Buffalo Law Review

Volume 65 | Number 3 Article 2

5-1-2017

Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten

McKay Cunningham
Concordia University School of Law

Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten

MCKAY CUNNINGHAM†

INTRODUCTION: THE 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 thirty-six word notice 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 thirty-six 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 thirty-six word notice and all reference to it.[6] Because the case turned on law

---

† Associate Professor, Concordia University School of Law

1. *See* Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos* (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [hereinafter Case C-131/12, *Google Spain SL*]; EUROPEAN COMM'N, FACTSHEET ON THE "RIGHT TO BE FORGOTTEN" RULING (C-131/12) (2014), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf; Daniel Lyons, *Assessing the Right to Be Forgotten*, 59 BOS. B.J. 26, 26 (2015).

2. EUROPEAN COMM'N, *supra* note 1; Lyons, *supra* note 1.

3. Lyons, *supra* note 1.

4. Case C-131/12, *Google Spain SL* ¶¶ 18–20.

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

6. Case C-131/12, *Google Spain SL*; *see also* Dave Lee, *What Is the "Right To*

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 CJEU 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 CJEU offered little guidance in determining when personal information is subject to mandatory erasure due to irrelevance or inadequacy.[11]

The CJEU did not identify or characterize how the new right to delete information comports with countervailing

---

Be Forgotten"?, BBC (May 13, 2014), http://www.bbc.com/news/technology-27394751.

7. Case C-131/12, *Google Spain SL* ¶¶ 5–10; *see also* EUROPEAN COMM'N, *supra* note 1.

8. EUROPEAN COMM'N, *supra* note 1.

9. *See* Meg Leta Ambrose, *A Digital Dark Age and the Right to Be Forgotten*, J. INTERNET L., Sept. 2013, at 1, 9–11; 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); 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); 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.

10. Case C-131/12, *Google Spain SL*, ¶ 94; *see also* EUROPEAN COMM'N, *supra* note 1.

11. *See* Case C-131/12, *Google Spain SL*, ¶ 94.

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 March 2017, Europeans had submitted over 715,000 requests to deactivate two million URLs.[17] Google has deleted over forty-three percent of those, approximately 732,000 links.[18] Early reports suggested that a large percentage of deleted content involved

---

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

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

14. Caitlin Dewey, *Want to Remove Your Personal Search Results from Google? Here's How the Request Form Works*, WASH. 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. 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.

16. *Id.*

17. *Transparency Report: European Privacy Requests for Search Removals*, GOOGLE (Mar. 31, 2017), http://www.google.com/transparencyreport/removals/europeprivacy/.

18. *Id.*

accusations of fraud, child pornography, and other serious crimes.[19] 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."[20] After Google inadvertently revealed information about those requesting data deletion, it appeared that ninety-five percent of the erasure requests derive from "ordinary members of the public."[21] Regardless, it remains difficult to know who is requesting content deletion and why.[22]

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.[23] One law professor claims "[a]n overly expansive right to be forgotten will lead to censorship of the Internet because data

---

19. 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; Preece et al., *supra* note 15.

20. David Mitchell, *The Right To Be Forgotten Will Turn the Internet into a Work of Fiction*, GUARDIAN (July 5, 2014), http:// www.theguardian.com/commentisfree/2014/jul/06/right-to-be-forgotten-internet-work-of-fiction-david-mitchell-eu-google.

21. Sylvia Tippmann & Julia Powles, *Google Accidentally Reveals Data on 'Right to be Forgotten' Requests*, 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.").

22. *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).

23. 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 part of the 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.").

subjects can force search engines or websites to erase personal data, which may rewrite history."[24] If content becomes less searchable, others assert it will "derogate[ ] the role of counterspeech."[25]

Wikipedia's founder portrayed the right to be forgotten as "completely insane," maintaining that

> [i]n 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 use the law to prevent Google from publishing truthful information.[26]

Admittedly, the author of this Article agreed, writing that "European filtering of Internet content worldwide through the right to be forgotten . . . effectuates international censorship in the guise of privacy. . . ."[27]

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 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."[28] Today, a Google search under Costeja's name generates thousands of articles,

---

24. *Id.* at 372.

25. 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).

26. Preece, *supra* note 15 (internal quotations omitted).

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

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

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.[29] 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.[30]

An assortment of unaffiliated entities purposely undermine efforts to delete links under the right to be forgotten.[31] 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.[32] 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.[33] 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,[34] and others like

29. *See* Antani, *supra* note 22, at 1174–77.

30. See *infra* Part V.

31. See *infra* Section III.B.

32. HIDDEN FROM GOOGLE (Sept. 19, 2016), https://web.archive.org/web/20160919031318/http://hiddenfromgoogle.afaqtariq.com/?.

33. Jeff Roberts, *"Hidden from Google" Shows Sites Censored Under EU's Right-to-be-Forgotten Law*, GIGAOM (July 16, 2014, 6:41 AM), https://gigaom.com/2014/07/16/hidden-from-google-shows-sites-censored-under-eus-right-to-be-forgotten-law/.

34. Neel McIntosh, *List of BBC Web Pages Which have been Removed from Google's Search Results*, BBC INTERNET BLOG (June 25, 2015, 2:40 PM), http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379.

Wikimedia and Reddit maintain logs that track the content from each link that Google truncates.[35]

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.[36] The best-case scenario for proponents of the right to be forgotten, is that "deleted" content becomes more difficult to find.[37] 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.[38] 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.[39] This is already taking place; Google's market share fell from 81.56

---

35. *Notices Received from Search Engines*, WIKIMEDIA FOUND., https://wikimediafoundation.org/wiki/Notices_received_from_search_engines (last visited Mar. 31, 2017); *Things That Were Not Meant to Be Forgotten*, REDDIT, https://www.reddit.com/r/nevertoforget/ (last visited Mar. 31, 2017) (The forum is described as a "[f]orum to post articles that have been removed by Google from search results as a consequence of the right to be forgotten" when searched on Reddit.); *see also* Geoff Brigham & Michelle Paulson, *Wikipedia Pages Censored in European Search Results*, WIKIMEDIA FOUND. (Aug. 6, 2014), https://blog.wikimedia.org/2014/08/06/wikipedia-pages-censored-in-european-search-results.

36. *See* sources cited *supra* note 35.

37. See Roberts, *supra* note 33 ("The issue is more complicated still because the law applies only to national versions of Google—meaning that the story . . . disappeared from sites like Google.co.uk but not Google.com or Google.ca.").

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

39. *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.

percent in 2012 to 71.4 percent in 2016[40] with some prognosticating that Google's market share "is now likely in permanent decline."[41]

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 the search engine juggernaut—a perhaps unsurprising secondary effect, given the European Commission's ongoing efforts to diminish Google's dominance in Europe.[42] The EU's failure to effectuate privacy goals through the right to be forgotten is emblematic of EU privacy regulation generally.[43] The borderless flow of information over the Internet eludes traditional territorial-based jurisdiction and enforcement.[44] 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.

---

40. *Desktop Search Engine Market Share*, NETMARKETSHARE, https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0&qptimeframe=Y (last visited Apr. 1, 2017).

41. 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/.

42. *See* Spencer Weber Waller, *Antitrust and Social Networking*, 90 N.C. L. REV. 1771, 1793–94 (2012).

43. *See* 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); 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).

44. *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).

I. 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.[45] 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.[46] Data origins evolve as digital data packets are augmented, duplicated, or otherwise altered.[47] 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.[48]

Despite the nuances of transnational information flow, laws that seek to regulate such information derive from exemplars that existed long before the Internet.[49] The EU's seminal privacy law, the Data Directive, was enacted twenty years ago—well before Internet commercialization.[50] Such

---

45. *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) ("The market for data protection is characterized by widely dispersed individuals, with low stakes, entering into ad hoc transactions with large enterprises.").

46. *See* Curt Franklin, *How Internet Search Engines Work*, HOWSTUFFWORKS TECH, http://computer.howstuffworks.com/internet/basics/search-engine.htm (last visited Apr. 1, 2017).

47. *See id.*

48. 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?*, INFO. SEC. BUZZ (Apr. 15, 2016), http://www.informationsecuritybuzz.com/articles/know-proxy-servers/ (explaining that proxy servers allow internet users to take a "side door" into a website to hide the user's identity).

49. *See* LISA J. SOTTO, PRIVACY AND DATA SECURITY LAW DESKBOOK § 1.04 (2011).

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

"[e]arly privacy law could not have imagined, much less accounted for, the ubiquity and complexity of Internet communication. . . ."[51] 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.[52] Nazis discovered and leveraged personal information—often religious, racial, and cultural—to destabilize occupied territory and identify those for deportation to concentration camps.[53] A series of treaties, charters, and accords stem from this historic catalyst, ultimately leading to the right to be forgotten.[54]

The United Nations adopted the Declaration of Human Rights soon after World War II, a portion of which promised that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."[55] 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

---

51. McKay Cunningham, *Free Expression, Privacy, and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship*, 69 ARK. L. REV. 71, 72 (2016); *see also* 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).

52. *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1143–44, 1170 (2000).

53. *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*, 1 GOV'T INFO. Q. 431 (1984) (A report on a 1984 conference on data protection in which "[o]ne 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.").

54. *See* Rustad & Kulevska, *supra* note 23, at 356–60.

55. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

information.[56] 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.[57] The level of generality in Article 16 of the Consolidated Treaty on the Functioning of the European Union is noteworthy: "[e]veryone has the right to the protection of personal data concerning them."[58]

This framework remains at the heart of modern regulatory efforts. Europe's Data Directive (hereinafter "Directive"), largely characterized as the most influential and progressive data privacy law worldwide,[59] 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.[60]

A new European privacy law will soon replace the Directive.[61] The forthcoming General Data Protection

---

56. Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364/01).

57. 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.

58. Consolidated Version of the Treaty on the Functioning of the European Union art. 16, Oct. 26, 2012, 2012 O.J. (C 326) 55.

59. *See* Christopher Kuner, *The European Union and the Search for an International Data Protection Framework*, 2 GRONINGEN J. INT'L L. 55, 55 (2014) ("focusing . . . on E.U. law as the most influential body of data protection law worldwide"); Shaffer, *supra* note 45, at 55–88.

60. Data Directive, *supra* note 50, art. 6.

61. *See* Commission 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 (hereinafter "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.[62] 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.[63] The Regulation, effective in 2017, legislatively confirms the CJEU ruling by expressly codifying the right to be forgotten.[64]

B. *The Right to Be Forgotten*

With the Regulation, EU residents may "have their data fully removed when it is no longer needed for the purposes for which it was collected."[65] Removable data includes text, video, photographs, and other forms of information published in various contexts including links accessed by search engines and websites themselves.[66] 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.[67] 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

---

Regulation].

62. *See* Treaty on European Union (Maastricht Treaty) art. 288, Feb. 7, 1992, 1992 O.J. (C 191) 1.

63. *See id.*; Data Regulation, *supra* note 61.

64. *See* Data Regulation, *supra* note 61; European Commission Press Release, MEMO/14/186, Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote (Mar. 12, 2014).

65. *See* European Commission Press Release MEMO/10/542, Data Protection Reform—Frequently Asked Questions (Nov. 4, 2010) ("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 id*.

67. *See infra*, Section III.B.

the abstention from further dissemination of such 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 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.[68] Under the Directive, organizations and individuals who process personal data must provide notice before collecting it[69] and obtain consent that is a "freely given, specific and informed indication of [the resident's] wishes."[70] 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

68. *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).

69. *See* Data Directive, *supra* note 50, art. 7; Data Regulation, *supra* note 61, art. 6.

70. Data Regulation, *supra* note 61, art. 2(h).

incompatible with those purposes."[71] In many cases, an EU resident maintains authority to access and correct the personal data processed by an organization or individual.[72] Most recently, EU residents have gained the power to have it deleted altogether through the right to be forgotten.[73] 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.[74] To forestall an exodus of information-reliant businesses, European policymakers engrafted extra-jurisdictional provisions in both the Directive and the Regulation.[75] 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."[76]

---

71. *Id.* art. 6(1)(b).

72. *Id.* art. 6. Those who control private data must also protect it. *Id.* 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." *Id.* art. 17.

73. Case C-131/12, *Google Spain SL*; *see also* EUROPEAN COMM'N, *supra* note 1.

74. *See Transferring Your Personal Data Outside the EU*, EUROPEAN COMMISSION (Dec. 3, 2015), http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm.

75. *Id*; *see* Kuner, *supra* note 59, at 60–71.

76. *Transferring Your Personal Data Outside the EU*, *supra* note 74.

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" the "personal information" of EU residents.[77] The laws define these terms so broadly it is difficult to know who does not have to comply.[78] 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 more factors specific to his physical, physiological, mental, economic, cultural, or social identity."[79]

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.[80] Information is "personal," according to European officials, even though "the person has not been identified yet, it is possible to do it."[81] 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

77. *See* Data Directive, *supra* note 40, art. 2 ("[P]rocessing . . . shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.").

78. *See* Liat Clark, *ICO Commissioner Slams EU Data Protection Directive*, WIRED (Feb. 7, 2013), https://web.archive.org/web/20160507055713/http://www.wired.co.uk/news/archive/2013-02/07/ico-against-eu-data-protection.

79. Data Directive, *supra* note 50, art. 2(a).

80. *See* Art. 29 Working Party Opinion 1/2008 on Data Protection Issues Related to Search Engines, 00737/EN/WP148, Apr. 4, 2008, at 3, 8; 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, 1819–20 (2011).

81. *See* Art. 29 Working Party Opinion 4/2007 on Concept of Personal Data, 01248/07/EN/WP136, June 20, 2007.

fact that the information is related to an individual capable of being identified results in the data being 'personal data' under the Directive."[82]

The new Regulation builds on the capacious scope of "personal data" by defining it as "any information relating to a data subject."[83] 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.[84] Professors Paul Schwartz and Daniel Solove note that Europe's data privacy law arguably applies to anyone engaging in any commerce within the EU or with residents therefrom.[85]

As noted above, these broad definitions are not circumscribed to those within the territorial boundaries of the EU. The Directive and Regulation amplify broad definitions with extra-territorial provisions. First, both laws prohibit transfer of personal data outside the EU unless the law's requirements are met.[86] Only nations with "adequate" data privacy laws may receive data transfers from within the EU.[87] European officials, however, have identified only eleven nations as adequate.[88] To avoid truncating Europe's

---

82. McKay Cunningham, *Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law*, 44 GEO. WASH. INT'L L. REV. 643, 657 (2012).

83. Data Regulation, *supra* note 61, art. 4.

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

85. *See* Schwartz & Solove, *supra* note 80, at 1817, 1874–76.

86. Data Directive, *supra* note 50, art. 25; Data Regulation, *supra* note 61, 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 organisation in question ensures an adequate level of protection.").

87. Data Directive, *supra* note 50, art. 25(1).

88. *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (last visited Apr. 14, 2017) (listing Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Israel, Isle

international commerce by allowing data transfers to only eleven nations,[89] the Directive offers other avenues for transfer to those countries that are inadequate.[90] Strict contractual agreements and "Binding Corporate Rules," import the Directive's strictures to individual organizations.[91] The Directive allows very little margin for parties to alter or manipulate the model contracts or binding corporate rules.[92]

Another extra-territorial provision ties the Directive's applicability to "equipment" within the EU. 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.[93]

> 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.[94]

Any transaction involving an EU resident likely falls within this provision if the transaction occurs online. It

---

of Man, Jersey, New Zealand, Switzerland, and Uruguay as providing adequate protection). While the United States appears among the nations with adequate protections, it is included due to the EU-US Privacy Shield and not its adequate protections. *See id.*

89. *See* Shaffer, *supra* note 45, at 39.

90. The principal avenues for U.S. companies seeking to comply with the EU Directive and thereby receive personal information from the EU include obtaining actual consent of the data subject, standard contractual clauses, binding corporate rules, and until recently, participation in the Privacy Shield program. *See* Data Directive, *supra* note 50, art. 26.

91. *See* Data Directive, *supra* note 50, art. 26(2); Art. 29 Working Party Working Document on Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 11639/02/EN/WP74, June 3, 2003, at 5, 6.

92. *See* Data Directive, *supra* note 50, art. 26.

93. *Id.* art. 4.

94. *Id.*

captures all e-commerce with Europeans, presuming that EU residents use a laptop, smart phone, or other such device to facilitate the interaction.[95]

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 EU.[96] 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."[97]

It appears that European policymakers sought to protect the personal data of EU residents regardless of where it is processed.[98] "[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."[99] Accordingly, both the Directive and Regulation diverge from normative jurisdictional law.[100]

---

95. *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).

96. Data Regulation, *supra* note 61, art. 3.

97. DAN JERKER B. SVANTESSON, EXTRATERRITORIALITY IN DATA PRIVACY LAW 107 (2013).

98. *See* Kuner, *supra* note 59, at 57.

99. Soma et al., *supra* note 95, at 205.

100. Data Directive, *supra* note 50, art. 4 (stating 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); *See* Yahoo! Inc. v. La Ligue Contre Le Racisme et l'Antisemitisme, 433 F.3d 1199, 1205–11 (9th Cir. 2006); Shaffer, *supra* note 45, at 39 ("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.").

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.[101] It restricts a host of innocent companies and individuals, whose information use does not harm Europeans' privacy.[102] It invites uneven enforcement by data privacy officials who can indiscriminately select disfavored entities for prosecution.[103] Finally, it disregards the sovereignty of other nations by imposing European privacy law extra-jurisdictionally.[104]

II. EU 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,[105] 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.[106] The scope of innocents caught by the law broadens when considering the law's application to data that

101. *See supra* Part II.

102. *See supra* Section II.A.

103. *See supra* Section II.B.

104. *See supra* Section II.C.

105. *See supra* Section II.C.

106. *See* Cate, *supra* note 84, at 183.

could feasibly *enable* the holder to connect it to a specific person, even if the holder herself cannot make the connection.[107] Through such a capacious scope, the law captures an ocean of "innocent" activities—data processing that threatens no privacy harm to European citizens.[108]

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 person can be de-coded and matched once again with the proper individual.[109] "The emergence of powerful re-identification algorithms demonstrates . . . the fundamental inadequacy of the entire privacy protection paradigm based on 'de-identifying' the data."[110] De-anonymizing algorithms can leverage as few as three data points to connect "anonymous" data to an individual.[111] Given the ubiquity of data points already available, "any attribute can be identifying in combination with others."[112]

---

107. *See id*.

108. 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 EU 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 generally* Schwartz & Solove, *supra* note 80.

109. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706–18 (2010).

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

111. *See id*. at 26.

112. *Id.* at 26 (emphasis omitted).

In fact, "the more data [available], the less any of it can be said to be private. . . ."[113] 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.[114] Applied literally, officials could seize almost any laptop or smartphone at the European border in light of the Directive's near-universal application.[115] 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 United States.[116] They give enforcement officers carte blanche authority to prosecute disfavored citizens, prompting corruption over compliance.[117]

---

113. Patrick Tucker, *Has Big Data Made Anonymity Impossible?*, MIT TECH. REV. (May 7, 2013), https://www.technologyreview.com/s/514351/has-big-data-made-anonymity-impossible/.

114. *See generally* Cate, *supra* note 84.

115. *See generally id.*

116. *See, e.g.*, Chicago v. Morales, 527 U.S. 41, 50–52 (1999) (holding a law cannot be so vague that a person of ordinary intelligence cannot figure out what is innocent activity and what is illegal); People v. Golb, 15 N.E.3d 805 (N.Y. 2014) (striking down harassment statute where language was overbroad); People v. Dietze, 549 N.E.2d 1166 (N.Y. 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); John Leland, *Top Court Champions Freedom to Annoy*, N.Y. TIMES (May 13, 2014), nytimes.com/2014/05/14/nyregion/top-court-champions-freedom-to-annoy.html?_r=0 (discussing People v. Golb).

117. *See Morales*, 527 U.S. at 50–52. *But see* John C. O'Quinn, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, 12 HARV. J.L. & TECH. 683, 691 (2000) (book review) ("the more cooperative approach to enforcement generally taken toward regulatory regimes in Europe, . . . and . . . the role of discretionary approach to enforcement that is

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."[118] As a result, some commentators questioned whether the Directive was itself a bluff.[119] "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."[120] Literal enforcement would effectively truncate the European market from the international economy.[121]

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.[122] 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.[123] There is an abundance of other enforcement actions under the Data Directive, mostly

---

taken . . . in Europe").

118. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 155 (1998).

119. *See id.*

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

121. *Id.*

122. Johanna Laas, *Germany: DPA Imposes Fine on Insurance Company*, PRIVACY EUROPE (Jan. 7, 2015, 12:05 PM), https://www.privacy-europe.com/blog/germany-dpa-imposes-fine-insurance-company/.

123. Geert De Clercq, *France Fines Google Over Data Privacy*, REUTERS (Jan. 8, 2014, 3:32 PM), http://www.reuters.com/article/us-france-google-fine-idUSBREA0719U20140108.

prosecuting a selection of large businesses.[124] These prosecutions suggest uneven application of the law because they target specific entities among a ubiquity of violations.[125]

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.[126] As a result, each Member State drafted discrete privacy laws and each Member State retains discretion regarding implementation and enforcement.[127] 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-compliance: the greater of €10,000,000 or 2 percent of annual worldwide turnover or the greater of €20,000,000 or 4 percent of annual worldwide turnover depending on the violation.[128] 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.[129]

---

124. *See* SOTTO, *supra* note 49, at § 18.02(A)(4)(b)(9) (listing notable enforcement examples).

125. *See id.*

126. *See* Treaty on European Union, *supra* note 62; Data Directive, *supra* note 50, art. 28.

127. *Data Directive*, *supra* note 50, art. 28.

128. Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) art. 83, 2016 O.J. (L 119) 1.

129. *Data Transfers Outside the EU*, EUROPEAN COMM'N (Nov. 24, 2016),

They also purport to capture transnational data flow by restricting entities that have no physical presence in Europe.[130] 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.[131] 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.[132]

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.[133] A request for data erasure from a Frenchman, for example, would only affect google.fr rather than searches under all Google domain names.[134] Google has a strong argument, given the fact that ninety-five percent of European users search Google under their respective country's domain name.[135]

Limiting the scope of the right to be forgotten through domain names is not the only alternative. Geographic

---

http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm ("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.").

130. Data Directive, *supra* note 50, art. 4; Data Regulation, supra note 61, art. 3; Soma et al., *supra* note 95, at 205–06.

131. *See* Data Directive, *supra* note 50, art. 4

132. *See id.*; Soma et al., *supra* note 95, at 205–06.

133. *See* Sam Schechner & Frances Robinson, *EU Says Google Should Extend 'Right to Be Forgotten' to '.com' Websites*, WALL ST. J. (Nov. 26, 2014, 10:59 AM), http://www.wsj.com/articles/eu-says-google-should-extend-right-to-be-forgotten-to-com-websites-1417006254.

134. *See* Antani, *supra* note 22, at 1178.

135. *See* Brendan Van Alsenoy & Marieke Koekkoek, *The Extra-Territorial Reach of the EU's "Right to be Forgotten"* 16 (Ctr. for IT & IP Law, Working Paper No. 20/2015); Letter from Peter Fleischer to Isabelle Falque-Pierrotin (July 31, 2014), http://online.wsj.com/public/resources/documents/google.pdf.

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.[136] All searches conducted in Germany, for example, would conceal personal information that Germans and/or Europeans successfully erased under the right to be forgotten. Identical searches conducted in the United States 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: "[s]ome 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

136. *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) (discussing how geotechnologies provide an automated means of identifying a user's location); 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) (discussing the legal framework for determining personal jurisdiction in cyberspace).

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

138. *See id.*

139. Antani, *supra* note 22, at 1177–79.

140. *Id*. at 1178.

141. Charles Arthur, *What Is Google Deleting Under the 'Right to Be Forgotten'—and Why?*, GUARDIAN (June 4, 2014), http://www.theguardian.com/technology/2014/jul/04/what-is-google-deleting-under-the-right-to-be-forgotten-and-why (internal quotations omitted).

are national networks."[142] The Internet of Spain is not the Internet of France or the Internet of the United States.[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, unequivocally rejected 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 in any case de-listing should also be effective on all relevant domains, including .com.[144]

A French data protection authority recently confirmed this admonition when it ordered Google to remove links from its database entirely, across all domains.[145] 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."[146] Google has thus far refused to comply, but the French pronouncement reflects the Working Party's statement as well as the forthcoming Regulation.[147] The

---

142. Toobin, *supra* note 5 (internal quotations omitted).

143. *See* Antani, *supra* note 22, at 1178.

144. Art. 29 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-131/12, 14/EN/WP225, Nov. 26, 2014, at ¶ 20.

145. Farhad Manjoo, '*Right to be Forgotten' Online Could Spread*, N.Y. 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.

146. *Id.* (internal quotations omitted).

147. *See* Julia Fioretti & Mathieu Rosemain, *Google Appeals French Order for*

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 server of a company processing data is located, non-European companies, when offering services to European consumers, must apply European rules."[148]

Upon the Regulation's enactment, one person on the other side of 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.[149] It will delete links not only in Munich, but also in Philadelphia, New Delhi, Auckland, and all points in between.[150] The 732,550 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, "effective[ly] and complete[ly]."[151] 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 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."[152] 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.

Global 'Right to be Forgotten,' REUTERS (May 19, 2016), http://www.reuters.com/article/us-google-france-privacy-idUSKCN0YA1D8.

148. EUROPEAN COMM'N, *supra* note 1.

149. *See* Data Regulation, *supra* note 61.

150. *See id.*

151. Art. 29 Working Party Guidelines, *supra* note 144.

152. Terry Carter, *Erasing the News: Should Some Stories Be Forgotten?* A.B.A. J. (Jan. 1, 2017, 12:10 AM), http://www.abajournal.com/magazine/article/right_to_be_forgotten_US_law (quoting Jonathan Peters, Chair of the First Amendment subcommittee of the ABA Section of Litigation) (internal quotations omitted).

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 all other countries in the world—particularly where such court orders stem from restrictive, undemocratic laws with an extraterritorial effect.[153]

Unilateral and extra-jurisdictional laws derogate normative international comity.[154] They ignore democratic values,[155] and in many cases, they upend alternative privacy protection regimes that tailor legal restrictions to the harms that result from privacy breaches.[156] Extra-territorial privacy laws promote one culture's devotion to privacy over another culture's preference for free expression.[157] Finally, they lay out an unfortunate blueprint for other nations to do likewise.[158] The EU Directive and Regulation are one-way ratchets. 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.[159] It is entirely possible that "there will be a race to the bottom towards adopting the norms of the most restrictive legal system."[160]

---

153. Svantesson, *supra* note 9, at 155.

154. *See* Rustad & Kulevska, *supra* note 23, at 409 (asking what country's law applies among the hundreds of countries regulating the Internet) ("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.).

155. Svantesson, *supra* note 9, at 155.

156. See *infra* Part V.

157. *See* Robert Kirk Walker, *The Right to Be Forgotten*, 64 HASTINGS L.J. 257, 274–76 (2012); 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.

158. Rustad & Kulevska, *supra* note 23, at 409.

159. *See id.*

160. *Id.*

III. 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.[161] But perhaps these negative secondary effects are necessary to achieve the law's primary goal—European data privacy. The central tenant of this Article suggests that even broadly applicable laws flounder 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.[162] In *Google Spain*, the CJEU required only that Google de-link Costeja's name from the newspaper article that originally published Costeja's debt.[163] The Court did not require the newspaper to take down the offending information from its website.[164] In thousands of deletion requests that followed, implementation was similarly limited to de-listing links rather than requiring data erasure from websites.[165]

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

---

161. *See supra* Part III.

162. Rustad & Kulevska, *supra* note 23, at 374 ("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.").

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

164. *See id.*

165. *See* EUROPEAN COMM'N, *supra* note 1.

be forgotten.[166] In other words, the websites that contain illicit EU 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.[167] 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 over 83 percent market share.[168] By 2015, however, Google's market share had slipped to 66.41 percent,[169] and "is now likely in permanent decline."[170] The search engine DuckDuckGo, by contrast, grew over seventy percent in 2015, receiving 3.25 billion search queries.[171] It attracted three million new searchers in October 2015 alone, "represent[ing] more than 100 percent year-over-year growth . . . ."[172]

Google, Bing, Yahoo!, AOL, and Ask formerly comprised

---

166. *See* McIntosh, *supra* note 34; *supra* note 35 and accompanying text.

167. *See* EUROPEAN COMM'N, *supra* note 1.

168. *Desktop Search Engine Market Share*, NETMARKETSHARE (Dec. 1, 2011), https://web.archive.org/web/20111201121858/http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0&qptimeframe=Y. In the United States, one 2015 study showed Google's share at 63.8 percent. *comScore Releases August 2015 U.S. Desktop Search Engine Rankings*, COMSCORE (Sept. 16, 2015), https://www.comscore.com/Insights/Rankings/comScore-Releases-August-2015-U.S.-Desktop-Search-Engine-Rankings.

169. *Desktop Search Engine Market Share*, *supra* note 40.

170. Frommer, *supra* note 41.

171. 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/.

172. *Id*.

the world's most popular search engines,[173] but scores of others exist, and several are regionally dominant.[174] Yandex has a sixty-two percent market share in Russia, while Baidu is China's most popular search engine.[175] Naver accounts for over seventy percent of South Korea's searches, and Yahoo! Japan services most searches in that country.[176] Other general search engines include Exalead, Gigablast, Munax, Qwant, Sogou, and Youdao.[177]

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.[178] Others are customized to trades, like IFACnet (accountancy); Fashion Net (fashion); and GlobalSpec (business).[179] Importantly, some search engines self-restrict by geography, including Accoona (China and United States); Ansearch (Australia, United States, United Kingdom, and New Zealand); Biglobe (Japan); Maktoob

---

173. *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, 11:00 AM), http://searchengineland.com/study-google-bing-yahoo-ask-aol-see-17-32-decline-search-traffic-last-6-months-194634.

174. *See* Julie Marie Bedas, *Search Engines Across the Globe*, FOUNDER'S GUIDE (July 10, 2015), http://foundersguide.com/search-engines-across-the-globe/.

175. *Id*. Baidu is the second largest search enginge in the world. Konrad Krawczyk, *Google Is Easily the Most Popular Search Engine*, *but Have You Heard Who's in Second?*, DIGITAL TRENDS (July 3, 2014, 11:34 AM), http://www.digitaltrends.com/web/google-baidu-are-the-worlds-most-popular-search-engines/.

176. Bedas, *supra* note 174.

177. *See If You Search Only with Google then you Miss A LOT!!!! About 95%*, SEARCH (Aug. 19, 2015), http://srch.3dmovies.com/2015/08/19/hello-world/ [hereinafter *If You Search Only with Google*].

178. *See* Sullivan, *supra* note 39.

179. A list of search engines delineated by trade, geographic scope, specific type of information sought and more can be found at *Search Engines*, FASHION, http://efemale.blogspot.com/2015/01/search-engines.html (last visited Apr. 2, 2017).

(Arab world); Rediff (India); Seznam (Czech Republic); and many more.[180] Customized search engines exist for food recipes, job searches, legal and medical information, news, real estate, and more.[181]

This proliferation reflects the decline in traditional and generalized desktop searching.[182] One study shows that the total number of people using traditional search engines decreased from fifty-five percent in the first quarter of 2014 to forty-nine percent in the first quarter of 2015.[183] More and more searches occur on mobile devices, through apps, and through social media.[184] According to Abid Chaudhry, a senior director at BIA/Kelsey, local searches on mobile apps are increasingly taking share, given that eighty-six percent of users' time on a mobile device is spent on an app.[185] "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 engines continues to decline."[186]

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

180. *If You Search Only with Google*, *supra* note 177.

181. *Search Engines*, *supra* note 179.

182. *See* Sullivan, *supra* note 39.

183. *See id.*

184. *Id.*

185. *Id.*

186. *Id.*

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."[187]

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,[188] but larger players followed, including the BBC, Reddit, and the Wikimedia Foundation.[189]

Wikipedia's page entitled, "Notices received from search engines," catalogues erasure requests by country of origin, website, and file.[190] Screen shots of the erasure requests are also included.[191] 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.[192]

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,

187. James Ball, *EU's Right to Be Forgotten: Guardian Articles Have Been Hidden by Google*, GUARDIAN (July 2, 2014), http://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google.

188. *Hidden from Google*, *supra* note 32; *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).

189. *See* McIntosh, *supra* note 34; sources cited *supra* note 35.

190. *Notices Received from Search Engines*, *supra* note 35.

191. *Id.*

192. *See e.g.*, *id*.

61, a pedophile who abducted an 11-year old girl with learning difficulties before abusing and murdering her."[193] 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.[194]

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.[195] *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.[196]

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,

---

193. 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.

194. Ball, *supra* note 187; 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.

195. T.C., *What Is the Streisand Effect?*, ECONOMIST (Apr. 16, 2013), http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect (noting the term was coined after American entertainer Barbara Streisand's attempt to suppress photographs of her Malibu Home resulted in extensive publicity, videos, spoof songs, and more).

196. *See generally* Greg Sterling, *Media Companies Republishing Google Right-To-Be-Forgotten Links*, SEARCH ENGINE LAND, (Oct. 17, 2014), 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.

Reddit, and others republish de-listed content, but these efforts take place on the surface web.[197] 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.[198]

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,[199] researchers describe the deep web's size in various and conflicting ways: over 96 percent of content on the world wide web,[200] unguessable,[201] 7500 terabytes,[202] infinite,[203] and 500x the size of the surface web.[204] 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.[205] The only U.S. court that has attempted to define the deep web,

---

197. *See* McIntosh, *supra* note 34; sources cited *supra* note 35.

198. Michael K. Bergman, White Paper: The Deep Web: Surfacing Hidden Value, J. Elec. Publ'g (Aug. 2001), http://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main.

199. Sharon D. Nelson & John W. Simek, *Ashley Madison and the Deep (and Sometimes Dark) Web*, MONT. LAW., Nov. 2015, at 18.

200. *Id.*; *see* Joseph Hirschhorn Howard, *Searching the Deep Web and the Unmapped Internet*, WEEKLY PIQUE (Oct. 16, 2015), http://www.weeklypique.com/2015/10/16/searching-the-deep-web/.

201. *See* Jose Pagliery, *The Deep Web You Don't Know About*, CNN MONEY (Mar. 10, 2014, 9:18 AM), http://money.cnn.com/2014/03/10/technology/deep-web/.

202. Bergman, *supra* note 198.

203. *Common Deep Web and Big Data Questions Answered—Part 1*, BRIGHTPLANET (Nov. 25, 2014), 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.").

204. SCH. INFO. MGMT. & SYS., HOW MUCH INFORMATION? at 4 (2003), http://groups.ischool.berkeley.edu/archive/how-much-info-2003/printable_report.pdf ("[T]he 'deep web' is perhaps 400 to 550 times larger than the information on the 'surface.'").

205. *See* Bergman, *supra* note 198.

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.[206]

The deep web contains all manner of content including text, photographs, videos, and music.[207] Large academic, library, and proprietary databases are stored on the deep web,[208] including core content from the U.S. Patent and Trademark Office, Thomson Reuters Westlaw, and NASA.[209] 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.[210] Similarly, the deep web can be searched even though it is not indexed like the surface web.[211] 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.[212]

The dark web has been characterized as a subset of the deep web.[213] Controversial and illicit transactions reputedly

---

206. *Am. Library Ass'n v. United States*, 201 F. Supp. 2d 401, 418–19 (E.D. Pa. 2002), *rev'd*, 539 U.S. 194 (2003).

207. *See* Pagliery, *supra* note 201.

208. *See* Bergman, *supra* note 198 (listing sixty of the largest deep web databases, including NASA, National Climatic Data Center, U.S. Trademarks and Patents, U.S. Census, SEC EDGAR, and more).

209. *Id.*

210. *Id.*

211. *See Tor: Overview*, TORPROJECT, https://www.torproject.org/about/overview.html.en (last visited Apr. 14, 2017).

212. *See* Stephanie Minnock, *Should Copyright Laws Be Able to Keep Up with Online Piracy?*, 12 J. ON TELECOMM & HIGH TECH. L. 523, 539–40 (2014).

213. *See* Stuart Andrews, *The Dark Side of the Web*, ALPHR (Mar. 9, 2010), http://www.alphr.com/features/356254/the-dark-side-of-the-web.

transpire on the dark web, including human trafficking, narcotic sales, and contracts for killings.[214] The dark web relies on anonymity tools to conceal both the seeker and the provider of such services.[215] It is not accessible through surface web browsers like Internet Explorer or Firefox, but is accessible via specialized and anonymized browsers such as Tor or I2P.[216] 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.[217] The Tor protocol leverages pseudomains like .onion as well as anonymous introduction points and relays between users, making de-anonymization difficult.[218]

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.[219] Journalists pursue controversial leads in the deep web to avoid government monitoring.[220] An array of law enforcement agencies search for illicit conduct using Tor because Tor hides government IP addresses, ensuring covert surveillance.[221] Whistleblowers reveal corporate and governmental malfeasance on the deep web to avoid retribution.[222]

---

214. *See* Abdulmajeed Alhogbani, *Going Dark: Scratching the Surface of Government Surveillance*, 23 COMMLAW CONSPECTUS 469, 482 (2015).

215. *Id.* at 482–83.

216. *See id.*

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

218. *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.").

219. TORPROJECT, *supra* note 211.

220. *See* Nelson & Simek, *supra* note 199, at 18.

221. Pell, *supra* note 218, at 528.

222. Watson, *supra* note 217, at 723.

But increasingly, normal Internet users opt for deep web browsing simply for additional privacy.[223] 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."[224] 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.[225] 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 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.[226] Technology infused objects gather, analyze, and send data through the Internet automatically, without an individual's prompting, and often without that individual's awareness.[227] Some libraries, for example,

223. *See* TORPROJECT, *supra* note 211.

224. TOR, https://www.torproject.org/ (last visited Apr. 14, 2017).

225. *See id.*

226. See Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98–117 (2014) (explaining the functioning of the Internet of Things).

227. *See id.*

electronically tag every book in the collection,[228] while tech savvy dentists prescribe toothbrushes engrafted with tiny sensors to determine hygiene behavior.[229] A pint of beer with tilt sensors records, analyzes, and transmits consumption rates.[230] 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 absorb everything we allow, and even more of which we are unaware.[231] Precise locational data is captured by license plate readers, automobile GPS, and smart phones.[232]

"Smart meters," another interesting example, produce meaningful efficiencies in utility consumption.[233] Replacing monthly inspections by utility employees, smart meters capture and transmit precise utility usage in real time.[234] While still in the nascent stages in the United States,[235] over

---

228. *See* Kendra Mayfield, *Tagging Books to Prevent Theft*, WIRED (May 20, 2002, 12:00 PM), http://www.wired.com/2002/05/tagging-books-to-prevent-theft/.

229. *See* Marcia Simon, *How the Kolibree 'Smart Toothbrush' Improves Dental Hygiene*, DENTISTRY IQ, (May 19, 2016), http://www.dentistryiq.com/articles/2016/05/how-the-kolibree-smart-toothbrush-improves-dental-hygiene.html.

230. *See* Kelsey Campbell-Dollaghan, *Vessyl: A Cup That Uses Molecular Sensors To Track Everything You Drink*, GIZMODO (June 12, 2014, 1:27 PM), http://gizmodo.com/vessyl-a-cup-that-uses-molecular-analysis-to-track-eve-1589975359 ("[A] cup that can calculate detailed information about what your [sic] drinking—and sync that information with your fitness tracker and peripheral apps.").

231. *See* 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, 1491–92 (2015).

232. VICTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 88–89 (2013).

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

234. Id. at 165.

235. *See Smart Meter Deployments Continue to Rise*, U.S. ENERGY INFO. ADMIN. (Nov. 1, 2012), https://www.eia.gov/todayinenergy/detail.php?id=8590 (identifying approximately thirty-six million smart meters recording and transmitting energy use in the United States as of 2012).

200 million smart meters are expected in the EU by 2020.[236] 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."[237] 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.[238] That data presents the groundwork for a multitude of observations about the resident's behaviors, attitudes, and proclivities.[239] One study claimed that the electrical signal coming from a resident's home revealed with ninety-six percent accuracy the specific television show viewed by the resident.[240]

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

---

236. PIKE RESEARCH, SMART METERS IN EUROPE: ADVANCED METERING INFORMATION FOR ELECTRIC UTILITIES IN EUROPE: BUSINESS AND TECHNOLOGY ISSUES, COUNTRY PROFILES, KEY INDUSTRY PLAYERS, AND MARKET FORECASTS *passim* (2012), http://www.navigantresearch.com/wp-content/uploads/2012/09/AMIEU-12-Executive-Summary.pdf

237. Patrick Thibodeau, *The Internet of Things Could Encroach on Personal Privacy*, COMPUTERWORLD (May 3, 2014, 7:45 AM), http://www.computerworld.com/article/2488949/emerging-technology/the-internet-of-things-could-encroach-on-personal-privacy.html (quoting Stephen Wicker).

238. *See* NAT'L INST. OF STANDARDS & TECH., GUIDELINES FOR SMART GRID CYBERSECURITY 231 (2014), 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); Stephen Wicker & R.J. Thomas, *A Privacy-Aware Architecture for Demand Response Systems*, CORNELL U., http://wisl.ece.cornell.edu/wicker/publications.html (last visited Apr. 2, 2017).

239. *See* Wicker & Thomas, *supra* note 238.

240. MIRO ENEV ET. AL., INFERRING TV CONTENT FROM ELECTRICAL NOISE 1 (2010), http://miro.enev.us/papers/EMI_CCS_2011.pdf; *see also* Chester Wisniewski, *Smart Meter Hacking Can Disclose Which TV Shows and Movies You Watch*, NAKED SEC. (Jan. 8, 2012), https://nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/.

refrigerator is open.[241] Software integrates this data with data from other smart home users to create predictive schematics.[242]

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."[243]

Something as anonymous as location points—with nothing more—can be used to pinpoint an individual. Cesar A. Hidalgo and Yves-Alexandre de Montjoye, researchers at MIT, correctly identified individuals using as few as four locational data points.[244] Indeed, a handful of past location points in conjunction with a few other data points reveals a person's "future" location.[245] 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.[246] Toll tags, license plate readers, and the

241. *See* Balough, *supra* note 233, at 165–66.

242. *See id.* at 162.

243. Narayanan & Shmatikov, *supra* note 110, at 25.

244. Yves-Alexande de Montejoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, SCI. REP., Mar. 25, 2013, at 1.

245. Tucker, *supra* note 113.

246. *See* Ben Waber, *Augmenting Social Reality in the Workplace*, MIT TECH. REV. (May 15, 2013), https://www.technologyreview.com/s/514371/augmenting-

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.[247] At the office, work badges loaded with sensors monitor employees' rapidity of speech, tone of voice, and workplace social interactions.[248] One organization seeks increased productivity by integrating software into the office infrastructure so that select employees are prompted to interact when economically expedient.[249] The software's algorithm spurs robotic movement of workplace walls, water coolers, and coffee machines to ensure that specific employees interact at discrete times.[250] While most offices have not integrated the passive data collected from employees this dramatically, the trend toward collection and use of passive data in workplaces continues.[251]

The Internet of Things is emerging. Over 220 billion connected devices worldwide are expected by 2020,[252] prompting Cisco to prognosticate that "pretty much

social-reality-in-the-workplace/; H. James Wilson, *Wearable Gadgets Transform How Companies Do Business*, WALL STREET J. (Oct. 20, 2013, 7:52 PM), https://www.wsj.com/articles/wearable-gadgets-transform-how-companies-do-business-1382128410?tesla=y.

247. CHING-YAO CHAN, CONNECTED VEHICLES IN A CONNECTED WORLD, 1–2 (2011), http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5783569; Francesca Svarcas, *Turning a New LEAF: A Privacy Analysis of CARWINGS Electric Vehicle Data Collection and Transmission*, 29 SANTA CLARA COMPUT. & HIGH TECH. L.J. 165, 167–74 (2012).

248. Waber, *supra* note 246; Wilson, *supra* note 246.

249. *See* Waber, *supra* note 246.

250. *Id.*

251. *See* Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe*, *Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1001–18 (2011).

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

everything you can imagine will wake up."[253] Combined with a world of other and 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.[254] Just because a particular data point is anonymous or non-identifying at the point of collection does not mean it will remain so.[255] Non-identifying information quickly loses anonymity when combined with the vast and diverse data already available, suggesting inevitability of "re-identification."[256]

Capacious privacy laws overlook the Internet of Things, passive data collection, and automated gathering of data exhaust. The EU Directive turns on data collection, requiring notice and consent before personal data can be lawfully collected.[257] 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. 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."[258]

V. REGULATING FOR PRIVACY, RISK OF HARM

Responding to loss of privacy in the Internet age with

253. *What Is the Internet of Everything?*, CISCO SYSTEMS, http://www.cisco.com/c/m/en_in/tomorrow-starts-here/ioe.html (last visited Apr. 2, 2017).

254. *See* Ohm, *supra* note 109, at 1716–25

255. *See id.* at 1703–04.

256. *See* Narayanan & Shmatikov, *supra* note 110, at 26.

257. Data Directive, *supra* note 50, art. 7, 10; Data Regulation, *supra* note 61.

258. A.T. KEARNEY, WORLD ECON. FORUM, RETHINKING PERSONAL DATA: A NEW LENS FOR STRENGTHENING TRUST 3 (2014), http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf.

unilateral, extra-jurisdictional laws that mandate deletion of personal information if that information is deemed irrelevant fails to meaningfully advance the original goal 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.[259] 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 sensitive data as it relates to particular risks or harms better comports with consumer law generally and permits the needed adaptability to reflect context and changing technology."[260]

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.[261] Rather than an over-broad EU law that captures oceans of harmless data processing and that incentivizes uneven enforcement at the expense of international comity,[262] privacy law should

259. *See supra* Section III.D.

260. McKay Cunningham, *Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm*, 2 GRONINGEN J. INT'L LAW 115, 142 (2014).

261. *See* Bajarin, *supra* note 252.

262. *See supra* Part III.

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.[263] 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.[264] It is not the fact of this data's processing that merits legal protection, but its inappropriate use.[265] 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.[266] 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 EU'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.[267] Privacy regulations more closely parallel this reality by distinguishing passively created data from actively created data, by delineating "external" data from "internal"

---

263. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 529 (2006); *see* 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, 895–96 (2011).

264. *See* Ambrose, *supra* note 9, at 18; Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1972–79 (2013).

265. *See generally* DANIEL SOLOVE, UNDERSTANDING PRIVACY 188–89 (2008).

266. *See id.* at 131–32.

267. *See* Solove, *supra* note 263 at 481–82, 485.

data, and by identifying original data from downstream transformation or modification of that data.[268] 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.[269] Privacy protections differ depending on such distinctions.[270] 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.[271]

Indeed, the legal infrastructure for many of these permutations is already in place. In the United States and the EU, defamation law protects against untrue harmful publications, reflecting the ethos behind the right to be forgotten.[272] Copyright law also advances objectives that are similar to the right to be forgotten.[273] 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.[274]

"[T]he Children's Online Privacy Protection Act provides for a right to delete personal data. The Fair Credit Reporting Act restricts the ability of consumer reporting agencies to

---

268. Ambrose, *supra* note 9, at 11.

269. *See id*.

270. *See generally* Solove, *supra* note 263.

271. *See* Ambrose, *supra* note 9, at 11, 18.

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

273. *See* Copyright Act, 17 U.S.C. § 107 (2012); Universal City Studios, Inc. v. Corley, 273 F.3d 429, 458–60 (2d Cir. 2001).

274. *See, e.g.*, Eriq Gardner, *Google Responds to Jennifer Lawrence Attorney's $100 Million Lawsuit Threat*, HOLLYWOOD REP. (Oct. 2, 2014, 12:23 PM), http://www.hollywoodreporter.com/thr-esq/google-responds-jennifer-lawrence-attorneys-737656.

report on bankruptcies and criminal proceedings that are beyond a certain number of years old."[275] These legal doctrines carry the added benefit of refinement through decades of case law, legislation, and other democratic processes.

Bankruptcy protections,[276] privacy controls integrated into criminal law,[277] like grand jury proceedings,[278] and laws allowing sealed and expunged court records for juveniles[279] all protect privacy rights in distinct contexts more closely associated with the potential harm that would result absent such protections.[280] One commentator suggests that specifically tailored privacy laws like these illustrate continuity with EU privacy objectives rather than disharmony: "developments in American law signal a receptivity to EU privacy norms that is not well reflected in media and free speech advocates' desire to cast the Atlantic divide as irreconcilable divergence."[281]

---

275. Daniel Solove, *What Google Must Forget: The EU Ruling on the Right to Be Forgotten*, LINKEDIN: TECH (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].

276. *See Process—Bankruptcy Basics*, U.S. CTS. http://www.uscourts.gov/services-forms/bankruptcy/bankruptcy-basics/process-bankruptcy-basics (last visited Apr. 3, 2017) (discussing United States Bankruptcy Code, 11 U.S.C. §§ 101–1532 (2012)).

277. *See, e.g.*, FED. R. CRIM. P. 32(d)(3) (2014). 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 (2004).

278. *See* FED. R. CRIM. P. 6(d).

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

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

281. *Id.* at 410.

In contrast to these specific measures, the right to be forgotten requires that data controllers delete links to "irrelevant" content.[282] Data controllers, like Google, decide whether the requested content is irrelevant or inadequate, not a court, agency, or other public body.[283] "[I]t 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."[284] Paralyzing fines for refusing valid erasure requests[285] incentivize Google to err on the side of deleting content, which perhaps explains why Google has so far approved forty-three percent of those requests, de-listing approximately 830,180 URLs as of the date of this publication.[286] Privacy is poorly served through a rubric of economic intimidation and the catch-all standard of irrelevance.[287] 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."[288] Claims that digital data are impossible to forget or that once posted, data forever remain readily accessible,

---

282. EUROPEAN COMM'N, *supra* note 1.

283. *Id.*

284. *Id.*

285. The current Data Directive allows fines up to two percent worldwide turnover, which will increase to the greater of €10 million or two percent of annual worldwide turnover or the greater of €20 million or four percent worldwide turnover under the new Regulation. *See* Data Regulation, *supra* note 61; Regulation (EU) 2016/679, *supra* note 128; *see also* Emily Adams Shoor, Note, *Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation*, 39 BROOK. J. INT'L L. 487, 488, 508 (2014).

286. *Transparency Report: European Privacy Requests for Search Removals*, *supra* note 17.

287. *See* Rustad & Kulevska, *supra* note 23, at 370, 373.

288. Ambrose, *supra* note 9, at 13.

are wrong.[289] 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.[290] Using URLs as a metric, one study tracked tweets about significant events including the H1N1 virus and the Syrian revolution.[291] Approximately eleven percent of the content associated with those tweets disappeared within one year, increasing to twenty-seven percent after two years.[292] A litany of diverse causes contributes to digital decay.[293] Importantly, personal bias is not among them.[294] If digital information must disappear, it should be culled through objective, automated processes, rather than by those with the most bias toward it.[295]

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

289. *Id.* at 1, 9, 12.

290. *See id.*

291. *Id.*

292. *Id.*

293. *Id.*

294. *See id.*

295. 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*, STAND. U., http://infolab.stanford.edu/~backrub/google.html (last visited Apr. 3, 2017).

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 EU, through legal recognition of the right to be forgotten, attempted to address that question. The EU 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 800,000 URLs have been delisted as individuals seek to erase access to their personal information, often indiscretions, from public view.

While laudable in the abstract, in 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,"[296] lawmakers seeking to regulate Internet use must consider its architecture. Instead, European

296. *See* Stephen Levingston & International Herald Tribune, *Internet Entrepreneurs Are Upbeat Despite Market's Rough Ride*, N.Y. 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.) (internal quotations omitted).

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 EU law to anyone who processes personal information theoretically addresses the problem of transnational data flow, but it also creates 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 EU 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 EU have created similar privacy laws, but the EU'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.