Desktop Search Engine Market Share*, NETMARKETSHARE, https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0&qptimeframe=Y (last visited May 8, 2016).

40 See Dan Frommer, *The Product that Made Google has Peaked for Good*, QUARTZ (Dec. 15, 2015), http://qz.com/573361/the-product-that-made-google-has-peaked-for-good/.

41 See Spencer Weber Waller, *Antitrust and Social Networking*, 90 N.C. L. REV. 1771, 1793—96 (2012).

regulation generally.[42] The borderless flow of information over the Internet eludes traditional territorial-based jurisdiction and enforcement.[43] Until the EU conforms its policymaking to the Internet's architecture, ongoing regulatory efforts will promote, if anything, unintended anti-trust consequences rather than privacy objectives.

II. Regulating for Privacy in the Information Economy

A. Conventional Regulatory Scheme, Unconventional Internet

Omnibus privacy laws have been ineffective because they ignore the manner in which digital data is generated, transferred, and used in the Internet age.[44] Not only does information arrive on the monitor of a connected device through circuitous and often unpredictable routes, but its derivation can be similarly elusive.[45] Data origins evolve as digital data packets are augmented, duplicated, or otherwise altered.[46] When it *is* possible to pinpoint the origin of particular data, the servers and IP addresses from which the information originate are easily replaced or masked.[47]

Despite the nuances of transnational information flow, laws that seek to regulate such information derive from exemplars that existed long before the Internet.[48] The EU's seminal privacy law, the Data Directive, was enacted twenty years ago – well before Internet commercialization.[49] Such "early privacy law

---

42 See Tracie B. Loring, *Comment, An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States*, 37 TEX. INT'L L.J. 421, 424-25 (2002); Fred H. Cate, THE FAILURE OF FAIR INFORMATION PRACTICE PRINCIPLES, IN CONSUMER PROTECTION IN THE AGE OF "INFORMATION ECONOMY" 341 (Jane K. Winn ed., 2006).

43 See Miriam Wugmeister et al., *Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 GEO. J. INT'L L. 449, 449 (2007).

44 See Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 22–38 (2000) (explaining that the exact origin of any given data, or the nations, if any, associated with that data may be impossible or impracticable to discern).

45 *See id*; Curt Franklin, *How Internet Search Engines Work*, HOWSTUFFWORKS TECH, http://computer.howstuffworks.com/internet/basics/search-engine.htm (last visited May 6, 2016).

46 See Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 22–38 (2000); Curt Franklin, *How Internet Search Engines Work*, HOWSTUFFWORKS TECH, http://computer.howstuffworks.com/internet/basics/search-engine.htm (last visited May 6, 2016).

47 Eric J. Feigin, *Architecture of Consent: Internet Protocols and Their Legal Implications*, 56 STAN. L. REV. 901, 935—38 (2004); David Balaban, *What Do You Know About Proxy Servers?* INFORMATION SECURITY BUZZ (Apr. 15, 2016), http://www.informationsecuritybuzz.com/articles/know-proxy-servers/ (Proxy servers allow internet users to take a "side door" into a website to hide the user's identity.).

48 *See* LISA J. SOTTO, PRIVACY AND DATA SECURITY LAW DESKBOOK § 1.04 (2010).

49 1995 O.J. (L 281), available at http://eur-

could not have imagined, much less accounted for, the ubiquity and complexity of Internet communication."[50] And yet, modern privacy law continues to advance by accretion, building on earlier iterations of laws that did not contemplate today's technological reality.

In Europe, Nazi exploitation of personal information during World War II prompted robust privacy laws and the labeling of privacy as a fundamental right.[51] Nazis discovered and leveraged personal information – often religious, racial, and cultural – to destabilize occupied territory and identify those for deportation to concentration camps.[52] A series of treaties, charters, and accords stem from this historic catalyst, ultimately leading to the right to be forgotten.[53]

The United Nations adopted the Declaration of Human Rights soon after World War II, a portion of which promised that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence . . . ."[54] The European Union's Charter of Fundamental Rights more directly identified privacy rights in personal information by conferring the right to consent, access, and rectify personal information.[55] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data also targeted how personal data is collected, stored, transferred and altered.[56] The level of generality in Article 16 of the Consolidated Treaty on the Functioning of the European Union is noteworthy: "everyone has the right to the protection of personal data concerning [her]."[57]

---

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [hereinafter Data Directive].

50 McKay Cunningham, *Free Expression, Privacy, and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship*, 69 ARK. L. REV. 71, 72 102 (2016); see Dennis D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74 OHIO ST. L.J. 1029, 1033 (2013).

51 See Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1170 (2000).

52 See Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 609-10 (2007); David H. Flaherty, Nineteen Eighty-Four and After: Final Report of the Bellagio Conference on Current and Future Problems of Data Protection, GOV'T INFO. Q. 5 (1984) (reporting on a 1984 conference on data protection in which "one of the prime motives for the creation of data protection laws in continental Europe is the prevention of the recurrence of experiences in the 1930s and 1940s with Nazi and fascist regimes").

53 See Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH. 349, 356—60 (2015).

54 Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III), art. 12 (Dec. 10, 1948).

55 2000 O.J. (C 364/01), available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

56 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data arts. 5-6, 8-9, Jan. 28, 1981, 1496 U.N.T.S. 65.

57 Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 47, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN.

This framework remains at the heart of modern regulatory efforts. Europe's Data Directive ("Directive"), largely characterized as the most influential and progressive data privacy law worldwide,[58] is patterned from these legislative progenitors. The EU Directive legislates based on consent, access, transfer, and use – just as in previous Charters and Conventions. The Directive requires that personal data must be (1) processed fairly and lawfully, (2) collected for legitimate and specified reasons, (3) adequate, relevant, and not excessive in relation to the purposes for which it is collected, (4) accurate and, where necessary, kept up to date, and, (5) retained as identifiable data for no longer than necessary to serve the purposes for which the data were collected.[59]

A new European privacy law will soon replace the Directive.[60] The forthcoming General Data Protection Regulation ("Regulation") directly binds EU member states, unlike the current Directive, which merely requires that member states enact national laws similar in spirit to the Directive.[61] True to form, the new Regulation again legislates by accretion, mirroring the Directive's structure and many of its provisions, while also adding new privacy rights and steeper penalties for privacy violations.[62] The Regulation, effective in 2017, legislatively confirms the CJEU ruling by expressly codifying the right to be forgotten.[63]

B. The Right to Be Forgotten

The Regulation states that EU residents may "have their data fully removed when it is no longer needed for the purposes for which it was collected."[64] Removable data includes text, video, photographs, and other forms of information published in various contexts including links accessed by search engines and

---

58 *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 55–88 (2000); Christopher Kuner, *The European Union and the Search for an International Data Protection Framework*, 2 GRONINGEN J. INT'L L. 55, 55 (2014) (characterizing "E.U. law as the most influential body of data protection law worldwide.")

59 Data Directive, *supra* note 51.

60 Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25 2012). [hereinafter Data Regulation].

61 *See* Treaty on European Union [Maastricht Treaty] art. 288, Feb. 7, 1992, 1992 O.J. (C 191) 1, 1759 U.N.T.S. 3.

62 *Id.*

63 *Id.*; See Press Release, *Eur. Comm'n, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote*, EUROPEAN COMMISION (Mar. 12, 2014),. http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

64 *See* Press Release, *Data Protection Reform – Frequently Asked Questions*, EUROPEAN COMMISION, (Nov. 4, 2010), http://europa.eu/rapid/press-release_MEMO-10-542_en.htm?locale=EN (stating that "People who want to delete profiles on social networking sites should be able to rely on the service provider to remove personal data, such as photos, completely").

websites themselves.[65] While lauded by privacy advocates, the new EU law sacrifices implementation for aspiration. Without regard to how data is gathered, duplicated, stored, transferred and used, the right to be forgotten can be enforced erratically, if at all.[66] The Regulation's Article 17, entitled "Right to Erasure" provides:

> The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, and to obtain form third parities the erasure of any links to, or copy or replication of that data…

This provision bolsters the CJEU's ruling in the Costeja case by legislatively recognizing the right to be forgotten. Like the court's ruling, the Regulation confirms a sweeping new right. The new right aligns with Europe's policy goals and tracks earlier laws that prescribe the collection, use, and transfer of personal information. But it again leaves questions of jurisdiction and enforceability to afterthought. If EU policymakers flipped their legislative approach by crafting privacy laws around jurisdiction and enforceability, it would reveal the inanity inherent in data privacy laws that fail to account for how data is generated, used, and transferred in the Internet age.

C. Transnational Data flow, Over-inclusive Terms, and Extra-jurisdictional Reach

It is not easy complying with the right to be forgotten as well as with the notice, consent, use, and transfer requirements required under the EU Directive and forthcoming Regulation. Most multinational companies have restructured leadership positions, appointing Chief Privacy Officers to oversee compliance with laws like the EU Directive.[67] Under the Directive, organizations and individuals who process personal data must provide notice before collecting it[68] and obtain consent that is a "freely given, specific and informed indication of [the resident's] wishes."[69] After providing notice and obtaining consent, personal data may only be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[70] In many cases, an EU

---

65 *See* Press Release, *Data Protection Reform – Frequently Asked Questions*, EUROPEAN COMMISION, (Nov. 4, 2010), http://europa.eu/rapid/press-release_MEMO-10-542_en.htm?locale=EN (stating that "People who want to delete profiles on social networking sites should be able to rely on the service provider to remove personal data, such as photos, completely").

66 See *infra*, Part IV b.

67 See Abraham Newman, *European Data Privacy Regulation on a Global Stage: Export or Experimentalism?, in* EXTENDING EXPERIMENTALIST GOVERNANCE? THE EUROPEAN UNION AND TRANSNATIONAL REGULATION 236—39 (Jonathan Zeitlin ed., 2015).

68 Data Directive, *supra* note 51, art. 7; Data Regulation, *supra* note 62, art. 6.

69 Data Regulation, *supra* note 62, art. 2(h).

70 Data Regulation, *supra* note 62, art. 6(1)(b).

resident maintains authority to access and correct the personal data processed by an organization or individual.[71] Most recently, EU residents have gained the power to have it deleted altogether through the right to be forgotten[72] These provisions along with the increasing fines levied by European officials for non-compliance, create a substantial burden on individuals and entities that process personal data.

European officials were aware of the hardships the law created. Compliance would be expensive and uncertain. Non-compliance created liability exposure both financially and politically. Because digital information can be collected, used, and transferred anywhere, the law unintentionally incentivized companies to relocate out of jurisdictional reach.[73] To forestall an exodus of information-reliant businesses, European policymakers engrafted extra-jurisdictional provisions in both the Directive and the Regulation.[74] The European Commission justified the long reach of the law by noting that "[w]ithout such precautions, the high standards of data protection established by the Data Protection Directive would quickly be undermined, given the ease with which data can be moved around in international networks."[75]

In other words, the Directive and forthcoming Regulation apply broadly and include extra-jurisdictional provisions. The laws apply by definition to "controllers" and/or "processors" who "process"[76] the "personal information" of EU residents. The laws define these terms so broadly it is difficult to know who does not have to comply.[77] Personal data is:

> Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or

---

71 Date Regulation, *supra* note 62, art.6. Those who control private data must also protect it. Data Regulation, *supra* note 62, art. 17. Protecting personal data requires that process it to "implement appropriate technical and organizational measures to protect personal data against . . . destruction or . . . loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network."

72 Case C-131/12, Spain SL, Google Inc. v. Mario Costeja González, 2014 O.J. C 212/4. *See also* European Commission Factsheet, *supra* note 1.

73 *See* EUROPEAN COMMISSION WEBSITE, http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm (last visited Apr. 13, 2016).

74 *Id*; see Christopher Kuner, *The European Union and the Search for an International Data Protection Framework*, 2 GRONINGEN JNL. INT'L L. 2 (2014).

75 *See* EUROPEAN COMMISSION WEBSITE, http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm (last visited Apr. 13, 2016).

76 *See* Data Directive, *supra* note 51, art. 2 (defining as processing as "[A]ny operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.").

77 Liat Clark, *ICO Commissioner Slams EU Data Protection Directive*, WIRED (Feb. 7, 2013), http://www.wired.co.uk/news/archive/2013-02/07/ico-against-eu-data-protection.

more factors specific to his physical, physiological, mental, economic, cultural or social identity.[78]

Identifying information that directly connects to a person, like home address, national identification number, and personal financial data clearly fall within this definition. But the definition, and subsequent interpretation, subsumes more than data directly identifying a person. It includes data that *could* lead to identification.[79] Information is "personal," according to European officials, even though "the person has not been identified yet, it is possible to do it."[80] The European Working Party, responsible in part for interpreting the Directive, announced that "information need not identify an individual directly to constitute 'personal data,' but the mere fact that the information is related to an individual capable of being identified results in the data being "personal data" under the Directive."[81]

The new Regulation builds on the capacious scope of "personal data" by defining it as "any information relating to a data subject."[82] The operative character of these critical definitions is inclusion rather than delimitation. One professor quipped that "neighborhood children who record orders for Girl Scout cookies" are "processors" of "personal information."[83] Professors Paul Schwartz and Daniel Solove note that Europe's data privacy law arguably applies to anyone engaging in any commerce within the European Union or with residents therefrom.[84]

As noted above, these broad definitions are not circumscribed to those within the territorial boundaries of the European Union. The Directive and Regulation amplify broad definitions with extra-territorial provisions. First, both laws prohibit transfer of personal data outside the E.U. unless the law's requirements are met.[85] Only nations with "adequate" data privacy laws may

---

78 Data Directive, *supra* note 51, art. 2.

79 *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1819 (2011); European Commission, Article 29 Data Protection Working Party, Opinion 1/2008 on Data Protection Issues Related to Search Engines, 00737/EN/WP148, 4 April 2008, 3, 8, available online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf (WP148).

80 *See Article 29 Data Protection Working Party*, (2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (Opinion on the Concept of Personal Data).

81 McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. REV. 643, 656—57 (2012).

82 Data Regulation, *supra* note 62, art 4.

83 *See* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 183 (1999).

84 Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1817, 1874—76 (2011).

85 Data Directive, *supra* note 51, art. 25; Data Regulation, *supra* note 62, art. 41 ("A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international

receive data transfers from within the E.U.[86] European officials, however, have identified only eleven nations as "adequate."[87] To avoid truncating Europe's international commerce by allowing data transfers to only eleven countries,[88] the Directive offers other avenues for transfer to those countries that are "inadequate," like the U.S.[89] Strict contractual agreements and "Binding Corporate Rules," import the Directive's strictures to individual organizations.[90] The Directive allows very little margin for parties to alter or manipulate the model contracts or binding corporate rules.[91]

Another extra-territorial provision ties the Directive's applicability to "equipment" within the E.U. The provision disregards where the data processing takes place or where the processor resides. It focuses instead on whether any European "equipment" was involved in the data transfer.[92]

> Each Member State shall apply … this Directive to the processing of personal data where: (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.[93]

Any transaction involving an E.U. resident likely falls within this provision if the transaction occurs online. It captures all e-commerce with Europeans, presuming

---

organisation in question ensures an adequate level of protection.").

86 Data Directive, *supra* note 51, art. 25(1), pmbl. ¶ 57.

87 *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries,* EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last visited May 6, 2016) (listing Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection).

88 *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 39 (2000).

89 The principal avenues for U.S. companies seeking to comply with the E.U. Directive and thereby receive personal information from the E.U. include obtaining actual consent of the data subject, standard contractual clauses, binding corporate rules, and until recently, participation in the Safe Harbor program. *See* Data Directive, supra note 51, art. 26; Article 29 Data Protection Working Party, Working Document: Transfers of Personal Data to Third Countries: Applying Article 26(2) of the E.U. Data Protection Directive to Binding Corporate Rules for International Data Transfers, at 5-6, 11639/02/EN, WP 74 (June 3, 2003).

90 *See* Data Directive, supra note 51, art. 26(2); Article 29 Data Protection Working Party, Working Document: Transfers of Personal Data to Third Countries: Applying Article 26(2) of the E.U. Data Protection Directive to Binding Corporate Rules for International Data Transfers, at 5-6, 11639/02/EN, WP 74 (June 3, 2003).

91 See id.

92 Data Directive, *supra* note 51 art. 4.

93 Id.

that E.U. residents use a laptop, smart phone or other such device to facilitate the interaction.[94]

The new Regulation abandons the equipment nexus. The Regulation, however, does not abandon an extra-territorial reach. Instead of an equipment nexus, the Regulation applies to all non-EU entities that offer goods or services to persons in the E.U.[95] Dan Jerker B. Svantesson characterizes this provision as "bring[ing] all providers of Internet services such as websites, social networking services and app providers under the scope of the EU Regulation as soon as they interact with data subjects residing in the European Union."[96]

It appears that European policymakers sought to protect the personal data of E.U. residents regardless of where it is processed.[97] "[B]ecause of the scope of the Data Protection Directive, any business that has contact with EU residents on anything other than an anonymous cash-only basis has effectively collected some form of personal data and thus would be subject to the Data Protection Directive."[98] Accordingly, both the Directive and Regulation diverge from normative jurisdictional law.[99]

In one sense, these extra-jurisdictional provisions are critical. They are vital to a privacy law modeled on pre-Internet progenitors. Without a scope that applies to anyone who "processes" information that feasibly relates to a European, the law is too easily circumvented by proxy servers and off-shore enterprises. But the law's over-broad scope generates a raft of negative secondary effects.[100] It restricts a host of innocent companies and individuals, whose information use does not harm Europeans' privacy.[101] It invites uneven enforcement by data privacy

---

94 John T. Soma et al., *An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./E.U. E-Commerce Privacy Safe Harbor*, 39 TEX. INT'L L.J. 171, 205—06 (2004).

95 *See* Data Regulation, supra note 62, art. 3.

96 Dan Jerker B. Svantesson, *Extraterritoriality in Data Privacy Law*, 107 (Ex Tuto Publishing, 2013).

97 See Christopher Kuner, *The European Union and the Search for an International Data Protection Framework*, 2 GRONINGEN JNL. INT'L L. 55 (2014).

98 John T. Soma et al., *An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./E.U. E-Commerce Privacy Safe Harbor*, 39 TEX. INT'L L.J. 171, 205 (2004).

99 Data Directive, *supra* note 51 art. 4 (Article 4 of the Directive states that if a data controller is located outside the EU, but uses equipment within the EU for any purpose other than transmission, the law of the Member State where the equipment is located will apply); *Yahoo! Inc. v. La Ligue Conlre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1205—11 (9th Cir. 2006); *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 39 (2000) ("Were a country that attracted little U.S. trade and investment to restrict data transfers to the United States, a ban would pose little harm to overall U.S. commercial interests because of the small size of the country's market.").

100 See *supra*, Part III.

101 See *supra*, Part III (A).

officials who can indiscriminately select disfavored entities for prosecution[102]. Finally, it disregards the sovereignty of other nations by imposing European privacy law extra-jurisdictionally.[103]

III. E.U. Privacy Law, Negative Secondary Effects

A. Innocent (Harmless) Processing

The extra-territorial reach of European privacy law, viewed as necessary to capture transnational information flow,[104] renders the law grossly over-inclusive. Countless innocuous transactions fall within the law's ambit, exposing harmless individuals and organizations to liability under the extra-territorial provisions. A small business in rural Ohio violates European privacy law if it conducts any business of any kind with a European resident and fails to adhere to the Directive's mandates. Indirect connections to European data through social media, business contact lists, and websites that require registration, for example, also prompt compliance.[105] The scope of innocents caught by the law broadens when considering the law's application to data that could feasibly *enable* the holder to connect it to a specific person, even if the holder herself cannot make the connection.[106] Through such a capacious scope, the law captures an ocean of "innocent" activities – data processing that threatens no privacy harm to European citizens.[107]

Some institutions, seeking to avoid European privacy restrictions, attempted to anonymize European personal information and thus claim that they had not processed "personal information" and need not comply with the law. Re-identification software, however, forestalls such a strategy, broadening the law's reach over harmless transactions even further. Professor Paul Ohm, among others, confirms that even information that remotely or tangentially relates to a

---

102 See *supra*, Part III (B).

103 See *supra*, Part III (C).

104 See id.

105 *See* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 183 (1999).

106 *Id*.

107 Applying this definition of "personal information" to the right to be forgotten also broadens the scope of the right to be forgotten. It amplifies the range of data that is subject to deletion since the right to be forgotten is tethered to an E.U. resident's "personal information." As noted above, the definition and subsequent interpretation of that term reaches far beyond its denotation. It reaches beyond a request to delete photographs or links to Facebook profiles. It includes IP addresses, search histories, anonymized locational data, meta-data and a host of other data because that data could enable the holder to eventually link it to the data subject. See Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1819 (2011).

person can be de-coded and matched once again with the proper individual.[108] "The emergence of powerful re-identification algorithms demonstrates…the fundamental inadequacy of the entire privacy protection paradigm based on 'de-identifying' the data."[109] De-anonymizing algorithms can leverage as few as three data points to connect "anonymous" data to an individual.[110] Given the ubiquity of data points already available, "any attribute can be identifying in combination with others."[111] In fact, the more data available, the less any of it can be said to be private.[112] Through broad definitions of "personal data" and "processing" and through extra-territorial provisions that expand its applicability, European privacy law captures a sea of innocuous transactions, revealing the wide gap between the privacy law and the harms it purports to redress.

B. Discretionary Enforcement

Europe's privacy law has been criticized due to inherent unfairness that attends enforcement of an over-broad law.[113] Applied literally, officials could seize almost any laptop or smartphone at the European border in light of the Directive's near-universal application.[114] Enforcement of laws that incriminate a disproportionately large ratio of those governed by it, or that are so broad as to capture the entire body politic have historically been declared invalid in the US.[115] They give enforcement officers carte blanche authority to prosecute disfavored citizens, prompting corruption over compliance.[116]

---

108 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1706–1718 (2010).

109 Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of "Personally Identifiable Information,"* 53 COMM. ACM 24, 24–26 (2010).

110 See *id*.

111 Id.

112 Patrick Tucker, *Has Big Data Made Anonymity Impossible?* MIT TECH. REV. (May 7, 2013), onlitechnologyreview.com/news/514351/has-big-data-made-anonymity-impossible/.

113 *See* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 183 (1999).

114 See id.

115 *See People v Raphael Golb*, 2014 NY Slip Op 03426, Decided on May 13, 2014 Court of Appeals Abdus-Salaam, J. Published by New York State Law Reporting Bureau pursuant to Judiciary Law, Section 431; *People v Dietze* 75 NY2d 47 (1989), striking down a similar harassment statute, former Penal Law, Section 240.25, which prohibited the use of abusive or obscene language with the intent to harass, annoy or alarm another person; Leland, J., *Top Court Champions Freedom to Annoy*, NY TIMES (13 May 2014), nytimes.com/2014/05/14/nyregion/top-court-champions-freedom-to-annoy.html?_r=0 (last visited 17 October 2014); *see generally,* Chicago v. Morales, 527 U.S. 41 (1999) (A law cannot be so vague that a person of ordinary intelligence cannot figure out what is innocent activity and what is illegal).

116 See id; *but see*, John C. O'Quinn, book note, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, 12 HARV. J.L. & TECH. 683, 691 (2000) (noting a "more cooperative approach to enforcement generally taken toward regulatory regimes in Europe," and highlighting "the role of discretionary approach to enforcement that is taken in Europe").

By reaching anyone who processes EU personal data or data that could eventually lead to personal data, the law creates a conundrum; "Europe cannot strictly enforce the letter of the Directive and at the same time announce that organizations can routinely ignore it."[117] As a result, some commentators questioned whether the Directive was itself a bluff.[118] "Because the data-flow restrictions are potentially so harmful not only to third-party nation economies, but also to Europe's economy itself, one has to wonder whether the risk of noncompliance is really significant."[119] Literal enforcement would effectively truncate the European market from the international economy.[120]

And yet, European officials have prosecuted multiple companies and imposed millions of dollars in fines. In December 2014, a German data protection commissioner levied a €1,300,000 fine on the insurance group Debeka for failing to administer internal controls over personal information.[121] In France, data protection officials fined Google €150,000 because Google had not adequately informed users how it processes personal information, including violations relating to consent for cookie usage, unclear data retention terms, and personal data collected without adequate legal basis.[122] There is an abundance of other enforcement actions under the Data Directive, mostly prosecuting a selection of large businesses.[123] These prosecutions suggest uneven application of the law because they target specific entities among a ubiquity of violations.[124]

Notably, the Directive does not directly bind Member States. Instead, it requires that each Member State enact its own privacy law consonant with the Directive's spirit.[125] As a result, each Member State drafted discrete privacy laws and each Member State retains discretion regarding implementation and enforcement.[126] This fragmented approach compounds inconsistent enforcement. It will change, however, with the enactment of the forthcoming Regulation, which directly binds Member States and which carries a heightened price for non-

---

117 Peter P. Swire & Robert E. Litan, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE, 155 (Brookings Institution Press 1998).

118 *Id.*

119 Steven R. Salbu, *Regulation of Borderless High-Technology Economies: Managing Spillover Effects*, 3 CHI. J. INT'L L. 137, 141 (2002).

120 *Id.*

121 Johanna Laas, *Germany: DPA Imposes Fine on Insurance Company*, PRIVACY EUROPE (Jan. 7, 2015), https://www.privacy-europe.com/blog/germany-dpa-imposes-fine-insurance-company/.

122 Geert De Clercq, *France Fines Google Over Data Privacy*, REUTERS (Jan. 8, 2014), http://www.reuters.com/article/us-france-google-fine-idUSBREA0719U20140108.

123 See Sotto, § 18.02[A] 4, b, 9 (listing notable enforcement examples).

124 See id.

125 See Treaty on European Union [Maastricht Treaty] art. 288, Feb. 7, 1992, 1992 O.J. (C 191) 1, 1759 U.N.T.S. 3; Data Directive, *supra* note 51, art. 28.

126 *Id.*

compliance: the greater of €100,000,000 or 5% of annual worldwide turnover.[127] Although the Regulation harmonizes previously disparate laws of the twenty-eight Member States, discretionary enforcement will continue under the Regulation due to its nebulously broad scope.

C. Spurned Sovereignty

As noted above, both the Directive and Regulation include extra-jurisdictional provisions. Those provisions, in part, seek to prevent the exodus of data-reliant businesses.[128] They also purport to capture transnational data flow by restricting entities that have no physical presence in Europe.[129] If a European citizen contacts an Idaho company, which then sells its product through an Internet exchange, the Directive applies to the Idaho company, which otherwise had no contact with Europe.[130] By using "equipment" located in Europe (the buyer's laptop or smart phone) to consummate the Internet sale, Article 4 of the Directive purports to capture the Idaho company.[131]

The right to be forgotten, in like manner, will soon stretch beyond Europe's borders. Google resists universal application of the right to be forgotten, arguing that it only applies to European domain names – searches that are directed toward users in Europe.[132] A request for data erasure from a Frenchman, for example, would only affect google.fr. rather than searches under all Google domain names.[133] Google has a strong argument, given the fact that ninety-five percent of European users search Google under their respective country's domain name.[134]

---

127 Data Regulation, *supra* note 62.

128 *See* EUROPEAN COMMISSION WEBSITE, http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm (last visited Apr. 13, 2016) ("Without such precautions, the high standards of data protection established by the Data Protection Directive would quickly be undermined, given the ease with which data can be moved around in international networks.").

129 Data Directive, *supra* note 51 art. 4; Data Regulation, supra note 62, art. 3; John T. Soma et al., *An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./E.U. E-Commerce Privacy Safe Harbor*, 39 TEX. INT'L L.J. 171, 205—06 (2004).

130 Data Directive, *supra* note 51 art. 4

131 Id. See John T. Soma et al., *An Analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The U.S./E.U. E-Commerce Privacy Safe Harbor*, 39 TEX. INT'L L.J. 171, 205—06 (2004).

132 *See* Sam Schechner & Frances Robinson, *EU Says Google Should Extend 'Right to Be Forgotten' to '.com' Websites*, WALL STREET JOURNAL (Nov. 26, 2014), http://www.wsj.com/articles/eu-says-google-should-extend-right-to-be-forgotten-to-com-websites-1417006254.

133 *See* Ravi Antani, *The Resistance of Memory: Could the European Union's Right to be Forgotten Exist in the United States?* 30 BERKELEY TECH. L.J. 1173, 1178 (2015).

134 See Peter Fleischer, "Response to the Questionaire addressed to Search Engines by the Article 29 Working Party regarding the implementation of the CJEU judgment on the "right to be forgotten," July 31, 2014, 3-4.; Brendan Van Alsenoy & Marieke Koekkoek, *The Extra-territorial Reach of the EU's "Right to be Forgotten,"* INTERDISCIPLINARY

Limiting the scope of the right to be forgotten through domain names is not the only alternative. Geographic filtering, for which software already exists, more closely approximates territorial jurisdictional limitations by deleting data under the right to be forgotten only for those searches conducted in relevant European countries.[135] All searches conducted in Germany, for example, would conceal personal information that Germans and/or Europeans successfully erased under the right to be forgotten.[136] Identical searches conducted in the U.S. would not.

The CJEU's ruling was unclear on this point.[137] It did not specify that Google must de-list all links across all domain extensions and/or all geographic boundaries.[138] As a result, Google currently limits data deletions to European domains.[139] A search for Mario Costeja on "google.fr" will reveal his old debt; the same search under Google's Spanish domain will not.[140] Google searches under European domains prompt the following alert: "some results may have been removed under data protection law in Europe."[141] This present-day disclaimer reveals that Jennifer Granick's prediction was not too far afield when she posited that the right to be forgotten "marks the beginning of the end of the global Internet, where everyone has access to the same information, and the beginning of an Internet where there are national networks..."[142] The Internet of Spain is not the Internet of France or the Internet of the U.S.[143]

But national differences in information access may not last long. European officials recently signaled disapproval of the approach, characterizing it as unsatisfactory and easily circumvented. The Article 29 Working Party, tasked with implementation of European data privacy law,[144] unequivocally rejected

---

CENTRE FOR LAW AND ICT (Jan. 19, 2015), http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2551838.

135 See generally, Kevin F. King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61, 66-68, 91-92 (2011); A. Benjamin Spencer, *Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network-Mediated Contacts*, 2006 U. ILL. L. REV. 71, 80-85 (2006).

136 See id.

137 See Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, Mario Costeja González (May 13, 2014), *available at* http:// curia.europa.eu.

138 Id.

139 *See* Ravi Antani, *The Resistance of Memory: Could the European Union's Right to be Forgotten Exist in the United States?* 30 BERKELEY TECH. L.J. 1173, 1177—79 (2015);

140 *See id*.

141 *See* Charles Arthur, *What is Google deleting under the "right to be forgotten" – and why?*, THE GUARDIAN (June 4, 2014), http://www.theguardian.com/technology/2014/jul/04/what-is-google-deleting-under-the-right-to-be-forgotten-and-why.

142 Toobin, *supra* note 5.

143 *See* Ravi Antani, *The Resistance of Memory: Could the European Union's Right to be Forgotten Exist in the United States?* 30 BERKELEY TECH. L.J. 1173, 1178 (2015).

144 Article 29 Data Protection Working Party, "Guidelines on the implementation of the Court of the Justice of the European Union judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales" – C-

application of the right to be forgotten through domain extensions:

> [D]e-listing decisions must be implemented in a way that guarantees the effective and complete protection of these rights and that EU law cannot be easily circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment. In practice, this means that any case de-listing should also be effective on all relevant domains, including .com.[145]

A French data protection authority recently confirmed this admonition when it ordered Google to remove links from its database entirely, across all domains.[146] Harvard Professor, Jonathan L. Zittrain, noted that "France is asking Google to do something here in the U.S. that if the U.S. government asked for, it would be against the First Amendment."[147] Google has thus far refused to comply, but the French pronouncement reflects the Working Party's statement as well as the forthcoming Regulation.[148] The Regulation not only legislatively memorializes the right to be forgotten, but according to the European Commission website, it also "leaves no legal doubt that no matter where the physical sever of a company processing data is located, non-European companies, when offering services to European consumers, must apply European rules."[149]

Upon the Regulation's enactment, one person on the other side to the globe will determine what the rest of us see. A German citizen's request to erase Internet content will blot that information not only from searches conducted on google.de but also on google.com.[150] It will delete links not only in Munich, but also in Philadelphia, New Delhi, Auckland and all points in between.[151] The 657,000 links that have already been de-listed in Europe under the right to be forgotten would disappear from Google searches entirely, or as the Working Party terms it, "effectively and completely."[152] Under this approach, European law unilaterally determines global information access.

Extra-territorial laws, like Europe's privacy Regulation, undermine national sovereignty and democratic principles. "France has no territorial

---

131/12 (2014) WP225, ¶ 20.

145 *Id*.

146 Farhad Manjoo, *Right to be Forgotten Online Could Spread*, THE NEW YORK TIMES (Aug. 5, 2015) http://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html?_r=0.

147 *Id*.

148 See Julia Fioretti & Mathieu Rosemain, *Google appeals French order for Global "right to be forgotten,"* REUTERS, (May 19, 2016) available at, http://www.reuters.com/article/us-google-france-privacy-idUSKCN0YA1D8.

149 *Factsheet on the "Right to be Forgotten" Ruling* (2014), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [hereinafter *Factsheet*]. *Factsheet*, *supra* note 3.

150 See Data Regulation, *supra* note 62.

151 See id.

152 See id.

jurisdiction over the U.S., but it's purporting to tell Google to delete content from the U.S. market, the Canadian and Mexican markets, and others."[153] Citizens of non-European countries did not vote and had no representation in determining the right to be forgotten, but the law purports to directly impact non-European citizens. One European commentator blithely acknowledged the lack of comity:

> [W]e may be tempted to say that when our courts conclude that certain content is to be blocked or removed, we want that blocking or removal to be global. However, [many people] may not necessarily wish for Internet intermediaries to engage in global blocking/removal based on court orders from other countries in the world – particularly where such court orders stem from restrictive, undemocratic laws with an extraterritorial effect.[154]

Unilateral and extra-jurisdictional laws derogate normative international comity.[155] They ignore democratic values,[156] and in many cases, they upend alternative privacy protection regimes that tailor legal restrictions to the harms that result from privacy breaches.[157] Extra-territorial privacy laws promote one culture's devotion to privacy over another culture's preference for free expression.[158] Finally, they lay out an unfortunate blueprint for other nations to do likewise.[159] The EU Directive and Regulation are one-way ratchets.[160] Other nations, in the name of privacy, can restrict more information than the EU, but they cannot go the other way by providing more access to information.[161] It is entirely possible that "there will be a race to the bottom towards adopting the

---

153 Terry Carter, *Erasing the News: Should Some Stories be Forgotten?* ABA JOURNAL, Jan. 1, 2017 (quoting Jonathan Peters, Chair of the First Amendment subcommittee of the ABA Section of Litigation).

154 Dan Jerker B. Svantesson, *Delineating the Reach of Internet Intermediaries' Content Blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach?"*, 11 SCRIPTed 153, 155 (2014), http://script-ed.org/wp-content/uploads/2014/10/svantesson.pdf. Svantesson, *supra* note 5.

155 Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH. 349, 409 (2015) (asking what country's law applies among the hundreds of countries regulating the Internet and noting that an "Islamic fundamentalist female might be held in contempt for appearing on a website that shows her unveiled face" in some countries but not others).

156 Dan Jerker B. Svantesson, *Delineating the Reach of Internet Intermediaries' Content Blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach?"*, 11 SCRIPTed 153, 155 (2014), http://script-ed.org/wp-content/uploads/2014/10/svantesson.pdf. Svantesson, *supra* note 5.

157 See *infra*, Part VI.

158 *See* Robert Krulwich, *Is the 'Right to be Forgotten' the 'Biggest Threat to Free Speech on the Internet'?*, NPR (Feb. 24, 2012, 9:06 AM), http://www.npr.org/blogs/krulwich/2012/02/23/147289169/is-the-right-to-be-forgotten-the-biggest-threat-to-free-speech-on-the-internet; Robert K. Walker, *The Right to be Forgotten*, 64 HASTINGS L.J. 257, 274—76 (2012).

159 Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH. 349, 409 (2015).

160 Id.

161 Id.

norms of the most restrictive legal system."[162]

IV. EU Privacy Law, Impotent Primary Effect

The Directive and Regulation attempt to capture borderless digital information through provisions that have near-universal application. The breadth of the law carries secondary negative effects, including discretionary enforcement and a disregard for international sovereignty.[163] But perhaps these negative secondary effects are necessary to achieve the law's primary goal – European data privacy. The central tenant of this paper suggests that even broadly applicable laws founder when purporting to regulate personal information because they do not account for the Internet's resilience and the digital architecture of information flow.

A. Search Engines

The right to be forgotten applies to search engines, not individual web pages.[164] In *Google Spain*, the CJEU required only that Google de-link Costeja's name from the newspaper article that originally published Costeja's debt.[165] The Court did not require the newspaper to take down the offending information from its website.[166] In thousands of deletion requests that followed, implementation was similarly limited to de-listing links rather than requiring data erasure from websites.[167]

The BBC, Wikipedia and others continue to publish articles on their respective websites even though Google de-listed links to those websites in compliance with the right to be forgotten.[168] In other words, the websites that

---

162 Id.

163 See *supra*, Part IV.

164 Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH. 349, 374 (2015) ("After Google approves a takedown request, the requestor's name and other personal information would still exist on other web pages, which would not lead to the actual 'forgetting' of any such information.").

165 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, Mario Costeja González (May 13, 2014), *available at* http:// curia.europa.eu;

166 Id.

167 See European Commission Factsheet, *supra* note 1.

168 Neel McIntosh, *List of BBC Web Pages Which have been Removed from Google's search results*, BBC INTERNET BLOG (June 25, 2015), http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379; *Notices Received from Search Engines*, WIKIPEDIA, https:// wikimediafoundation.org/wiki/Notices_received_from_search_engines (last visited July 11, 2016); Subreddit, *Things That Were Not Meant to be Forgotten*, available at https://www.reddit.com/r/nevertoforget/? (described as a "forum to post articles that have been removed by Google from search results as a consequence of the righto to be

contain illicit E.U. personal information still exist; the most frequently used path to that information does not. The European Commission tacitly confirmed this approach, positing a hypothetical in which a deletion request results in Google de-listing links rather than requiring that each website scrub the offending personal information.[169] The personal information remains, it is just more difficult to access using a Google search.

Implementing the right to be forgotten in this way presupposes only one or two search engines, a logical supposition in 2011 when Google dominated the market with 82.5% market share.[170] By 2015, however, Google's market share had slipped to 66.41%,[171] and "is now likely in permanent decline."[172] The search engine DuckDuckGo, by contrast, grew over 70% in 2015, receiving 3.25 billion search queries.[173] It attracted three million new searchers in October 2015 alone, representing more than 100% year-over-year growth.[174]

Google, Bing, Yahoo!, AOL, and Ask formerly comprised the world's most popular search engines,[175] but scores of others exist, and several are regionally dominant.[176] Yandex has a 61.9% market share in Russia, while Baidu is China's most popular search engine.[177] Naver accounts for over 70% of South Korea's

---

forgotten); *see also* Geoff Brigham & Michelle Paulson, *Wikipedia Pages Censored in European Search Results*, WIKIMEDIA BLOG (Aug. 6, 2014), https://blog.wikimedia.org/2014/08/06/wikipedia-pages-censored-in-european-search-results.

169 See European Commission Factsheet, *supra* note 1.

170 *Desktop Search Engine Market Share*, NETMARKETSHARE, https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0&qptimeframe=Y (last visited May 8, 2016). In the United States, one 2015 study showed Google's share at 63.8%. See *comScore Releases August 2015 U.S. Desktop Search Engine Rankings*, COMSCORE (September 16, 2015) https://www.comscore.com/Insights/Rankings/comScore-Releases-August-2015-U.S.-Desktop-Search-Engine-Rankings.

171 *See id.*

172 See Dan Frommer, *The Product that Made Google has Peaked for Good*, QUARTZ (Dec. 15, 2015), http://qz.com/573361/the-product-that-made-google-has-peaked-for-good/.

173 See Dan Frommer, *DuckDuckGo, The Search Engine that Doesn't Track its Users, Grew More than 70% this Year*, QUARTZ (Dec. 16, 2015), http://qz.com/574853/duckduckgo-the-search-engine-that-doesnt-track-its-users-grew-more-than-70-this-year/.

174 *Id.*

175 See Amy Gesenhues, *Study: Top 5 Search Engines See Search Traffic Drop By As Much As 31% Since December 2013*, SEARCH ENGINE LAND (June 24, 2014) http://searchengineland.com/study-google-bing-yahoo-ask-aol-see-17-32-decline-search-traffic-last-6-months-194634.

176 *See* Julie Marie Bedas, *Search Engines Across the Globe, Know more about the Leading Search Engines in terms of Internet Usage*, FOUNDER'S GUIDE (July 10, 2015) http://foundersguide.com/search-engines-across-the-globe/.

177 *See id.*; Konrad Krawczyk, *Google is Easily the Most Popular Search Engine, But Have you Heard Who's in Second?* DIGITAL TRENDS, (July 3, 2014) http://www.digitaltrends.com/web/google-baidu-are-the-worlds-most-popular-search-engines/ (identifying Baidu as the second largest search engine in the world).

searches,[178] and Yahoo! Japan services most searches in that country.[179] Other general search engines include Exalead, Gigablast, Munax, Qwant, Sogou and Youdao.[180]

Not only are the number and popularity of alternative search engines growing, so is their diversity. Generalized web search engines like Google now compete with selection-based search engines, metasearch engines, web portals, apps, and vertical market websites that embed search functions within them.[181] Others are customized to trades, like IFACnet (accountancy), Fashion Net (fashion), and GlobalSpec (business).[182] Importantly, some search engines self-restrict by geography, including Accoona (China and United States), Ansearch (Australia, United States, United Kingdom, New Zealand), Biglobe (Japan), Maktoob (Arab world), Rediff (India), Seznam (Czech Republic) and many more.[183] Customized search engines exist for food recipes, job searches, legal and medical information, news, real estate and more.[184]

This proliferation reflects the decline in traditional and generalized desktop searching.[185] One study shows that the total number of people using traditional search engines decreased from 55% in the first quarter of 2014 to 49% in the first quarter of 2015.[186] More and more searches occur on mobile devices, through apps, and through social media.[187] According to Abid Chaudhry, a senior director at BIA/Kelsey, local searches on mobile apps are increasingly taking share, given that 86% of users' time on a mobile device is spent on an app.[188] "Mobile behavior, marketplaces like Amazon, social sites such as Facebook, and shrinking screen sizes continue to introduce quicker, smarter and more vocal ways of finding information, services and products. In fact, the number of people using search

---

178 *See* Julie Marie Bedas, *Search Engines Across the Globe, Know more about the Leading Search Engines in terms of Internet Usage*, FOUNDER'S GUIDE (July 10, 2015) http://foundersguide.com/search-engines-across-the-globe/.

179 *See id*.

180 See Search the World, A better way to search globally, (August 19, 2015) http://srch.3dmovies.com/2015/08/19/hello-world/.

181 See Laurie Sullivan, *Search Engines Struggle To Keep Web Traffic*, MEDIA POST (Dec. 18, 2015), http://www.mediapost.com/publications/article/265120/search-engines-struggle-to-keep-web-traffic.html.

182 A list of search engines delineated by trade, geographic scope, specific type of information sought and more can be found at *Search Engines*, Fashion, (last visited July 25, 2016) http://efemale.blogspot.com/2015/01/search-engines.html.

183 See Search the World, A better way to search globally, (August 19, 2015) http://srch.3dmovies.com/2015/08/19/hello-world/.

184 A list of search engines delineated by trade, geographic scope, specific type of information sought and more can be found at *Search Engines*, Fashion, (last visited July 25, 2016) http://efemale.blogspot.com/2015/01/search-engines.html.

185 Laurie Sullivan, *Search Engines Struggle To Keep Web Traffic*, MEDIA POST (Dec. 18, 2015), http://www.mediapost.com/publications/article/265120/search-engines-struggle-to-keep-web-traffic.html.

186 See id.

187 See id.

188 *Id.*

engines continues to decline."[189]

These developments exacerbate enforcement of the right to be forgotten. An Australian-based search platform, for example, that specializes in legal information might link Costeja to his 1998 debt, even if that 1998 debt does not appear through a similar search on Google. If websites containing European information can be accessed through a litany of evolving search capabilities operated by various and multiplying entities around the world – many without assets in Europe – the right to be forgotten offers little anonymity. One commentator identified this easy "workaround" by simply switching search engines to "DuckDuckGo, which has no EU footprint and also doesn't track cookies – and for now, you'll see the full unfiltered results."[190]

B. Web Wardens

In conjunction with diversifying search platforms, more and more entities track and re-publish information that was "erased" under the right to be forgotten. Afaq Tariq's website, "Hidden from Google," was among the first,[191] but larger players followed, including the BBC, Reddit, and the Wikimedia Foundation.[192]

Wikipedia's page entitled, "Notices received from search engines," catalogues erasure requests by country of origin, website, and file.[193] Screen shots of the erasure requests are also included, a few of which have been appended to

---

189 *Id.*

190 *See* James Ball, *EU's Right to be Forgotten: Guardian Articles have been Hidden by Google*, THE GUARDIAN (July 2, 2014), http://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google;

191 *About Us*, HIDDEN FROM GOOGLE, http://hiddenfromgoogle.afaqtariq.com/#aboutus (last visited July 25, 2016); see Charlie Osborne, "*Hidden from Google" Tracks Sites Removed from Internet Searches*, CNET NEWS (July 16, 2014), http://www.cnet.com/news/hidden-from-google-tracks-sites-removed-from-internet-searches (describing Tariq's efforts).

192 See Neel McIntosh, *List of BBC Web Pages Which have been Removed from Google's search results*, BBC INTERNET BLOG (June 25, 2015), http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379; *Notices Received from Search Engines*, WIKIPEDIA, https://wikimediafoundation.org/wiki/Notices_received_from_search_engines (last visited July 11, 2016); Subreddit, *Things That Were Not Meant to be Forgotten*, available at https://www.reddit.com/r/nevertoforget/? (described as a "forum to post articles that have been removed by Google from search results as a consequence of the righto to be forgotten); *see also* Geoff Brigham & Michelle Paulson, *Wikipedia Pages Censored in European Search Results*, WIKIMEDIA BLOG (Aug. 6, 2014), https://blog.wikimedia.org/2014/08/06/wikipedia-pages-censored-in-european-search-results.

193 See *Notices Received from Search Engines*, WIKIMEDIA FOUNDATION, https://wikimediafoundation.org/wiki/Notices_received_from_search_engines (last visited May 8, 2016).

this paper.[194] While these sites do not pinpoint the identity of the person who requested data erasure, they do highlight the webpages targeted for anonymity. Webpages involving criminal activity in Italy, murderers in Germany, and a "porn star" in France vanish from Google searches in Europe, but re-emerge on an increasing number of websites in the digital commons that are accessible through a growing number of alternative search capabilities.[195]

News media also report on websites and stories that were de-linked under European law. The Daily Mail, for instance, reported on deleted links about Josef Fritzl who criminally held his family in captivity, and "Ronald Castree, 61, a pedophile who abducted an 11-year old girl with learning difficulties before abusing and murdering her."[196] News media reported on vanishing data about Scottish football referee Dougie McDonald, who admitted to lying about reversing a penalty, Paul Baxendale-Walker being accused of fraud, and about Stan O'Neal, the former chair of Merrill Lynch.[197]

Europeans sought suppression of all these stories, which ironically boosted them further into the spotlight, creating a "Streisand effect," an attempt to hide information that spurs the unintended consequence of publicizing it more widely.[198] The Guardian, the New York Times, the Wall Street Journal, the Daily Mail and scores of others publish stories about the right to be forgotten generally and often cite to particular stories targeted for erasure.[199]

---

194 *See infra* Appendix 1.

195 *See e.g.*, *Notices Received from Search Engines*, WIKIMEDIA FOUNDATION, https://wikimediafoundation.org/wiki/Notices_received_from_search_engines (last visited May 8, 2016).

196 Katherine Rushton, *More than 280,000 people ask Google for the Right to be Forgotten and Request more than a MILLION Pages are Wiped from the Search Engine's Results*, DAILY MAIL (July 10, 2015), http://www.dailymail.co.uk/news/article-3156779/More-280-000-people-ask-Google-right-forgotten-request-MILLION-pages-wiped-search-engine-s-results.html.

197 *See* James Ball, *EU's Right to be Forgotten: Guardian Articles have been Hidden by Google*, THE GUARDIAN (July 2, 2014), http://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google; Danny Sullivan, *Thanks To "Right To Be Forgotten," Google Now Censors The Press In The EU,* MARKETING LAND (July 2, 2014), http://marketingland.com/eu-right-to-be-forgotten-censorship-89783.

198 *What is the Streisand effect?*, THE ECONOMIST (Apr. 15, 2013), http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect (The term was coined when American entertainer Barbara Streisand's attempt to suppress photographs of her Malibu home resulted in extensive publicity, videos, spoof songs and more.).

199 *See e.g.,* Greg Sterling, *Media Companies Republishing Google Right-To-Be-Forgotten Links,* SEARCH ENGINE LAND, (October 17, 2014) available at http://searchengineland.com/media-companies-republishing-google-right-forgotten-removals-206101. Of course, the right to be forgotten is not the only avenue for attempting to scrub Internet data. Copyright law, defamation law, and non-legal strategies, have been employed to bar or limit access to personal data.

C. Deep Web

The futility of implementing the right to be forgotten extends beyond diversifying search platforms and re-publication of content from deleted links. Wikipedia, BBC, Reddit, and others republish de-listed content, but these efforts take place on the surface web.[200] The surface web is the entire Internet for most users, but it represents a fraction of available content. The surface web is "that part of the Internet that is accessible by standard search engines, either by indexing, or through use of the site's IP address."

By contrast, the deep web is unfamiliar to most of the public and is larger by orders of magnitude. Characterized as the submerged part of the iceberg,[201] researchers describe the deep web's size in various and conflicting ways: over 96% of content on the world wide web,[202] unguessable,[203] 7,500 terabytes,[204] infinite,[205] and 500x the size of the surface web.[206] Although imprecise, these estimates indicate that the deep web contains much more content than the surface web.

Generally speaking, the deep web is the content not indexed by standard search engines, like Google.[207] The only U.S. court that has attempted to define

---

[200] See Neel McIntosh, *List of BBC Web Pages Which have been Removed from Google's search results*, BBC INTERNET BLOG (June 25, 2015), http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379; *Notices Received from Search Engines*, WIKIPEDIA, https://wikimediafoundation.org/wiki/Notices_received_from_search_engines (last visited July 11, 2016); Subreddit, *Things That Were Not Meant to be Forgotten*, available at https://www.reddit.com/r/nevertoforget/? (described as a "forum to post articles that have been removed by Google from search results as a consequence of the righto to be forgotten); *see also* Geoff Brigham & Michelle Paulson, *Wikipedia Pages Censored in European Search Results*, WIKIMEDIA BLOG (Aug. 6, 2014), https://blog.wikimedia.org/2014/08/06/wikipedia-pages-censored-in-european-search-results.

[201] See Sharon D. Nelson & John W. Simek, *Ashley Madison and the Deep (and Sometimes Dark) Web*, 41 MONT. LAW. 18, 26 (Nov. 2015).

[202] See *Searching the Deep Web and the Unmapped Internet*, THE WEEKLY PIQUE (Oct. 16, 2015) at http://www.weeklypique.com/2015/10/16/searching-the-deep-web/; Sharon D. Nelson & John W. Simek, *Ashley Madison and the Deep (and Sometimes Dark) Web*, 41 MONT. LAW. 18, 26 (Nov. 2015).

[203] Jose Pagliery, *The Deep Web you don't know about*, CNN MONEY, (Mar. 10, 2014) at http://money.cnn.com/2014/03/10/technology/deep-web/.

[204] See Michael K. Bergman, *White Paper: The Deep Web: Surfacing Hidden Value*, THE J. OF ELEC. PUBL'G 1 (2001), available at http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.

[205] See *Common Deep Web and Big Data Questions Answered – Part 1,* BRIGHTPLANET, (Nov. 25, 2014) at https://brightplanet.com/2014/11/common-deep-web-big-data-questions-answered-part-1/. ("The Internet has grown so vast and so large that we now classify the Deep Web as infinite.").

[206] See Peter Lyman & Hal R. Varian, *How Much Information?*, at http://groups.ischool.berkeley.edu/archive/how-much-info-2003/printable_report.pdf (last visited Aug. 2, 2016) (citing a 2000 study quantifying the deep web as "perhaps 400 to 550 times larger than the information on the 'surface'").

[207] See Michael K. Bergman, *White Paper: The Deep Web: Surfacing Hidden Value*, THE J. OF ELEC. PUBL'G 1 (2001), available at http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.

the deep web, described it as follows:

> The portion of the Web that is not theoretically indexable through the use of "spidering" technology, because other Web pages do not link to it, is called the "Deep Web." Such sites or pages can still be made publically accessible without being publically indexable by, for example, using individual or mass emailings (also known as "spam") to distribute the URL to potential readers or customers, or by using types of Web links that cannot be found by spiders but can be seen and used by readers.[208]

The deep web contains all manner of content including text, photographs, videos and music.[209] Large academic, library, and proprietary databases are stored on the deep web,[210] including core content from the U.S. Patent and Trademark Office,[211] Thomson Reuters Westlaw,[212] and NASA.[213] The distinctions between the deep web and the surface web are sometimes imprecise because content on the deep web can be "surfaced" in several ways.[214] Similarly, the deep web can be "searched" even though it is not indexed like the surface web.[215] While research in the deep web requires considerable technical facility, specialized deep web browsers, like Tor, allow visitors to browse the deep web without having to rely entirely on pre-identified URLs.[216]

The dark web has been characterized as a subset of the deep web.[217] Controversial and illicit transactions reputedly transpire on the dark web, including human trafficking, narcotic sales, and contracts for killings.[218] The dark web relies on anonymity tools to conceal both the seeker and the provider of such services.[219] It is not accessible through surface web browsers like Internet Explorer or Firefox, but is accessible via specialized and anonymized browsers

---

208 *American Library Ass'n, Inc. v. U.S.,* 201 F. Supp. 2d 401, 419 (E.D. Pa. 2002), judgment rev'd, 539 U.S. 194 (2003).

209 Jose Pagliery, *The Deep Web you don't know about*, CNN MONEY, (Mar. 10, 2014) at http://money.cnn.com/2014/03/10/technology/deep-web/.

210 See Michael K. Bergman, *The Deep Web: Surfacing Hidden Value*, 7 J ELEC PUB 1 (August 2001) (listing sixty of the largest deep web databases, including NASA, National Climatic Data Center, US Trademarks and Patents, US Census, SEC Edgar, and more).

211 See id.

212 See id.

213 See id.

214 See id.

215 See Tor: Overview, TorProject, https:// www.torproject.org/about/overview.html.en (last visited Aug. 2, 2016).

216 See Stephanie Minnock, *Should Copyright Laws Be Able to Keep Up with Online Piracy?,* 12 COLO. TECH. L.J. 523, 539 (2014).

217 See Stuart Andrews, *The Dark Side of the Web*, PC PRO (Mar. 9, 2010), http://www.pcpro.co.uk/features/356254/the-dark-side-of-the-web.

218 See id.

219 See Abdulmajeed Alhogbani, *Going Dark: Scratching the Surface of Government Surveillance,* 23 COMMLAW CONSPECTUS 469, 480—82 (2015).

such as Tor or I2P.[220] Tor facilitates browsing of dark web services without disclosing the user's IP address, which would otherwise reveal the user's network identity and location.[221] The Tor protocol leverages "pseudomains" like .onion as well as anonymous introduction points and relays between users, making de-anonymization difficult.[222]

While the dark web and deep web contain criminal elements, both are routinely used for less nefarious purposes by those seeking anonymity. The U.S. Navy uses Tor for intelligence gathering.[223] Journalists pursue controversial leads in the deep web to avoid government monitoring.[224] An array of law enforcement agencies search for illicit conduct using Tor because Tor hides government IP addresses, ensuring covert surveillance.[225] Whistleblowers reveal corporate and governmental malfeasance on the deep web to avoid retribution.[226]

But increasingly, "normal" Internet users opt for deep web browsing simply for additional privacy.[227] Tor's website states that Tor "prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location."[228] Invasive commercial browsers and search engines cannot monitor, collect, aggregate, and sell user information, like browsing history, if the user is effectively hidden while searching the web. Similarly, governmental surveillance is rendered substantially more difficult.

In such a landscape it is difficult to imagine how EU authorities could enforce the right to be forgotten. Both content providers and users are effectively anonymous.[229] Regulating browsers like Tor would be highly difficult and ultimately futile, as browsers differ materially from search engines and regulation of one international browser would only spawn regional browsers outside European reach. It is somewhat ironic that the deep web, used

---

220 See id.

221 Keith D. Watson, *Note: The Tor Network: A Global Inquiry Into the Legal Status of Anonymity Networks,* 11 WASH. U. GLOBAL STUD. L. REV. 715, 721 (2012).

222 See Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix -- Doctrine to Follow,* 14 N.C. J.L. & TECH. 489, 525-26 (2013) ("Tor is an 'onion routing' technology which hides a user's IP address, making it appear to originate from a Tor server rather than the actual address from which the user is connecting to the Internet.").

223 Tor: Overview, TorProject https:// www.torproject.org/about/overview.html.en (last visited Aug. 2, 2016).

224 See Sharon D. Nelson & John W. Simek, *Ashley Madison and the Deep (and Sometimes Dark) Web*, 41 MONT. LAW. 18, 26—27 (Nov. 2015).

225 See Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix -- Doctrine to Follow,* 14 N.C. J.L. & TECH. 489, 528 (2013).

226 Keith D. Watson, *Note: The Tor Network: A Global Inquiry Into the Legal Status of Anonymity Networks,* 11 WASH. U. GLOBAL STUD. L. REV. 715, 721, 723 (2012).

227 See Tor: Overview, TorProject https:// www.torproject.org/about/overview.html.en (last visited Aug. 2, 2016).

228 See id.

229 See id.

increasingly by those seeking privacy, undermines the privacy objective at the heart of the right to be forgotten.

D. Internet of Things

The right to be forgotten must also confront the Internet of Things, a context in which everyday objects communicate autonomously online. Technology infused objects gather, analyze, and send data through the Internet automatically, without an individual's prompting, and often without that individual's awareness.[230] Some libraries, for example, electronically tag every book in the collection,[231] while tech savvy dentists prescribe toothbrushes engrafted with tiny sensors to determine hygiene behavior.[232] A pint of beer with tilt sensors records, analyzes, and transmits consumption rates.[233] Of course, smart watches, smart phones and computer tablets absorb gigabytes of data exhaust. From steps taken in a day, to hours clocked in sleep, the technology in our pockets and on our wrists absorbs everything we allow, and even more of which we are unaware.[234] Precise locational data is captured by license plate readers, automobile GPS, and smart phones.[235]

"Smart meters," another interesting example, produce meaningful efficiencies in utility consumption.[236] Replacing monthly inspections by utility employees, smart meters capture and transmit precise utility usage in real time. While still in the nascent stages in the US,[237] over 200 million smart meters are

---

230 Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98 (2014) (explaining the functioning of the Internet of Things).

231 See Kendra Mayfield, *Tagging Books to Prevent Theft,* WIRED, (May 20, 2002) available at http://www.wired.com/2002/05/tagging-books-to-prevent-theft/.

232 See Marcia Simon, *How the Kolibree 'smart toothbrush' improves dental hygiene*, DENTISTRY IQ, (May 19, 2016) available at http://www.dentistryiq.com/articles/2016/05/how-the-kolibree-smart-toothbrush-improves-dental-hygiene.html.

233 See Kelsey Campbell-Dollaghan, *Vessyl: A Cup That Uses Molecular Sensors To Track Everything You Drink,* GIZMODO, (June 12, 2014) available at http://gizmodo.com/vessyl-a-cup-that-uses-molecular-analysis-to-track-eve-1589975359 (depicting "a cup that can calculate detailed information about what your drinking—and sync that information with your fitness tracker and peripheral apps").

234 Jeremy Andrew Ciarabellini, *Trading Privacy for Angry Birds*: *A Call for Courts to Reevaluate Privacy Expectations in Modern Smartphones,* 38 SEATTLE U. L. REV. 1491 (2015).

235 VICTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA, A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK, (Houghton Mifflin Harcourt Publishing, 2013).

236 See Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161 (2011).

237 US Energy Information Administration, *Smart Meter Deployments Continue to Rise*, 1 November 1 2012, available at eia.gov/todayinenergy/detail.cfm?id=8590. (identifying approximately thirty-six million smart meters recording and transmitting energy use in the U.S. as of 2012).

expected in the E.U. by 2020.[238] One commentator noted that such metering can "distinguish the microwave from the refrigerator, or even the light bulb in the bathroom from the light bulb in the dining room."[239] Rather than simply transmitting a resident's electricity usage for billing, smart meters now unveil when the resident showers, leaves for work, cooks, and vacations.[240] That data presents the groundwork for a multitude of observations about the resident's behaviors, attitudes and proclivities.[241] One study claimed that the electrical signal coming from a resident's home revealed with 96% accuracy the specific television show viewed by the resident.[242]

Data collection from smart meters is augmented by "smart homes," which festoon the home with sensors to track and calibrate everything from garage door usage to the patterns and frequency with which the oven is used or the refrigerator is open.[243] Software integrates this data with data from other "smart home" users to create predictive schematics.[244]

Even if the homeowner knowingly consents to such data collection through smart meters and smart homes, what about guests? It is tempting to think that a guest's entertainment preferences ascertained when visiting in a "smart home" could not be linked to that guest. It is tempting to think that data exhaust from a passenger in a "smart car" could not be linked to that particular passenger. While probably true today, such bromides will soon dissolve. "They fundamentally rely on the fallacious distinction between 'identifying' and 'non-identifying' attributes."[245]

Something as anonymous as location points – with nothing more – can be used to pinpoint an individual. Cesar A. Hidalgo and Yves-Alexandre de

---

238 Navigant Research, *Smart Meters in Europe*, available at navigantresearch.com/research/smart-meters-in-europe.

239 Stphen Wicker & R.J. Thomas, Cornell University, *A Privacy-Aware Architecture For Demand Response Systems*, Proceedings of the 44th Hawaiian Conference on System Science (HICSS-44), Kauai, Hawaii, January 2011 available at http://wisl.ece.cornell.edu/wicker/publications.html.

240 See id.; 2 NAT'L INST. OF STANDARDS & TECH., GUIDELINES FOR SMART GRID CYBERSECURITY 27 (2010), available at http:// nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (stating that, smart meter data can reveal information about people's lifestyles and appliance use).

241 See id.

242 See Miro Enev et. al., *Inferring TV Content from Electrical Noise*, 2011, available at http://miro.enev.us/papers/EMI_CCS_2011.pdf; *see also* Naked Security, Wisniewski, C., *Smart meter hacking can disclose which TV shows and movies you watch*, 8 January 2012, available online at <nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/> (accessed 20 October 2014).

243 See Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161 (2011).

244 See id.

245 Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security Myths and Fallacies of "Personally Identifiable Information",* 53 Communications of the ACM, 6, 24—26 (2010).

Montjoye, researchers at MIT, correctly identified individuals using as few as four locational data points.[246] Indeed, a handful of past location points in conjunction with a few other data points reveals a person's "future" location.[247] There are oceans of data already available, already recorded and archived. Given that a handful of locational points reveals identity, privacy regimes must abandon the futile focus on outlawing data collection, and instead prescribe data uses that are associated with discrete privacy harms.

Smart offices and smart cars are not far behind, with monitoring devices embedded in car engines, work badges, and water coolers.[248] Toll tags, license plate readers, and the wealth of information captured by event data recorders ("black boxes") transform car travel into discrete chambers for passive data collection, particularly in light of newer automobiles that increasingly trumpet Internet connectivity.[249] At the office, work badges loaded with sensors monitor employees' rapidity of speech, tone of voice, and workplace social interactions.[250] One organization seeks increased productivity by integrating software into the office infrastructure so that select employees are prompted to interact when economically expedient.[251] The software's algorithm spurs robotic movement of workplace walls, water coolers, and coffee machines to ensure that specific employees interact at discrete times.[252] While most offices have not integrated the passive data collected from employees this dramatically, the trend toward

---

246 See Larry Hardesty, *How hard is it to 'de-anonymize' cellphone data?*, MIT NEWS, (Mar. 27 2013) available at newsoffice.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data.

247 P. Tucker, *Has Big Data Made Anonymity Impossible?,* MIT TECHNOLOGY REVIEW (May 7, 2013) available at technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/.

248 See MIT Technology Review, Waber, B., *Augmenting Social Reality in the Workplace*, 15 May 2013, available online at <technologyreview.com/news/514371/augmenting-social-reality-in-the-workplace/> (accessed at 20 October 2014); Wall Street Journal, Wilson, J. H., Wearable Gadgets Transform How Companies Do Business, 20 October 2013, available online at <online.wsj.com/articles/wearable-gadgets-transform-how-companies-do-business-1382128410?tesla=y>.

249 Francesca Svarcas, *Turning a New LEAF: A Privacy Analysis of CARWINGS Electric Vehicle Data Collection and Transmission*, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 165, 167—74 (2012); Ching-Yao Chan, *Connected Vehicles in a Connected World, Int'l Symp. on VLSI Design, Automation & Test* (VLSI-DAT), Apr. 2011, at 1, 2.

250 See MIT Technology Review, Waber, B., *Augmenting Social Reality in the Workplace*, 15 May 2013, available online at <technologyreview.com/news/514371/augmenting-social-reality-in-the-workplace/> (accessed at 20 October 2014); Wall Street Journal, Wilson, J. H., Wearable Gadgets Transform How Companies Do Business, 20 October 2013, available online at <online.wsj.com/articles/wearable-gadgets-transform-how-companies-do-business-1382128410?tesla=y>.

251 See MIT Technology Review, Waber, B., *Augmenting Social Reality in the Workplace*, 15 May 2013, available online at <technologyreview.com/news/514371/augmenting-social-reality-in-the-workplace/> (accessed at 20 October 2014);

252 Id.

collection and use of passive data in workplaces continues.[253]

The Internet of Things is emerging. Over 220 billion connected devices worldwide are expected by 2020,[254] prompting Cisco to prognosticate that "pretty much everything you can imagine will wake up."[255] Combined with a world of other, easily accessible data points, the identity and entertainment preferences of the guest in the "smart home" and the identity of the passenger in the smart car are readily uncovered.[256] Just because a particular data point is "anonymous" or non-identifying at the point of collection does not mean it will remain so.[257] Non-identifying information quickly loses anonymity when combined with the vast and diverse data already available, suggesting inevitability of re-identification."[258]

Capacious privacy laws overlook the Internet of Things, passive data collection, and automated gathering of data exhaust. The E.U. Directive turns on data collection, requiring notice and consent before personal data can be lawfully collected.[259] As a result, the Directive ignores the growing reality that individuals rarely know when their personal information is collected, rendering notice and consent requirements irrelevant.[260] This digital landscape portends the futility of omnibus privacy laws, a notion tacitly acknowledged in a report from the 2014 World Economic Forum: "The growth of data, the sophistication of ubiquitous computing and the borderless flow of data are all outstripping the ability to effectively govern on a global basis."[261]

V. Regulating for Privacy, Risk of Harm

Responding to loss of privacy in the Internet age with unilateral, extra-jurisdictional laws that mandate deletion of personal information if that information is deemed "irrelevant," fails to meaningfully advance the original goal

---

253 Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1001-1017 (2011).

254 Tim Bajarin, *The Next Big Thing for Tech: The Internet of Everything*, TIME, (Jan. 13 2014) available at time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/.

255 CISCO, *What is the Internet of Everything?*, available at cisco.com/web/tomorrow-starts-here/ioe/index.html.

256 See Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1716—7125 (2010).

257 See id.

258 Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of "Personally Identifiable Information,"* 53 COMM. ACM 24, 24–26 (2010).

259 Data Directive, *supra* note 51; Data Regulation, *supra* note 62.

260 Id.

261 A.T. Kearney, *Rethinking Personal Data: A New Lens for Strengthening Trust*, World Economic Forum, (May 2014) available at http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf.

of increased privacy. To a large degree, the personal data individuals seek to protect has already been published. Recapturing and quarantining or erasing that data is implausible for the reasons detailed above. Further, the means available for gathering more such information are increasingly automated and integrated into daily life.[262] As a result, new privacy regulation cannot simply supplement old privacy regulation, especially when the analogue predated the Internet. Rather, effective privacy regulation must adapt to the current landscape by tailoring the law to risk of harm. Surreptitious monitoring of others' browser history that is then shared with marketers or aggregated for profiling purposes, for example, constitutes a discrete use of personal information that policymakers could choose to regulate. "Regulating the *use* of private data as it relates to particular risks or harms better comports with consumer law generally and permits the needed adaptability to reflect context and evolving technology."[263]

Data generated by online transactions, as well as data generated "passively," simply by living within the Internet of Things, cannot be outfitted with innumerable notice and consent forms. Technology has nullified those legal tools. Data collection, both active and passive, increases by orders of magnitude in conjunction with integrated systems capable of transferring and analyzing that data.[264] Rather than an over-broad E.U. law that captures oceans of harmless data processing and that incentivizes uneven enforcement at the expense of international comity,[265] privacy law should directly address harm to the user in conjunction with user expectation.

Users expect online purchases, geolocation logs, health and activity data from wearable devices, Internet banking transactions, and email addresses required for specific business deals to remain with the relevant parties for the original and intended uses.[266] Regulatory schemes, like the Directive, that hinge on the "processing" of this data, or even the collection of it, dilute the privacy goal by capturing the deluge of data that falls within the regulation's ambit.[267] It is not the fact of this data's processing that merits legal protection, but its inappropriate

---

262 See *infra*, Part IV (D).

263 McKay Cunningham, *Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm*, 2 GRON. J. INT'L LAW 2, 142 (2014) (citing Alessandro Spina, *Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?,* 5 EURO. JNL OF RISK REG., 2, 248–252 (2014)).

264 Tim Bajarin, *The Next Big Thing for Tech: The Internet of Everything*, TIME, (Jan. 13 2014) available at time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/.

265 *See infra*, Part IV.

266 *See* Daniel J. Solove, UNDERSTANDING PRIVACY 102–69 (President and Fellows of Harvard College 2008); Joshua J. McIntyre, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV. 895 (2011).

267 See Paul M. Schwartz, *The E.U.-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1984—87 (2013).

use.[268] Secretive monitoring, undisclosed transfer to unidentified parties, and monetization of personal data through marketing and profiling more readily approximate privacy harms and justify regulatory safeguards.[269] Determining the risk of harm based on discrete and unwarranted uses of personal data narrows the legislative scope, allowing incremental and targeted reform.

Effective privacy regulation must reject the E.U.'s capacious definitions of "personal information" and "processing," in favor of a taxonomy that better approximates the Internet's architecture and the malleable manner in which digital data originates, transforms, and eventually recedes.[270] Privacy regulations more closely parallel this reality by distinguishing passively created data from actively created data, by delineating "external" data from "internal" data, and by identifying original data from downstream transformation or modification of that data.[271] Passive data, like records of where a user's mouse hovers when visiting a website or data exhaust captured by the Internet of Things, merits a different legal paradigm than "active" data that was deliberately and originally created, like a photograph of the user taken by the user and posted by the user.[272] Privacy protections differ depending on such distinctions.[273] A person seeking to take down a picture of herself that she posted on a social networking site deserves separate legal treatment from a politician seeking to take down text from an unflattering blog posted by a third party.[274]

Indeed, the legal infrastructure for many of these permutations is already in place. In the U.S. and the E.U., defamation law protects against untrue harmful publications, reflecting the ethos behind the right to be forgotten.[275] Copyright law also advances objectives that are similar to the right to be forgotten.[276] When hackers illegally obtained and published revealing photographs of U.S. celebrities, lawyers for the celebrities leveraged copyright law to force websites and search engines to "erase" the pilfered images.[277] "[T]he Children's Online Privacy Protection Act provides for a right to delete personal

---

268 DANIEL SOLOVE, UNDERSTANDING PRIVACY 10—11, 171—74 (2008).

269 Id.

270 Daniel J. Solove, *A Taxonomy of Privacy*, 154 PENN. L. REV. 477, 478 (2006).

271 Meg L. Ambrose, *A Digital Dark Age and the Right to Be Forgotten*, 17 J. INTERNET L. 1, 11 (2013).

272 *See id*.

273 Daniel J. Solove, *A Taxonomy of Privacy*, 154 PENN. L. REV. 477 (2006).

274 Meg L. Ambrose, *A Digital Dark Age and the Right to Be Forgotten*, 17 J. INTERNET L. 1, 11 (2013).

275 *See* New York Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964); Gertz v. Robert Welch, Inc., 418 U.S. 323, 342—43 (1974).

276 Copyright Act, 17 U.S.C. § 107 (2006); Universal City Studios, Inc. v. Corley, 273 F.3d 429, 458-61 (2d Cir. 2001).

277 *See* Eriq Gardner, *Google Responds to Jennifer Lawrence Attorney's $100 Million Lawsuit Threat*, HOLLYWOOD REPORTER (Oct. 2, 2014), http://www.hollywoodreporter.com/thr-esq/google-responds-jennifer-lawrence-attorneys-737656

data. The Fair Credit Reporting Act restricts the ability of consumer reporting agencies to report on bankruptcies and criminal proceedings that are beyond a certain number of years old."[278] These legal doctrines carry the added benefit of refinement through decades of case law, legislation, and other democratic processes.[279]

Bankruptcy protections,[280] privacy controls integrated into criminal law,[281] like grand jury proceedings,[282] and laws allowing sealed and expunged court records for juveniles[283] all protect privacy rights in distinct contexts more closely associated with the potential harm that would result absent such protections.[284] One commentator suggests that specifically tailored privacy laws like these illustrate continuity with E.U. privacy objectives rather than disharmony: "Recent academic and political initiatives on privacy in the United States emphasize subject control and contextual analysis, reflecting popular thinking that is not so different after all from that which animates Europe's 1995 directive and 2012 proposed regulation."[285]

In contrast to these specific measures, the right to be forgotten requires that data controllers delete links to "irrelevant" content.[286] Data controllers, like Google, decide whether the requested content is irrelevant or inadequate, not a court, agency, or other public body.[287] "It is for the company—and not the individual—to prove that the data cannot be deleted because it is still needed or is still relevant."[288] Paralyzing fines for refusing valid erasure requests[289]

---

278 Daniel Solove, What Google Must Forget: The EU Ruling on the Right to Be Forgotten (May 13, 2014), https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten [perma.cc/9XGZ-9YK3]

279 *See id*.

280 *Process - Bankruptcy Basics*, UNITED STATES COURTS, http://www.uscourts.gov/services-forms/bankruptcy/bankruptcy-basics/process-bankruptcy-basics (last visited May 8, 2016).

281 *See* FED. R. CRIM. P. 32(c)(3). Upon conviction, the federal code and most state criminal procedure codes provide for a pre-sentence investigation and report, usually researched and written by a probation officer to guide the judge's sentencing ruling. The pre-sentencing reports often contain hearsay, opinion, and speculation. As a result, most criminal procedure codes call for confidentiality of pre-sentence reports. *See* Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 WASH. L. REV. 307, 309–311 (2004).

282 *See e.g.*, FED. R. CRIM. P. 6(d).

283 See Anna Kessler, *Excavating Expungement Law: A Comprehensive Approach*, 87 TEMP. L. REV. 403, 417–18 (2015).

284 Richard J. Peltz-Steele, *The New American Privacy*, 44 GEO. J. INT'L L. 365 (2013).

285 Id.

286 *Factsheet on the "Right to be Forgotten" Ruling* (2014), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

287 Id.

288 Id.

289 The current data Directive allows fines up to two percent worldwide turnover, which will increase to the greater of €100 million or five percent of annual worldwide turnover under the new Regulation. See Data Regulation supra note 62; see Emily Shoor, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the*

incentivize Google to err on the side of deleting content, which perhaps explains why Google has so far approved 43% of those requests, de-listing approximately 657,000 URLs as of the date of this publication.[290] Privacy is poorly served through a rubric of economic intimidation and the catch-all standard of "irrelevance."[291] Negative secondary effects swallow what little, if any, privacy objectives the law seeks to effectuate.

Moreover, data's shelf life on the web is far shorter than conventionally believed. "Like other resources, information is perishable, depreciating in value over time. Depreciation will occur at different rates for different pieces of information, which correlates to the content's relevance and accuracy."[292] Claims that digital data are "impossible to forget" or that once posted, data forever remains readily accessible,[293] are wrong.[294] An entire subculture of archivists strain to offset the Internet's digital decay and educate the public to the fact that the Internet continuously sheds tremendous amounts of information.[295] Using URLs as a metric, one study tracked tweets about significant events including the H1N1 virus and the Syrian revolution.[296] Approximately 11% of the content associated with those tweets disappeared within one year, increasing to 27% after two years.[297] A litany of diverse causes contributes to digital decay.[298] Importantly, personal bias is not among them.[299] If digital information must disappear, it should be culled through objective, automated processes, rather than by those with the most bias towards it.[300]

Proposed Data Protection Regulation, 39 BROOK. J. INT'L L. 487, 488 (2014).

290 *Transparency Report: European Privacy Requests for Search Removals*, GOOGLE, http://www.google.com/transparencyreport/removals/europeprivacy/ [https://perma.cc/44BG-9DNM] (last updated August 15, 2016).

291 Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH. 349, 352–53 (2015).

292 Id.

293 Meg L. Ambrose, *A Digital Dark Age and the Right to Be Forgotten*, 17 J. INTERNET L. 1, 13 (2013).

294 Id.

295 Id.

296 Id.

297 Id.

298 Id.

299 Id.

300 The Stanford research paper written by Google founders Sergey Brin and Larry Page describes the web as "a vast collection of completely uncontrolled heterogeneous documents," and suggest that search engines provide decontextualized content through black box algorithms. See Sergey Brin & Lawrence Page, *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, available at http://infolab.stanford.edu/~ backrub/google.html.

VI. Conclusion

Near-universal access to information through the Internet arrived without lead-time to develop policy to guide its use. Within two decades, the Internet connected people across the globe to great oceans of data on an infrastructure itself unbounded by national borders. The Internet's international and fluid architecture increased its resilience to discrete regulation of the information accessible thereon, creating a built-in barrier to state sponsored censorship. This advantage was largely unhindered by search engines and algorithms biased, if at all, by their primary objective – usefulness.

But the inability to censor information on the Internet carries a high price in privacy. Personal data, vital to social interaction, are readily extracted, monitored, copied, transferred, and leveraged without the individual's concomitant control. Identity theft, cyber stereotyping, public embarrassment, and degraded confidentiality are among the many harms incident to the erosion of privacy through digital connectivity. The question arises, how to maintain the benefit of uncensored data while simultaneously reducing privacy harms?

The European Union, through legal recognition of the right to be forgotten, attempted to address that question. The E.U. law facilitates individualized control over personal information on the Internet by requiring that data controllers, like Google, delist links to irrelevant personal information. The lawyer with an extinguished twenty-year-old debt successfully demanded that Google delist a newspaper article that connected him to the debt. Others followed. More than 400,000 URLs have been delisted as individuals seek to erase access to their personal information, often indiscretions, from public view.

While laudable in the abstract, it its application, the new law not only generates negative secondary effects, it largely fails to achieve meaningful privacy for those who "exercise" the right to be forgotten. The law emerged by accretion. It was built on the scaffolding of previous privacy laws – laws that long predated the Internet. If we are, in fact, "still in the first minutes of the first day of the Internet revolution,"[301] lawmakers seeking to regulate Internet use must consider its architecture. Instead, European lawmakers mostly ignored the ephemeral and borderless nature of data creation, modification, transmission and storage on the Internet. The only provisions acknowledging the transnational nature of Internet data flow are catchall extra-jurisdictional provisions that purport to govern any entity anywhere that "processes" or "controls" personal information.

Application of E.U. law to anyone who processes personal information theoretically addresses the problem of transnational data flow, but it also creates

---

[301] *See* Stephen Levingston, *Internet Entrepreneurs Are Upbeat Despite Market's Rough Ride*, NEW YORK TIMES (May 24, 2000), http://www.nytimes.com/2000/05/24/business/worldbusiness/24iht-hype.2.t.html (quoting Scott Cook, then chairman of Intuit, Inc.).

a raft of negative secondary effects. Instead of targeting the harms that result from loss of privacy, the law captures almost every entity doing business on the Internet, most of which are innocuous. Because of its near-universal application, the law invites arbitrary enforcement. European officials can target disfavored organizations for investigation and prosecution. The law also disregards the sovereignty and democratic principles of other nations, whose citizens must comply with European law without having a participatory voice in the creation of the law.

Even individuals who successfully petition for deletion of their personal information achieve little under the right to be forgotten. Many experience a "Streisand effect;" their attempt to conceal information only amplifies it. The resilience of the Internet also undermines the right to be forgotten. Dedicated websites monitor each delisted URL. News agencies repost delisted links and the deep web remains largely unreachable by the E.U. law. The Internet of Things continues to advance, exacerbating enforcement of the law, as more and more personal information is unknowingly collected by ordinary objects and transmitted over the Internet.

Several nations outside the E.U. have created similar privacy laws, but the European Union's example in this regard should not be emulated. Policing privacy on the Internet through omnibus legislation that accounts for transnational data flow by requiring everyone's compliance while simultaneously overlooking the resilience of the Internet, foments more harm than facilitates good. Protecting privacy in the information age requires policies tailored to privacy harms. Until policymakers require a closer nexus between user privacy and potential harm attending its violation, efforts to regulate the Internet generally will yield outsized and unwanted secondary effects while only minimally achieving meaningful privacy protections.