ARTICLES

THE NEW AMERICAN PRIVACY

RICHARD J. PELTZ-STEELE*

ABSTRACT

Conventional wisdom paints U.S. and European approaches to privacy at irreconcilable odds. But that portrayal overlooks a more nuanced reality of privacy in American law. The free speech imperative of U.S. constitutional law since the civil rights movement shows signs of tarnish. And in areas of law that have escaped constitutionalization, such as fair-use copyright and the freedom of information, developing personality norms resemble European-style balancing. Recent academic and political initiatives on privacy in the United States emphasize subject control and contextual analysis, reflecting popular thinking not so different after all from that which animates Europe's 1995 directive and 2012 proposed regulation. For all the handwringing in the United States over encroachment by anti-libertarian EU regulation, a new American privacy is already on the rise.

TABLE OF CONTENTS

---

* Professor, University of Massachusetts School of Law. I am indebted to the *European Law Review*, which solicited from me a feature on this topic, forthcoming at the time of this writing in December 2012; to Randy Aliment, American Bar Association Tort Trial Insurance Practice Section, and Paul A.M. Witteveen, Union Internationale des Avocats, for the opportunity to present on this and related subjects at the Dresden 2012 meeting of the Union Internationale des Avocats; to the UMass Law School for a grant that supported this work; and most of all to Ashley Messenger, who brought this topic to my attention and generously visited UMass to talk to my students. Ms. Messenger is counsel for National Public Radio in the United States and adjunct professorial lecturer in the American University School of Communication. She wrote ably on this topic in *What Would a "Right to be Forgotten" Mean for Media in the United States?*, 29 COMM. LAW. 29 (2012).

I. INTRODUCTION AND THE "RIGHT TO BE FORGOTTEN" PROBLEM

The European Union (EU) fired the first shot this year in what pundits are sizing up as a new front in the trans-Atlantic war over the right to privacy. A proposed regulation[1] is likely to become law in some form in the 27-member EU, and it will supersede the 1995 Data Protection Directive (DPD).[2] The new regulation substantially increases burdens on data handlers,[3] enhancing reporting requirements, toughening the expectation of explicit personal consent to the use of personal data, and giving data subjects more control over their information through rights of revocation and, the flashpoint of intercontinental controversy, the "right to be forgotten." Most importantly, the regulation as proposed would sweep within its ambit for the first time foreign actors who do business in the EU. Critics, especially in the United States, forewarn of inevitable collision between EU privacy and the U.S. First Amendment.[4]

Fn1 Fn2 Fn3 Fn4

1. *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 Proposal], http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

2. Directive 95/46/EC of the European Parliament and the Council 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 Directive], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF.

3. This article refers broadly and informally to data processors and processing, meaning all entities and activities within the regulatory scope of the DPD. The DPD is broad itself. It pertains to data "controller[s]," which "alone or jointly with others determine[] the purposes and means of the processing of personal data," *id.* art. 2(d), and to data "processor[s]," "which process[] personal data on behalf of the controller," *id.* art. 2(e). "[P]ersonal data" in turn means "any information relating to an identified or identifiable natural person ('data subject') . . . 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." *Id.* art. 2(a). "[P]rocessing" means "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." *Id.* art. 2(b). The proposed regulation has comparable scope except as explained here as to territoriality. *See* Proposal, *supra* note 1, art. 4.

4. U.S. CONST. amend. I.

The simple picture of irreconcilable conflict across the Atlantic conceals nuances on both sides. An observer of American constitutional law from a comparative perspective is impressed on the one hand by the free speech imperative of the First Amendment, of which the firm rule against prior restraint is a part. The imperative posits free speech as the presumptive winner when it comes into conflict with other interests, such as statutory prohibitions, or even with other
Fn5 constitutional rights.[5] To lose out, the free speech claim must be
Fn6 rebutted by countervailing interests, few of which can measure up.[6]

---

5. Free expression law in the United States employs a complex hierarchy of heightened scrutiny to test the viability of statutes that contravene private speech interests. In a nutshell: Viewpoint-discriminatory regulations are flatly invalid. *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 391-92 (1992). Content-based and viewpoint-neutral regulations are valid only if they survive strict scrutiny, *i.e.*, directly furthering compelling state interests in the absence of less restrictive alternatives. *See, e.g.*, United States v. Playboy Entertainment Group, 529 U.S. 803, 812-13 (2000). Regulations both content- and viewpoint-neutral are valid only if they survive intermediate scrutiny, *i.e.*, furthering significant state interests in a narrowly tailored manner. *See, e.g.*, Turner Broadcasting Sys., Inc. v. F.C.C., 520 U.S. 180, 189 (1997). And even regulations subject to no heightened scrutiny, perhaps owing to a special context such as prison or school, must meet some minimal threshold of rationality. *See* Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260, 273 (U.S. 1988) (schools); Turner v. Safley, 482 U.S. 78, 89 (1987) (prisons). The heightened-scrutiny system extends furthermore into the realm of torts insofar as the specter of civil liability would dampen free expression. *See* New York Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964) (powerfully elevating burdens on public-official defamation plaintiffs); Gertz v. Robert Welch, Inc., 418 U.S. 323, 342-43 (1974) (extending *Sullivan* to public-figure plaintiffs); *see also* Hustler, Inc. v. Falwell, 485 U.S. 46, 50-53 (1988) (extending *Sullivan* doctrine in part to intentional infliction of emotional lest doctrine be undermined). The government bears the burden of rebutting the presumption of regulation invalidity. *Playboy*, 529 U.S. at 817. This system resembles the affirmative-right/public-welfare-exception model of free expression commonly represented in international and constitutional legal instruments such as the European Convention on Human Rights, Convention for the Protection of Human Rights and Fundamental Freedoms art. 10, Nov. 4, 1950, 213 U.N.T.S. 222. But perhaps owing to the breadth of the "necessary in a democratic society" exception, those analyses tend to reduce to balancing more than strong presumption favoring free expression. *See, e.g.*, Observer & Guardian v. United Kingdom, App. No. 13585/88, 14 Eur. H.R. Rep. 153, ¶¶ 61-65 (1992). The U.S. First Amendment generates an analysis closer to the human rights balancing approach when it collides with a countervailing interest of constitutional magnitude, such as fair trial. *See* Sheppard v. Maxwell, 384 U.S. 333, 349-52 (1966). But even when rights collide, the First Amendment may demand a least-restrictive-means analysis, as when weighing the necessity for closure to the public of the criminal courtroom. *See, e.g.*, Press-Enterprise Co. v. Superior Court, 438 U.S. 1, 15 (1986).

6. Strict scrutiny is notoriously fickle, despite the Court's repeated assertions to the contrary. *See* Emp't Div. v. Smith, 494 U.S. 872, 888 (1990) (in religious freedom case, warning against "watering . . . down" compelling-state-interest prong of strict scrutiny). *Compare* Fullilove v. Klutznick, 448 U.S. 448, 507 (1980) (Marshall, J., concurring) (describing strict scrutiny in equal protection context as "strict in theory, but fatal in fact"), *with* Adarand Constructors, Inc. v. Peña, 515 U.S. 200, 237 (endeavoring to "dispel the notion" of "strict in theory, but fatal in fact"). *See*

The observer is impressed on the other hand by the weak development in American constitutional law of rights of personality, including reputation and privacy. Lacking the full constitutional gravitas of free speech, these "rights" fare poorly when they run up against the American free speech imperative.

Throw into the mix the American affection for *laissez faire* economic regulation, and the conflict between privacy in Europe and free speech in the United States starts to come into focus. Even supposing that U.S. lawmakers were inclined to regulate the commercial information marketplace, rules that preclude the dissemination of lawfully obtained, truthful information run headlong into the free speech imperative and the rule against prior restraints. The controverted commercial speech doctrine offers some room for an information-regulatory regime in the United States, subject to an intermediate constitutional scrutiny. But the EU system is not confined to the commercial context.

The "right to be forgotten" is one small part of the proposed EU
Fn7 regulation,[7] but it exposes the crux of the problem. Under the proposal, a person may demand the removal of personal information from
Fn8 data processing and dissemination.[8] Prohibiting the subsequent dissemination of truthful information, lawfully obtained, defies the American free speech imperative. Worse from the American perspective, the rebutting privacy claim is not necessarily even an interest of constitutional magnitude. Any reasonably identifying information triggers the
Fn9 EU regulatory framework,[9] because the broader right of personality animates the regulation, not the narrower American conception of
Fn10 privacy in the intimate or "highly offensive."[10]
Fn11 A recent European case against Google is illustrative.[11] Alfacs Va-

---

generally Ozan O. Varol, *Strict in Theory, but Accommodating in Fact?*, 75 MO. L. REV. 1243, 1244-57 (2010).

7. *See* Proposal, *supra* note 1, art. 17 ("Right to be forgotten and to erasure").

8. *Id.* arts. 17, 19.

9. *Id.* art. 4(1).

10. Invasion of privacy in U.S. state law typically requires that the invasion or its disclosure be "highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS §§ 652B (intrusion), 652D (disclosure), 652E (false light) (1977); *see, e.g.*, Stien v. Marriott Ownership Resorts, Inc., 944 P.2d 374, 379 (Utah Ct. App. 1997) (affirming trial court finding as a matter of law that "highly offensive" element could not be met in display of humorous video).

11. *See* S. Juz. Prim., Feb. 23, 2012 (No. 32) (Spain), *available at* http://app.expansion.com/zonadescargas/obtenerDocumento.html?codigo=14474 (last visited July 24, 2012). *See generally* Miquel Peguera, *More on the Alfacs v. Google case and the "right to be forgotten"*, ISP LIABILITY (Feb. 29, 2012), http://ispliability.wordpress.com/; Miquel Peguera, *Google Spain wins lawsuit over the 'right to be forgotten'*, ISP LIABILITY (Feb. 27, 2012), http://ispliability.wordpress.com/.

cances, S.L., operates a campground in Spain at which a horrific propane-truck accident in 1978 incinerated 160 persons and gravely
Fn12 wounded 300 more.[12] Alfacs complained that searches on Google Spain (www.google.es) for the campground in 2005 called up firstly pictures of the blackened corpses with accompanying graphic descriptions of the tragedy, not to mention reports of persistent paranormal
Fn13 reverberations.[13] Alfacs submitted that its business reputation was
Fn14 impugned and customers lost to the tune of €300,000 in damages.[14] Google asserted a free speech interest in its links and in the ordering of
Fn15 search results.[15] But more importantly, Google Spain, S.L., the respondent within the personal jurisdiction of Spanish authorities, professed that it has no authority or ability to operate the Google search engine, which is administered by the corporate entity Google, Inc., in the
Fn16 United States.[16] A Spanish trial court agreed that Alfacs had sued the
Fn17 wrong party.[17]

Though the *Alfacs* case arose in the trial court as a claim of corporate reputational injury, the facts mirror a pattern in more than 100
Fn19 pending claims[18] before the Spanish data protection authority.[19] Spanish law, unexceptionally in the EU, goes beyond the barest requirements of the DPD, if not as far as the proposed regulation, to afford
Fn20 claimants a right to be forgotten, or to erasure.[20] These claims keep
Fn21 Google counsel up at night.[21] A person might employ the right to be forgotten to demand that Google purge from its data stores any

---

12. *See* S. Juz. Prim., Feb. 23, 2012 (No. 32) (Spain).

13. *Id.*

14. *Id.*

15. *Id.*

16. *Id.*

17. *Id.*

18. Sonya Angelica Diehn, *Spanish Firm Loses 'right to be forgotten'*, WORLD IT LAWYERS (Apr. 13, 2012), http://www.worlditlawyers.com/spanish-firm-loses-right-to-be-forgotten-with-cristina-sanchez-tembleque-ecija-comments; Jacob Sloan, *Spanish Court: You Do Not Have the Right to be Forgotten*, DISINFORMATION (Mar. 19, 2012), http://www.disinfo.com/2012/03/spanish-court-you-do-not-have-the-right-to-be-forgotten/.

19. *See also* T.C. Sottek, *Spain Challenges Google with "Right to Be Forgotten" in EU*, VERGE (Mar. 5, 2012), http://www.theverge.com/2012/3/5/2846192/google-right-to-be-forgotten-Spain-EU-court.

20. Protección de Datos de Carácter Personal arts. 5-6, 13, 16-17 (B.O.E. 1999, 298) (implementing Directive, *supra* note 2).

21. *See* Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, PETER FLEISCHER: PRIVACY . . . ? (Mar. 9, 2011, 8:59 AM), http://peterfleischer.blogspot.com; *see also* David Meyer, *Google Picks Holes in EU's "Right to Be Forgotten,"* ZDNET UK (Feb. 17, 2012), http://www.zdnet.co.uk/news/regulation/2012/02/17/google-picks-holes-in-eus-right-to-be-forgotten-40095071/.

identifying information to which the person objects—an unfavorable review of services or an embarrassing photo, regardless of truth, of previous consensual disclosure, or third-party content creator. Under the proposed regulation, domestic European authorities could bring Google, Inc. (U.S.) within reach of EU data protection enforcement (provided long-arm jurisdiction in domestic law[22]), because Google, Inc., provides its services to EU citizens.[23] Under data protection legislation, Google could face remedies that it would regard as censorship, including correction and redaction. Notwithstanding enforcement against a respondent's EU assets, an injunction against technological operations in the United States would set up a classic confrontation of foreign-judgment enforcement and First Amendment values.[24]

In fact, the nightmare scenario already has unfolded. Google and Yahoo in Argentina successfully battled defamation (or moral harm) claims over search results that led users to sexually provocative content regarding entertainer Virginia da Cunha.[25] While the two services were

22. Personal jurisdiction for online harms is still evolving, but the trend is towards U.S. long-arm jurisdiction. *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1205-11 (9th Cir. 2006) (predicating personal jurisdiction over foreign defendants upon their efforts to enforce foreign judgment against U.S. defendant), and a landmark Australian case, *Dow Jones & Co. v. Gutnick* (2002) 210 CLR 575 (predicating personal jurisdiction on allegedly defamatory publication in Australia), promise a broad reach for domestic courts. *See also* Aaron Warshaw, Note, *Uncertainty from Abroad: Rome II and the Choice of Law for Defamation Claims*, 32 BROOK. J. INT'L L. 269, 283 n.86 ("Notably, *Gutnick* has been cited with approval by a number of courts within Europe.") (citing as example Lewis v. King, [2004] EWCA (Civ.) 1329 (Eng.)). Large operations such as Google and Facebook have offices in Europe, so personal jurisdiction is not at issue.

23. *See* Proposal, *supra* note 1, art. 3.

24. This conflict is familiar in the area of defamation, especially in recent discussion and lawmaking regarding "libel tourism." The prospects for foreign enforcement of judgments arguably inconsistent with First Amendment values have waxed and waned. *See generally* Lili Levi, *The Problem of Trans-National Libel*, 60 AM. J. COMP. L. 507 (2012); Marissa Gerny, Note, *The SPEECH Act Defends the First Amendment: A Visible and Targeted Response to Libel Tourism*, 36 SETON HALL LEGIS. J. 409 (2012) (analyzing especially Securing the Protection of our Enduring and Established Constitutional Heritage Act, Pub. L. No. 111-223, 124 Stat. 2380 (2010) (codified at 28 U.S.C. §§ 4101-05) (2006))). Waxing prospects call to mind the personal jurisdiction decision and First Amendment non-decision in *Yahoo! Inc.*, 433 F.3d at 1199.

25. Cámara Federal de Apelaciones [CFed.] [federal court of appeals], 10/8/2010, "D.C.V. c. Yahoo de Argentina SRL" (Arg.) [hereinafter *D.C.V.*], *available at* SABER LEYES (Aug. 21, 2010), http://saberleyes.blogspot.com/2010/08/da-cunha-virginia-v-yahoo-de-argentina.html. *See generally* UNIVERSIDAD DE PALERMO FACULTAD DE DERECHO & CENTRO DE ESTUDIOS EN LIBERTAD DE EXPRESION Y ACCESO A LA INFORMACION, EMERGING PATTERNS IN INTERNET FREEDOM OF EXPRESSION: COMPARATIVE RESEARCH FINDINGS IN ARGENTINA AND ABROAD (2010), *available at* http://www.palermo.edu/cele/libertad-de-expresion-en-Internet.pdf.

exonerated of having themselves defamed da Cunha, the underlying content that she found offensive continues to be legally problematic. The appellate court rejected the defamation claim because Google and Yahoo lacked actual knowledge of the defamatory content,[26] a defense that only works once.[27] Google has maintained that it cannot redact specific items from its search returns for da Cunha,[28] and its Argentine search engine has continued to return controverted content.[29] So Google might still be on the hook. Yahoo's Argentine search engine meanwhile returns no data upon a search for da Cunha, rather an Orwellian message that search results are suspended by court order.[30] Moreover, da Cunha's case is not unique. *The New York Times* reported in August 2010 that more than 130 similar cases, including one by football star Diego Maradona,[31] were pending in Argentine courts.[32] Cases such as these lead constitutional law experts such as Professor

Fn26 Fn27 Fn28 Fn29 Fn30 Fn32

26. *See id.*

27. A similar safe harbor protected Google from defamation liability in a 2009 Spanish case commonly referred to as "*Palomo v. Google.*" *See* S.A.P, Feb. 19, 2010 (No. 95) (Spain) (applying Protección de Datos de Carácter Personal, art. 17 (B.O.E. 1999, 298, at 43088), *available at* RESPONSABILIDAD EN INTERNET, (Feb. 19, 2010), http://responsabilidadinternet.wordpress.com/, *and cited by* ISP LIABILITY, (Feb. 29, 2012), http://ispliability.wordpress.com/. Citing *Palomo* in its trial court manifestation, a U.K. court recognized a trend toward such limitation of liability in laws across Europe. Metro. Int'l Sch. Ltd. v. Designtechnica Corp., [2009] EWHC (QB) 1765 [97]-[114], [2010] 3 All E.R. 548, [2011] W.L.R. 1743 (Eng.), *available at* http://www.bailii.org/ew/cases/EWHC/QB/2009/1765.html, *cited by* More on the Alfacs v. Google case and the "right to be forgotten", ISP LIABILITY (Feb. 29, 2012), http://ispliability.wordpress.com/2012/02/29/more-on-the-alfacs-v-google-case-an-the-right-to-be-forgotten/. This scienter limitation does not, of course, go as far as 47 U.S.C. § 230 immunity in the United States.

28. *See, e.g.*, 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).

29. GOOGLE ARGENTINA, http://www.google.com.ar/ (search "Virginia da Cunha") (last visited July 24, 2012).

30. YAHOO! ARGENTINA, http://ar.yahoo.com/ (search "Virginia da Cunha") (last visited July 24, 2012) ("Con motivo de una orden judicial solicitada por partes privadas, nos hemos visto obligados a suprimir temporalmente todos o algunos de los resultados relacionados con ésta búsqueda.").

31. *See also* Uki Goni, *Can a Soccer Star Block Google Searches?*, TIME (Nov. 14, 2008), http://www.time.com/time/world/article/0,8599,1859329,00.html. Time furthermore reported that political figures as well as athletes, models, and entertainers are among the plaintiffs, *id.*, adding a distinctly *New York Times v. Sullivan*, 376 U.S. 254 (1964), dimension to the problem.

32. *See* Vinod Sreeharsha, *Google and Yahoo Win Appeal in Argentine Case*, N.Y. TIMES (Aug. 19, 2010), http://www.nytimes.com/2010/08/20/technology/internet/20google.html; *see also* Rosen, *supra* note 28, at 1533 (citing Vinod Sreeharsha, *Google and Yahoo Win Appeal in Argentine Case*, N.Y. TIMES (Aug. 20, 2010)). CNet reported about 70 pending lawsuits in 2008. Stephanie Condon, *Argentine Judge: Google, Yahoo Must Censor Searches*, CNET NEWS (Nov. 11, 2008), http://news.cnet.com/8301-13578_3-10094597-38.html.

Jeffrey Rosen to conclude that the effect of the EU regulation will be to diminish the range of information freely available to the world via the Internet.[33]

Fn33

There is, however, a dynamic on the United States' side of the equation that has not been well explored in the literature. While media and free speech advocates foretell a grave threat,[34] it might be that the American value threatened is not so hallowed after all. Underlying the free speech position is the assumption that the free speech imperative and its sacrosanct rule against prior restraints represent axiomatic American values. That might not be true.

Fn34

Contemporary free speech law in the United States, especially in areas of tort and criminal defense, was shaped dramatically by the civil rights movement. The doctrines that emerged from that era undoubtedly made crucial innovations in furtherance of fundamental human rights in the United States and around the world. But in some cases, the constitutional jurists might have reached too far—over-protecting interests such as free speech without fully considering the implications for competing interests. Technologies such as the Internet and social developments such as the 24-7 news appetite furthermore have changed the game in unforeseen ways. An American ethos in which free speech is king and rights of personality are relatively marginal was once axiomatic; now, with countervailing forces in play, that axiom is fissuring.

Free speech and media advocates might or might not be justified in their fears about the implications of EU privacy for the flow of information in the world. The purpose of this Article is not to adjudicate that question, but to posit an ancillary thesis: that the proposed EU regulation is a better reflection of already extant U.S. norms than media advocates would care to say; and therefore, American privacy norms already are moving in the direction of Europe's. The Atlantic divide that is often imagined as a collision of tides moving in opposite directions might instead be a convergence of waves moving the same way.

The following Part II examines summarily the proposed EU regula-

---

33. *See* Rosen, *supra* note 28, at 1533-34; *see also* Jeffrey Rosen, *A Grave New Threat from Europe*, NEW REPUBLIC (Feb. 10, 2012) [hereinafter Rosen, *Grave New Threat*], http://www.tnr.com/article/politics/100664/freedom-forgotten-internet-privacy-facebook; Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012) [hereinafter Rosen, *Right to be Forgotten*], http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.

34. *See generally* Rosen, *supra* note 28; Rosen, *Grave New Threat*, *supra* note 33; Rosen, *Right to be Forgotten*, *supra* note 33.

tion, especially with respect to the "right to be forgotten," to facilitate understanding of issues and objections. Part III examines the U.S. coastline, highlighting promontories in information and free expression law that reveal a less-than-monolithic commitment to EU-contrary principles often presumed to be axiomatically American. Part IV briefly engages recent scholarship in the area of privacy to demonstrate its consistency with a nuanced approach more common to U.S. and EU law than antithetical to either. Part V concludes by positing that this common vein represents the emergence of a new American privacy.

II. THE EU PROPOSED REGULATION

Fn36 While the DPD[35] caused its share of uproar in the 1990s,[36] its scope ultimately was limited to data processing occurring within EU Member Fn37 States.[37] The DPD therefore minimally obliged to provide information Fn38 giants such as Google and Facebook[38] based in the United States or Fn39 elsewhere outside Europe.[39] The new regulation would end that honeymoon and endeavor to bring businesses within reach of EU law if they "offer[] goods or service to . . . data subjects in the Union" or "monFn40 itor[] their behaviour."[40] Moreover, as a regulation rather than a directive, the proposed regulation would be self-executing in EU Member States, not dependent on the enactment of domestic legislaFn41 tion.[41] This change bolsters the central rationale for regime revision: the need to wrest uniformity from domestic implementations of the

35. Directive, *supra* note 2.

36. *See, e.g.*, Jane E. Kirtley, *The EU Data Protection Directive and the First Amendment: Why a "Press Exemption" Won't Work*, 80 IOWA L. REV. 639 (1995).

37. Directive, *supra* note 2, art. 4.

38. Facebook voluntarily submitted to EU jurisdiction for purposes of non-North American data when the company located an international office in Dublin. Garnering favorable worldwide publicity, the information giant cooperated with Irish data protection authorities to bring its practices into compliance with Irish and European law. *E.g.*, *Irish Privacy Watchdog Call for Facebook Changes*, BBC NEWS (Dec. 21, 2011), http://www.bbc.com/news/technology-16289426.

39. *See also* Patrick van Eecke, Cameron Craig & Jim Halpert, *The First Insight into the European Commission's Proposal for a New European Data Protection Law*, 15 J. INTERNET L. 19 (2012); *Private Data, Public Rules*, ECONOMIST (Jan. 28, 2012), http://www.economist.com/node/21543489 (describing data protection legislation in India and China, noting that by way of population, those systems might one day edge out EU law in world standard-setting).

40. Proposal, *supra* note 1, art. 3(2).

41. *Id.* mem. § 3.1.

Fn42 Fn43 Fn44 1995 DPD that have diverged over time[42] and thus mitigated the social and economic advantages of an EU-wide approach.[43] Reform supporters such as European Commissioner Viviane Reding have promised a skeptical business community that harmonization across EU governments will amount to cost savings in compliance.[44]

Fn45 The regulation is lengthy, but the following are some key substantive provisions that have fueled discussion.[45]

A. *Consent*

Fn46 Fn47 Fn48 Where the DPD required data subjects' "unambiguous[]" consent to data processing,[46] the proposed regulation makes plain that consent must be "explicit."[47] Explicit consent requires an affirmative act by the data subject, such as ticking a box upon a clear and plain statement of the data controller's policies.[48] The subject's "[s]ilence or inactivity"

---

42. *See generally* WAINER LUSOLI ET AL., PAN-EUROPEAN SURVEY OF PRACTICES, ATTITUDES AND POLICY PREFERENCES AS REGARDS PERSONAL IDENTITY MANAGEMENT (2012), http://is.jrc.ec.europa.eu/pages/TFS/documents/EIDSURVEY_Web_001.pdf.

43. Proposal, *supra* note 1, mem. § 2; *see also* J.C. Buitelaar, *Privacy: Back to the Roots*, 13 GER. L.J. 171 (2012) (detailing shortcomings of DPD).

44. *See* Proposal, *supra* note 1, mem. § 2; *see also* Peter Bright, *Europe Proposes a "Right to be Forgotten,"* ARS TECHNICA (Jan. 25, 2012), http://arstechnica.com/tech-policy/2012/01/eu-proposes-a-right-to-be-forgotten/ (reporting projected cost savings of €2.3 billion and business skepticism); Stanley Pignal & Maja Palmer, *New EU Privacy Rules Worry Business*, FIN. TIMES (Jan. 22, 2012), http://www.ft.com/cms/s/2/e14f2f3e-44f3-11e1-be2b-00144feabdc0.html?ftcamp=rss; Matt Warman, *Government Minister Ed Vaizey Questions EU "Right to Be Forgotten" Regulations*, TELEGRAPH (Feb. 28, 2012), http://www.telegraph.co.uk/technology/news/9109669/Government-minister-Ed-Vaizey-questions-EU-right-to-be-forgotten-regulations.html; Jane Yakowitz, *More Bad Ideas from the E.U.*, FORBES (Jan. 25, 2012), http://www.forbes.com/sites/kashmirhill/2012/01/25/more-bad-ideas-from-the-e-u/. A joint statement of Reding and U.S. Commerce Secretary John Bryson emphasized the desirability for business of "one-stop shop" and technological interoperability in data protection regulation. Press Release of European Union, EU-U.S. joint Statement on Data Protection (Mar. 19, 2012), http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/192.

45. *See also* Francoise Gilbert, *Proposed EU Data Protection Regulation: The Good, the Bad, and the Unknown*, 15 J. INTERNET L. 1 (2012); Somini Sengupta, *Europe Weighs Tough Law on Online Privacy*, N.Y. TIMES (Jan. 23, 2012), http://www.nytimes.com/2012/01/24/technology/europe-weighs-a-tough-law-on-online-pri?_r=1.

46. Directive, *supra* note 2, art. 7(a). DPD referred to "explicit consent," but only in perambulatory language. *Id.* pmbl. ¶ 33.

47. *See also* Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/big-data (comparing opt-in and opt-out privacy defaults).

48. Proposal, *supra* note 1, pmbl. ¶ 25.

Fn50 cannot suffice.[49] Moreover, consent must be "freely given."[50] Even explicit consent cannot suffice when data subject and controller are in Fn51 an imbalanced power relationship, such as employee-employer.[51] Finally, the proposed regulation clarified a data subject's "right to Fn52 withdraw his or her consent at any time,"[52] which terminates consent-based authority to continue data processing and authorizes the right to be forgotten, *infra.*

B. *Transparency*

The proposal encourages transparency in data controllers vis-à-vis Fn54 data subjects.[53] Controllers must employ "clear and plain language"[54] in informing subjects of all aspects of data processing policy, including Fn55 the purposes and time frame of the processing[55] and the subject's rights, including access, objection, rectification, erasure, and com- Fn56 plaint to data protection or judicial authorities.[56]

The overarching language requirement marks a particular departure from the DPD. The preamble to the proposal emphasizes that the new standard has "particular relevan[ce]" in "online advertising," where data subjects can be overwhelmed by "the proliferation of actors and Fn57 the technological complexity of practice."[57] When children are the subjects of data collection, the "clear and plain" standard requires that Fn58 language be comprehensible to the child.[58] The weaker transparency standards of the DPD required only identification of data processors and any data recipients, and disclosure of the "purpose of the processing," "whether replies to the questions are obligatory or voluntary," and Fn59 merely "the existence" of rights of access and correction.[59]

---

49. *Id.*

50. *Id.* pmbl. ¶ 25, art. 4(8).

51. *Id.* pmbl. ¶ 34, art. 7(4). The controller wishing to process data despite imbalance therefore must seek an alternative authority to consent, such as contract, legal necessity, or a vital interest of the data subject, per *id.* art. 6.

52. *Id.* art. 7(3).

53. *Id.* pmbl. ¶¶ 30, 38, 46, 48, 77.

54. *Id.* pmbl. ¶ 48, art. 11.

55. *Id.* art. 5.

56. *Id.* pmbl. ¶ 48.

57. Proposal, *supra* note 1, pmbl. ¶ 46.

58. *Id.*

59. Directive, *supra* note 2, art. 10.

C. *Right to be Forgotten*

The DPD contemplated a data subject's right of erasure upon non-compliant data practices, as well as notice to third parties to whom erroneous or otherwise non-compliant data disseminations had occurred,[60] but the proposed regulation goes farther. The proposed regulation makes clear that termination of the time frame or purpose of the data processing, or of the necessity for the data to the purpose triggers the right to be forgotten.[61] The subject's revocation of consent, further clarified by the proposed regulation, *supra*, also triggers the right to be forgotten.[62] The duties of data controllers upon the right to be forgotten also seem to go beyond mere notice with respect to third parties. Controllers must "take all reasonable steps, including technical measures . . . to inform third parties . . . that a data subject requests them to erase any links to, or copy or replication of that personal data."[63] A data controller is on the hook for (previously?) "authorised" third-party publications.[64] This latter provision leaves unclear the potential liability of a controller for the conduct of downstream data consumers and re-publishers when the right to be forgotten has been invoked.[65]

D. *International Data Transfers*

Salient in the Internet era when data can be disseminated worldwide virtually instantaneously, the proposed regulation adds substantial procedural flesh to the DPD's constraint on the transfer of information across international borders. The European Commission (EC) is empowered to assess the data protection regimes of non-EU countries and international organizations to find them "adequate" or not.[66] Transfers to authorities deemed inadequate are prohibited,[67] and transfers to authorities in the absence of an EC determination are constrained by complex safeguards.[68]

---

60. *Id.*, art. 12.

61. Proposal, *supra* note 1, pmbl. ¶ 53, art. 17.

62. *Id.* ¶ 53, art. 17(b). Processing may continue upon a legitimate basis alternative to subject consent, such as "historical, statistical, and scientific research purposes." *Id.* arts. 17(3)(c), 83.

63. *Id.* art. 17(2).

64. *Id.*

65. Neil Hodge, *The EU: Privacy by Default*, 8 IN-HOUSE PERSP. 19 (2012).

66. Proposal, *supra* note 1, art. 41. *Compare id., with* Directive, *supra* note 2, art. 25.

67. Proposal, *supra* note 1, art. 41(6).

68. *Id.* arts. 42-44.

E. *European Data Protection Board*

The proposed regulation would create a European Data Protection Board, comprised of national data protection supervisors.[69] The board's principal role is to ensure uniformity in the implementation and interpretation of the regulation in EU Member States,[70] where national data protection authorities retain front-line responsibility for data protection oversight and enforcement.[71]

F. *Sanctions*

The DPD authorized EU Member States to impose civil liability and administrative sanctions.[72] The proposed regulation adds detail,[73] including a specified fine of up to two percent of a business's annual worldwide turnover for negligent or intentional non-compliance with data processing restrictions.[74]

Businesses based outside the EU that wish to comply with the regulation naturally will face a range of new costs. Businesses even within the EU naturally are concerned that any cost savings from harmonization will be wiped out by additional burdens under the proposed regulation.[75] For example, obtaining explicit consent initially and then again upon changes in data uses arguably will require costly recurring interactions between data controllers and subjects. More detailed reporting requirements in the proposed regulation, especially in the procedures in case of security breach, plus management of consents, revocations, erasures, etc. arguably will consume additional human resources. And the right to be forgotten triggers its uncertain range of required actions, along with possible pain of liability, especially with regard to third-party data partners.

It is furthermore unclear that a uniform regulation will eliminate the burdens of compliance with multiple state regimes. The continuing decentralization of enforcement mechanisms in national data protection and judicial systems will lead inevitably to variations in interpretation; especially insofar as terms of the new regulation remain fuzzy. The

---

69. *Id.* art. 64.

70. *Id.* ch. VII, § 3.

71. *Id.* chs. VI-VII.

72. Directive, *supra* note 2, arts. 22-24.

73. *See* Proposal, *supra* note 1, arts. 77-79.

74. *Id.* art. 79(6).

75. *See, e.g.*, Pignal & Palmer, *supra* note 44 (explaining likelihood that businesses will "lobby heavily" to reduce costly new burdens while preserving harmonization of standards).

new oversight board will be tested to keep variability under control.

Finally there is a big-picture debate—and in this respect the United States gets into the mix in a big way—over whether regulation on the whole does more to facilitate or to stifle business innovation. An Amazon online bookstore or TiVo television delivery system might argue that it never would have developed effective algorithms for user-tailored recommendations for books and programming without a free hand to record, study, and re-deploy information about users' identities and preferences. The businesses assert that in the face of overbearing and enormously costly regulation, they simply will not invest in sophisticated data processing, and the next generation of
Fn76 "your recommendations" technology will never come to be.[76] Regulation proponents retort that if consumers lack confidence that their personal information will be managed with responsibility and account-
Fn77 ability, they will not provide information to business to begin with.[77]

The flashpoint of trans-Atlantic controversy, importing the weight of constitutional and human rights arguments, arises from the right to be
Fn78 forgotten.[78] The right to be forgotten is an expression of an extant
Fn79 concept under the umbrella of rights of personality in Europe.[79] The
Fn80 term in French is *le droit à l'oubli*, or "right to oblivion,"[80] which is at the same time enlightening and confusing. On the one hand, the concept smacks of a grand and absolute statement about a person's right to
Fn81 control her or his own destiny in all of time and space.[81] But what that could possibly mean in terms of earthbound law and policy is not so easy to articulate. Social contract theory postulates that no person living in civilized society is wholly the master of her or his own ship. So whether the approach is American or European, the right to be forgotten has to be about line-drawing.

The row on the American side over the right to be forgotten focuses

---

76. *See, e.g.*, Sengupta, *supra* note 45.

77. *See, e.g.*, *id.*

78. *E.g.*, Franz Werro, *The Right to Inform v. The Right to Be Forgotten: A Transatlantic Clash*, *in* HAFTUNGSRECHT IM DRITTEN MILLENNIUM—LIABILITY IN THE THIRD MILLENNIUM (Aurelia Colombi Ciacchi et al. eds., 2009), *available at* http://ssrn.com/abstract=1401357.

79. European cultural sensitivity with respect to privacy is often attributed to Nazi use of government records to identify Jews. *E.g.*, *Private Data*, *supra* note 39.

80. *See* Jean-Christophe Duton & Virginie Becht, *Le Droit à l'Oubli Numérique: Un Vide Juridique?*, LE JOURNAL DU NET (Feb. 24, 2010, updated Mar. 1, 2010), http://www.journaldunet.com/ebusiness/expert/45246/le-droit-a-l-oubli-numerique--un-vide-juridique.shtml (explicating French law); Fleischer, *supra* note 21.

81. *See generally* VIKTOR MAYER-SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009).

on the potential for censorship, as explained in Part I, in the context of *Alfacs Vacances v. Google Spain* and the Argentine celebrity cases. But the risk of censorship can be articulated with more urgent implication than in cases of a crippled campground or sexy celebrity photos. As suggested in connection with the Argentine cases, public officials often wish to be distanced from embarrassing associations that might turn up in Google results.[82] *Slate* suggested that a Nazi war criminal might take advantage of data protection to avoid exposure by investigative reporters.[83] They might regard the associations as irrelevant to public service and therefore within the scope of personal privacy and data protection. A segment of the electorate might nevertheless regard the associations as relevant. Where public officials are concerned, the American legal system tends to err prophylactically on the side of public disclosure, while the European balance of private and public is not so predictable.[84]

The proposed regulation has safeguards to preserve freedom of expression. The regulation instructs that it should be construed and supplemented by national legislation to exempt[85] "journalistic purposes" and "artistic and literary expression" from the purview of data processing constraints "in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information,"[86] that is, according to the preamble, "balancing these fundamental rights."[87] The instruction "should apply in particular to processing of personal data in the audiovisual field and in news archives and press libraries."[88] The scope of exception should be "broad[]," to encompass "disclosure of public

82. The dispute between U.S. Republican presidential candidate Rick Santorum and Google is renowned in this regard and raises compelling problems in tort, media, and technology law. *E.g.*, Jamie Lund, *Managing Your Online Identity*, 11 J. INTERNET L. 3, 5 (2012).

83. *The Problem with Europe's Strict Privacy Laws*, SLATE (Mar. 14, 2012), http://www.slate.com/blogs/future_tense/2012/03/14/_right_to_be_forgotten_heinrich_boere_and_the_eu_privacy_laws_.html (describing German criminal privacy prosecution and acquittal of Dutch reporters who secretly videotaped confession of elderly SS commando).

84. *See generally* Scott J. Shackelford, *Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures*, 49 AM. BUS. L.J. 125, 128-207 (2012) (comparing the United States, United Kingdom, France, and Germany, and observing "increasingly divergent" U.S. and European norms).

85. The language of exemption is "exemptions [and] derogations." Proposal, *supra* note 1, pmbl. ¶ 121, art. 80(1).

86. *Id.* pmbl. ¶ 121, art. 80(1) (in operative language, "in order to reconcile the right to protection of personal data with the rules governing freedom of expression").

87. *Id.* pmbl. ¶ 121.

88. *Id.*

information, opinions or ideas, irrespective of the medium which is used to transmit them," and irrespective of profit or non-profit motive.[89]

Journalistic, artistic, and literary exception should pertain, the proposed regulation further instructs, with respect to general principles, data subject rights, data processor conduct, international data transfer, data protection authorities, and consistency principles,[90] but not "other provisions."[91] By process of elimination, "other provisions" are liability and sanctions[92] and "specific data processing situations,"[93] the latter of which includes the operative language calling for journalist exception.[94] The "specific situations" chapter further contemplates specialized national legislation to manage healthcare data,[95] employment data,[96] secrecy in the professions,[97] religious activities,[98] and "historical, statistical and scientific research papers."[99] The last category at first blush would be the broadest, but it is limited by its own terms, which carry over the minimalism principle[100] and require consent, overriding research necessity, or subject waiver through publication before personal data may be processed.[101]

There is profound disagreement over whether these safeguards suffice to protect freedom of expression. Professor Jane Kirtley, then executive director of the Reporters Committee for Freedom of the Press, rejected a journalistic exception as adequate to protect free expression in the debate over the DPD,[102] and arguments from that time are still salient. Kirtley pointed out that exception invites government to define journalism (or art or literature), a principle anathema in the United States for its resemblance to colonial press licensing.[103] In the U.S. Supreme Court's balkanized approach to constitutional

89. *Id.*
90. *Id.* pmbl. ¶ 121, art. 80(1) (citing chs. II-VII).
91. *Id.*
92. *Id.* ch. VIII.
93. *Id.* ch. IX.
94. *Id.* art. 80(1). National laws in this vein are to be reported to the EC. *Id.* art. 80(2).
95. *Id.* art. 81.
96. *Id.* art. 82.
97. *Id.* art. 84.
98. *Id.* art. 85.
99. *Id.* art. 83.
100. *Id.* art. 83(2); *see also* Tene & Polonetsky, *supra* note 47 (discussing minimization).
101. Proposal, *supra* note 1, art. 83(3).
102. *See* Kirtley, *supra* note 36, at 646-49.
103. *See id.*

Fn104 media law, the press—which so far includes the Internet[104]—may not be subordinated to a regulatory regime in the same manner as the
Fn105 telecommunications industry.[105] Professor Jeffrey Rosen has vigorously raised alarm over the proposed regulation, pointing to the Spanish and Argentine cases against Google, as well as a case in Germany of convicted murderers seeking to erase their past misdeeds from Wikipe-
Fn106 dia in consonance with German law promoting rehabilitation.[106]

In contrast, John Hendel penned an article for *The Atlantic* in which
Fn107 he argued that handwringing over free expression was over-reactive.[107] Hendel quoted Commissioner Reding from a speech on January 22, 2012, in which she purported to limit the scope of the proposed
Fn108 regulation to "'personal data [people] have given out themselves'"[108]—though no such limitation is to be found in the proposed regulation as
Fn109 published on January 25, 2012.[109] Hendel acknowledged a cultural
Fn110 difference between American and European approaches to privacy.[110] But pointing to free expression-friendly language from Reding that

104. *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 868-70 (1997).

105. *See, e.g.*, Se. Promotions, Ltd. v. Conrad, 420 U.S. 546, 557-58 (1975).

106. Rosen, *Right to be Forgotten*, *supra* note 33, at 88 (citing John Schwartz, *Two German Killers Demanding Anonymity Sue Wikipedia's Parent*, N.Y. TIMES (Nov. 12, 2009), http://www.nytimes.com/2009/11/13/us/13wiki.html). Rehabilitation-oriented limitations on the freedom of expression are not uncommon in the world, but in the United States any limit purporting to reach beyond the government's own disseminations is an utter non-started under the rule against prior restraints. *See generally* Clay Calvert & Jerry Bruno, *When Cleansing Criminal History Clashes with the First Amendment and Online Journalism: Are Expungement Statutes Irrelevant in the Digital Age?*, 19 COMMLAW CONSPECTUS 123 (2010); Logan Danielle Wayne, Comment, *The Data-Broker Threat: Proposing Federal Legislation to Protect Post-Expungement Privacy*, 102 J. CRIM. L. & CRIMINOLOGY 253 (2012).

107. John Hendel, *Why Journalists Shouldn't Fear Europe's "Right to be Forgotten,"* ATLANTIC (Jan. 2012) [hereinafter Hendel, *Why Journalists*], http://www.theatlantic.com/technology/archive/2012/01/why-journalists-shouldnt-fear-europesright-to-be-forgotten/251955/; *see also* John Hendel, *In Europe, a Right to Be Forgotten Trumps the Memory of the Internet*, ATLANTIC (Feb. 2011) [hereinafter Hendel, *In Europe*], http://www.theatlantic.com/technology/print/2011/02/in-europe-a-right-to-be-forgotten-trumps-the-memory-of-the-internet/70643/; David Lindsay, *EU Privacy Laws: The "Right to Be Forgotten" is Not Censorship*, CRIKEY (Feb. 21, 2012), http://www.crikey.com.au/2012/02/21/eu-privacy-laws-the-right-to-be-forgotten-is-not-censorship/ (urging Australia to follow European example).

108. Hendel, *Why Journalists*, *supra* note 107 (quoting Viviane Reding, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Address at Innovation Conference Digital, Life, Design 5 (Jan. 22, 2012), http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF).

109. Rosen, *Right to be Forgotten*, *supra* note 33, at 89.

110. Hendel, *Why Journalists*, *supra* note 107.

Fn111 mirrored the admonitions of the proposed regulation,[111] Hendel predicted that any reforms driven from the European side would shake up only businesses that are presently allowed to profit from invasive
Fn112 data mining.[112]

Certainly a robust execution of the exemption language in the proposed regulation would ward off fears of chilling effects and censorship. But even could such efforts be promised, the proposed regulation would leave gaps that advocates on the United States' side would find intolerable. For example, in leaving the matter of exemption substantially to national legislation for implementation, there is no guarantee to media and creative producers of a uniformity of interpretation like what the proposed regulation purports to ensure for commercial interests. Even interpreting journalism broadly as the proposed regulation admonishes, national legislatures will differ over the worthiness of
Fn114 an "activist blogger,"[113] a news aggregator,[114] a reality television pro-
Fn116 gram,[115] a parody news program,[116] and a piece of performance art
Fn117 with an ideological message.[117] Awaiting uniformity through EC oversight and counting on the European Court of Human Rights to serve as backstop leaves a great deal to chance in the near term. Moreover, even when a human rights analysis occurs, the preamble to the proposed
Fn118 regulation revealingly refers to a *balance* of fundamental rights.[118] Out of the gate, balancing epitomizes the European approach embodied,

---

111. *Id.* (quoting Reding, *supra* note 108, at 5 ("It is clear that the right to be forgotten cannot amount to a right of the total erasure of history. Neither must the right to be forgotten take precedence over freedom of expression or freedom of the media.")).

112. *Id.*

113. ACTIVIST BLOGGER: THE JOSH WOLF STORY (Donna Lee 2008). *See generally* Sunny Woan, *The Blogosphere: Past, Present, and Future. Preserving the Unfettered Development of Alternative Journalism*, 44 CAL. W. L. REV. 477, 494-95 (2008).

114. *See generally* Anjali Dalal, *Protecting Hyperlinks and Preserving First Amendment Value on the Internet*, 13 U. PA. J. CONST. L. 1017, 1039 (2011).

115. *See generally* Francis X. Dehn, *Reality TV and the New Reality of Media Law*, 23 DEL. LAW. 14, 15 (2006).

116. *Cf.* Clifford A. Jones, *The Stephen Colbert Problem: The Media Exemption for Corporate Political Advocacy and the "Hail to the Cheese Stephen Colbert Nacho Cheese Doritos® 2008 Presidential Campaign Coverage,"* 19 U. FLA. J.L. & PUB. POL'Y 295, 305-07 (2008). *See generally* Roderick Spencer, *Fake News is the Real News*, HUFFINGTON POST (Sept. 30, 2009), http://www.huffingtonpost.com/roderick-spencer/fake-news-is-the-real-new_b_305799.html, *cited in* Akilah N. Folami, *Freeing the Press from Editorial Discretion and Hegemony in Bona Fide News: Why the Revolution Must Be Televised*, 34 COLUM. J.L. & ARTS 367, 370 (2011).

117. *See, e.g.*, JUICE RAP NEWS, http://thejuicemedia.com/ (last visited July 27, 2012); *see also* THE GREGORY BROTHERS, http://www.thegregorybrothers.com/ (last visited July 29, 2012).

118. Proposal, *supra* note 1, pmbl. ¶ 121.

for example, in the limitations provision of the free expression clause
Fn119 of the European Convention on Human Rights.[119] From the perspective of the United States, where the First Amendment at least purports to be an absolute command, balancing is prone to insufferable fuzziness in close cases, all the more when the mix of decision-makers includes legislators and executive regulators besides precedent-bound judges.

III. AMERICA'S TARNISHING ABSOLUTISM

Fn120 Law in the United States is famously favorable toward free speech.[120] This predisposition has been present since the First Congress enshrined expressive and religious liberties in the First Amendment. But the First Amendment got a game-changing boost in the civil rights era, especially in the areas of prior restraint, criminal defense, and tort. Nowhere is this radical transformation better exhibited than in the
Fn121 defamation doctrine of *New York Times Co. v. Sullivan*.[121] And upon the
Fn122 shoulders of the historic rule against prior restraint[122] and *Sullivan*'s
Fn123 exaltation of truthful expression,[123] the key corollary emerged that almost never will the First Amendment countenance penalty for the
Fn124 publication of truthful information lawfully obtained.[124] Like the rule of *Sullivan*, the truth rule developed through a series of cases, but it
Fn125 may be referenced inclusively as the rule of *Smith v. Daily Mail*.[125]

To media defenders, the rules of *Sullivan* and *Daily Mail* are holy

---

119. Convention for the Protection of Human Rights and Fundamental Freedoms art. 10(2), Nov. 4, 1950, 213 U.N.T.S. 221.

120. What I here describe as a free speech imperative, or a bent toward free speech absolutism, Professor George Werro perhaps less kindly but no less accurately describes as a "'fetishization'" of the First Amendment. *See* Hendel, *In Europe*, *supra* note 107 (quoting Werro).

121. New York Times Co. v. Sullivan, 376 U.S. 254 (1964); *see also* Kyu Ho Youm, *"Actual Malice" in U.S. Defamation Law: The Minority of One Doctrine in the World?*, 4 J. INT'L MEDIA & ENT. L. 1, 2 n.6 (2012) (citing RODNEY A. SMOLLA, THE LAW OF DEFAMATION § 2.1, at 2-3 (2d ed. 2011)).

122. *See generally* John Calvin Jeffries, Jr., *Rethinking Prior Restraint*, 92 YALE L.J. 409, 412-19 (1983); David McCarthy, *Equity Will Not Enjoin Libel: Was an "Iron Law" Saved by the Death of Johnnie Cochran?*, 21 DUPAGE CNTY. B. ASS'N BRIEF 8, 9-14 (2009).

123. *See* 376 U.S. at 271 ("Authoritative interpretations of the First Amendment guarantees have consistently refused to recognize an exception for any test of truth—whether administered by judges, juries, or administrative officials—and especially one that puts the burden of proving truth on the speaker."); *cf.* United States v. Alvarez, 132 S. Ct. 2537 (2012) (striking prophylactically criminalization of falsity in "Stolen Valor Act," 8 U.S.C. § 704(b)-(c) (2006)).

124. *E.g.*, Florida Star v. B.J.F., 491 U.S. 524, 541 (1989) ("We hold only that where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order.").

125. Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979).

Fn126 writ.[126] But time has taken a toll. *Sullivan* and *Daily Mail* moved the law toward a free speech absolutism that seemed attractive when civil rights passions burned brightly, but now seems less so as civil rights priorities wane and give way to Internet-age worries over reputation, security, and privacy.

A. *The Rule of* Sullivan

> *"These newspaper reporters . . . ever since Sullivan versus New York Times . . . have got a license to lie."*
>
> —Edward Bennett Williams

Fn127 In *Sullivan*[127] and its progeny, the U.S. Supreme Court constitutionalized and thereby federalized much of the state common law of defamation. The *Sullivan* rule, or really rules, are triggered by the Fn128 public-official or public-figure status of the plaintiff,[128] and triggered in a more limited fashion by public interest in the subject matter of the Fn129 expression at issue.[129] *Sullivan* demands that the defendant prove Fn130 truth, rather than that the plaintiff prove falsity.[130] Certain common law components of black-letter defamation become constitutionally compulsory, such as the "of and concerning" test of the identification Fn131 element.[131] Many defenses against defamation, such as the fair com-Fn132 ment privilege, similarly acquire a constitutional dimension.[132] Bur-Fn134 dens of proof[133] and standards of appellate review[134] are constitutionalized and toughened. And perhaps most famously of the *Sullivan* rules, the minimum requisite standard of fault is elevated to "actual malice," meaning actual knowledge of falsity or reckless disregard as to truth or

---

126. *See* Brief of Amici Curiae Washington Post et al. at 2-10, Pom Wonderful, LLC v. ALM Media Props. LLC, No. 10-CV-904 (D.C. Cir. July 30, 2010), *available at* http://www.rcfp.org/sites/default/files/20100730-amicusbriefinpomwonderfulvamericanlawyermedia.pdf; Brief for Media Entities and Organizations as Amici Curiae Supporting Respondents at 8-13, Bartnicki v. Vopper, 532 U.S. 514 (2001) (Nos. 99-1687, 99-1728), 2000 WL 1617961.

127. New York Times Co. v. Sullivan, 376 U.S. 254, 254 (1964).

128. *See id.* at 267; Gertz v. Robert Welch, Inc., 418 U.S. 323, 342-43 (1974).

129. *See, e.g.*, Philadelphia Newspapers, Inc. v. Hepps, 475 U.S. 767 (1986); *see also* Time, Inc. v. Hill, 385 U.S. 374 (1967) (false light invasion of privacy).

130. *Sullivan*, 376 U.S. at 267.

131. *See id.* at 288.

132. *E.g.*, Richard J. Peltz, *Fifteen Minutes of Infamy: Privileged Reporting and the Problem of Perpetual Reputational Harm*, 34 OHIO N.U. L. REV. 717, 722-25 (2008).

133. *See Sullivan*, 376 U.S. at 285-86 ("convincing clarity" as to actual malice).

134. *See id.* at 284-85.

Fn135 falsity.[135] The knowledge standard charges plaintiffs to prove what was in the mind of the defendant, and the recklessness standard, more than
Fn136 usual tort recklessness, practically requires a smoking gun.[136]

The *Sullivan* doctrine utterly transformed the relationship between
Fn137 media and public life in the United States.[137] Litigation often turns on the squishy definition of public official or public figure, because once *Sullivan* applies, the constitutional constraints are damning for plain-
Fn139 tiffs.[138] Wins on actual malice are extraordinarily rare.[139] Cases overwhelmingly resolve upon a defense motion for dismissal or summary
Fn140 judgment.[140] To avoid subversion of *Sullivan*, the U.S. Supreme Court
Fn141 extended its reach into infliction of emotional distress[141] and false light
Fn142 invasion of privacy.[142] No one doubts that *Sullivan* results in meritorious cases not being heard and injured plaintiffs denied compensation;
Fn143 the rule is unabashedly prophylactic in its consecration of free speech.[143]

Avoiding subversion of *Sullivan* through false light and emotional distress claims did not require a great leap of logic. False light already requires that a plaintiff prove falsity, and otherwise so resembles
Fn144 defamation that some jurisdictions have rejected it as duplicative.[144] Infliction of emotional distress in the absence of physical injury requires some constitutional safeguard lest lampooning political cartoon-
Fn145 ists be hauled into court.[145]

But enthusiasm for *Sullivan* beyond these contexts might be running thin. Extension of the doctrine to other torts is not so straightforward, especially when the heart of the matter is truth. In invasion-of-privacy-by-disclosure cases, unlike in defamation cases, injury results from the very truth of the matter disclosed. Arguably, as an ideal, there can or

---

135. *Id.* at 279-80; *see also* Youm, *supra* note 121, at 2.

136. *See, e.g.*, Harte-Hanks Commc'ns., Inc. v. Connaughton, 491 U.S. 657, 667-68, 685-86 (1989); St. Amant v. Thompson, 390 U.S. 727, 732-33 (1968).

137. *E.g.*, Youm, *supra* note 121, at 4-5.

138. *See, e.g.*, Kelsey Beltramea, *Public Figure Hurdle Remains High*, 23 STUDENT PRESS L. CTR. REP. 27 (2008), *available at* http://www.splc.org/news/report_detail.asp?id=1447&edition=46.

139. *See, e.g.*, Christopher P. Guzelian, *True and False Speech*, 51 B.C. L. REV. 669, 679 (2010) (describing actual malice as "nearly insurmountable protection from suits by public figures").

140. *See, e.g.*, Susan M. Giles, *Taking First Amendment Procedure Seriously: An Analysis of Process in Libel Litigation*, 58 OHIO ST. L.J. 1753, 1770-71 (1998).

141. *See* Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 53-56 (1988).

142. *See* Time, Inc. v. Hill, 385 U.S. 374, 386-91 (1967).

143. *See generally* Guzelian, *supra* note 139, at 678-80.

144. *See, e.g.*, Sandra F. Chance & Christina M. Locke, *When Even the Truth Isn't Good Enough: Judicial Inconsistency in False Light Cases Threatens Free Speech*, 9 FIRST AMEND. L. REV. 546, 557-60 (2011); *see also* 62A AM. JUR. 2D *Privacy* § 126 (2012).

145. *See Hustler Magazine*, 485 U.S. at 54-55.

Fn146 should be no liability for truthful statements.[146] The no-liability view is akin to the absolutist approach a minority of the *Sullivan* Court would have taken in simply immunizing media defendants in public-official Fn147 defamation cases.[147] The approach failed to win the day in *Sullivan*, and invasion of privacy by disclosure today has settled for balancing Fn148 free speech and privacy.[148]

It is not clear, then, what exactly what effect *Sullivan* has in sum in a public-figure disclosure case. Elevating the fault standard as to the private character of the information disclosed, akin to fault as to falsity, would preclude recovery for merely negligent disclosure. The burden of proof similarly may be elevated to clear and convincing evidence of fault, and the standard of review may be intensified. Are these measures Fn149 sufficiently protective of free speech in a *Sullivan* vein?[149] Where would this approach leave the extra-marital affair of a former presidential Fn150 candidate, such as John Edwards?[150]

In practice, the problem is averted almost invariably by the common law defense of public interest, or newsworthiness, which might be constitutionally compulsory. Professor David Elder observed that courts "uniformly" regard disclosures demonstrative of "fitness for office" as Fn151 matters of public interest, therefore privileged.[151] For a presidential candidate there probably is no private sphere. But finding the line between public and private becomes more difficult quickly as analysis descends the ranks and shifts from public officials to non-governmen- Fn152 tal public figures.[152] In an oft-cited case, an elected student government officer's transsexuality was not regarded as reflective of public

---

146. *See generally* Comment, *An Accommodation of Privacy Interests and First Amendment Rights in Public Disclosure Cases*, 124 U. PA. L. REV. 1385, 1407-17 (1976).

147. *See* New York Times Co. v. Sullivan, 376 U.S. 254, 293-97 (1964), 376 U.S. at 293-97 (Black, J., concurring, joined by Douglas, J.); *id.* at 297-305 (Goldberg, J., concurring, joined by Douglas, J.).

148. *See, e.g.*, 62A AM. JUR. 2D *Privacy* § 94 (2012); *see also* DAVID A. ELDER, PRIVACY TORTS §§ 3:7 (fault), 3:16 (public figures) (2012) (addressing fault requirement).

149. *See, e.g.*, J. THOMAS MCCARTHY, 1 RIGHTS OF PUBLICITY AND PRIVACY § 5.74 (2d ed. 2012) (discussing rejection of disclosure tort in part on First Amendment grounds in Hall v. Post, 372 S.E.2d 711 (N.C. 1988)).

150. *See, e.g.*, *Edwards Affair: Was Media Part of a "Conspiracy of Silence"?*, CNN (Aug. 10, 2008), http://articles.cnn.com/2008-08-10/politics/edwards.coverage_1_elizabeth-edwards-edwards-affair-edwards-scandal?_s=PM:POLITICS ("[M]ost major news networks took the stance that the rumors of an affair were not newsworthy.").

151. ELDER, *supra* note 148, § 3:16.

152. *See* Simon J. Frankel, Laura Brookover & Stephen Satterfield, *Famous for Fifteen People: Celebrity, Newsworthiness, and* Fraley v. Facebook, 64 STAN. L. REV. ONLINE 82 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/famous-fifteen-people.

Fn153 fitness.[153] Professor Elder described as "very questionable" a court ruling that disclosure of a medical malpractice plaintiff's AIDS infection "met the nexus requirement for the public figure-public interest
Fn154 privilege."[154]

The uneasy balance, then, between free expression and privacy is being hammered out over the fine, common law line of public inter-
Fn155 est.[155] The purview of courts on this question has always been uncomfortable for news media, for fear that judges will sit as "super-editors," prioritizing news values. Journalism ethicists since the yellow press have struggled to reconcile the public appetite for gossip and morbidity with the arguable paternalism of objective public-interest reporting. In these times of the 24/7 news cycle, vanishing print platforms, scarce investment in investigative reporting, and wildly popular talking-head cable stations that blur the line between news and opinion, courts are much less likely than they might have been in the Watergate era to defer to a mass media defendant's assessment of news value. Courts will continue to determine whether the public interest privilege pertains in privacy cases, but the resulting balance is malleable and likely to settle more along evolving mainstream norms than in inclination to anti-majoritarian-protective First Amendment absolutism.

Another family of civil wrongs not yet well reconciled with free expression can be found in the torts of interference with economic relations. Interference does not necessarily occur through otherwise protected free speech, but it can. This conflict came up when the Brown & Williamson tobacco company clashed with CBS's *60 Minutes* over whistle-blowing scientist Jeffrey Wigand. The story was told in the
Fn156 film, *The Insider*,[156] in which CBS news producer Lowell Bergman elicited an on-air interview with Wigand. Brown & Williamson threatened CBS with an interference suit if Wigand's statements violated a
Fn157 confidentiality contract with his former employer.[157] In a telling scene in the movie, in the offices of CBS News, CBS counsel Helen Caperelli (Gina Gershon) explained to the *60 Minutes* team that Brown &

---

153. *See* Diaz v. Oakland Tribune, Inc., 188 Cal. Rptr. 762 (Cal. Ct. App. 1983), *cited in* Frankel, Brookover, & Satterfield, *supra* note 152.

154. *See* ELDER, *supra* note 148, § 3:16 (discussing Lee v. Calhoun, 948 F.2d 1162 (10th Cir. 1991)).

155. *See* Frankel, Brookover, & Satterfield, *supra* note 152.

156. *See* THE INSIDER (Touchstone Pictures 1999). The screenplay drew on Marie Brenner, *The Man Who Knew Too Much*, VANITY FAIR (May 1996), *available at* http://www.vanityfair.com/magazine/archive/1996/05/wigand199605.

157. *See* INSIDER, *supra* note 156.

Williamson's case not only turned on the truth of Wigand's disclosures, but that greater truth would mean greater damages.[158] Bergman—who in real life was inculcated in the sanctity of journalistic truth spoken to power and in 1977 had co-founded the Center for Investigative Reporting[159]—muttered in retort, "Is this Alice in Wonderland?"[160]

Interference might have figured prominently in a high-profile case against Wikileaks,[161] had the matter ever come to hearing on the merits.[162] In 2008, Wikileaks published records that evidenced suspicious financial transactions in the Cayman Islands branch of the Swiss bank, Julius Baer.[163] Baer Bank quickly sought an injunction from a U.S. federal court in California, to shut down the Wikileaks domain "wikileaks.org."[164] Wikileaks did not appear, and upon a negotiated settlement with Wikileaks's co-defendant and California-based Internet service provider, the trial court entered a purportedly stipulated, permanent injunction.[165] Ultimately the court rescinded the injunction, citing both free expression and futility, after Wikileaks's website was mirrored around the world.[166]

Tortious interference in the United States generally requires that the tortfeasor "intentionally and improperly" interfered with performance on a contract or with prospective business relations.[167] Impropriety is key in the analysis and represents a built-in public policy test that accommodates the freedom of expression.[168] The *Restatement* lists a series of factors to consider in analyzing impropriety: (a) the nature of the actor's conduct (chief); (b) the actor's motive; (c) interests of the other with whom the actor interferes; (d) interests sought to be advanced by the actor; (e) social interests in protecting the freedom of

158. *See id.*

159. *See* CTR. FOR INVESTIGATIVE REPORTING, http://cironline.org/ (last visited July 28, 2012); *see also* LOWELL BERGMAN, http://journalism.berkeley.edu/faculty/bergman/ (last visited July 28, 2012).

160. INSIDER, *supra* note 156.

161. *See* Bank Julius Baer & Co. v. Wikileaks, 535 F. Supp. 2d 980 (N.D. Cal. 2008).

162. *See generally* Richard J. Peltz, *U.S. Business: Tort Liability for the Transnational Republisher of Leaked Corporate Secrets*, 1 AMITY J. MEDIA & COMM. STUD. 68, 71-73 (2011), *available at* http://ssrn.com/abstract=1947129.

163. *Id.* at 71.

164. *Id.*

165. *See* Bank Julius Baer & Co. v. Wikileaks, no. C-08-00824-JSW, 2008 WL 413737 (N.D. Cal. Feb. 13, 2008); Peltz, *supra* note 162, at 71.

166. *See Bank Julius Baer*, 535 F. Supp. 2d at 985-86; Peltz, *supra* note 162, at 71.

167. RESTATEMENT (SECOND) OF TORTS § 766 (interference with contract), § 766B (prospective relations) (1979).

168. *See, e.g.*, Peltz, *supra* note 162, at 72.

action of the actor and the contractual interests of the other; (f) proximity or remoteness of the actor's conduct to the interference; and
Fn169 (g) relations between the parties.[169] In the theory of the interference tort, the impropriety test patrols the line where plaintiff's business competitor crosses from legitimate market inducement to compensable civil wrong. The element therefore arguably has no application when a plaintiff and defendant—such as Wikileaks and Bank Julius Baer, or CBS and Brown & Williamson—collide over alleged interfer-
Fn170 ence with prospective economic advantage.[170] "But the case law does
Fn171 not seem to support that proposition."[171]

Thus in the final analysis, interference via impropriety is very much a soft question like that of public interest or newsworthiness in the privacy area. Again, such a balance might once have served to hold the line against imposition on a near-absolutist vision of free expression. But the presumption that journalists and not-for-profit publishers act in the public interest no longer holds sway. Wikileaks, for example, is
Fn172 avowedly absolutist in its approach to the freedom of information.[172] But Wikileaks stands on shaky ground when purporting to uphold the ideals of the Fourth Estate. In one of its mass releases of secret government records, Wikileaks disclosed the identity of Afghan infor-
Fn173 mants, arguably putting lives at risk.[173] The identification of wartime collaborators, placing them at risk, is comparable to the disclosure of wartime troop movements, the singularly undisputed exception to the
Fn174 rule against prior restraints.[174] On that basis, a powerful case can be made that Wikileaks does not advance the public interest, especially in the context of unproven allegations against a private foreign enterprise. Again amid the transformation of speaker-defendants in the media law landscape, courts will have a free hand to re-map the frontier of interference without deference to an absolutist philosophy of free expression.

The *Sullivan* doctrine suffers from other well-documented shortcomings. Anthony Lewis, in his seminal book on *New York Times Co. v.*

---

169. RESTATEMENT (SECOND) OF TORTS § 767 (1979).

170. *E.g.*, LOUIS ALTMAN & MALLA POLLACK, 1A CALLMAN ON UNFAIR COMPETITION, TRADEMARKS AND MONOPOLIES § 9:19 (4th ed. 2012).

171. *Id.* (citations omitted).

172. WIKIREBELS: THE DOCUMENTARY (SVT Sales & SVT Television 2010) (quoting Wikileaks spokesman Julian Assange).

173. *Id.*; Peltz, *supra* note 162, at 69-70.

174. New York Times Co. v. United States, 403 U.S. 713, 726 (1971) (Brennan, J., concurring) (citing Near v. Minnesota *ex rel.* Olson, 283 U.S. 697, 716 (1931)).

Sullivan, detailed the case extensively and placed it in its proper context in the civil rights movement.[175] And there is no doubt it was important. Lewis explained how even the mighty New York Times Co. could have been bankrupted by defamation torts turned into weapons to power southern resistance to desegregation and the civil rights movement.[176] The Supreme Court saw *Sullivan* not singularly as a defamation case, but as one front in a multi-front conflict over integration, voting rights, and the power vested in Congress to enforce the Fourteenth Amendment.[177] Accordingly, the Court per Justice Brennan construed the Constitution so as to arm civil rights advocates with the First Amendment as a shield.[178]

But in the latter chapters of his book, Lewis recognized the downside of constitutional lawmaking, namely its intransigence.[179] The Court might have over-corrected with *Sullivan*; the prophylaxis worked too well. In a system in which media defendants so plainly have the upper-hand against public figures and public officials, the usual behavioral economics of the tort system are perverted as to encourage carelessness, if not recklessness. Public servants suffer injury without compensation, and the hazard deters others from entering public life. Worse, there is no incentive for reform, because media have no reason to come to the table. Thus tort alternatives, such as alternative dispute resolution mechanisms or declaratory judgments of truth and falsity are complete non-starters. The Uniform Correction or Clarification of Defamation Act[180] has been a colossal flop, in part because media fear that rocking the boat in state legislatures will end in lost defensive ground.[181]

Sullivan's crushing blow to competing interests such as reputation has given pause to other nations, too. In a recent comparative survey, Professor Kyu Ho Youm asked whether the actual malice rule is in a "minority of one doctrine in the world."[182] Youm concluded that the actual malice doctrine has on the whole inspired world defamation law

---

175. ANTHONY LEWIS, MAKE NO LAW: THE *SULLIVAN* CASE AND THE FIRST AMENDMENT (1991).

176. *Id.* at 5-45.

177. *See id.* at 164-82.

178. *See id.* at 140-63.

179. *See id.* at 200-33.

180. UNIF. CORR. OR CLARIFICATION OF DEFAMATION ACT (1993). *See generally* Robert M. Ackerman, *Bringing Coherence to Defamation Law Through Uniform Legislation: The Search for an Elegant Solution*, 72 N.C. L. REV. 291 (1994).

181. *E.g.*, Wendy Tannenbaum, *Model Defamation Reform Slow to Catch On*, 27 THE NEWS MEDIA & THE L. 27 (2003), *available at* http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-spring-2003/model-defamation-reform-slo.

182. Youm, *supra* note 121, at 1.

to move toward the civil liberties position, and that positive impact should be the legacy of *Sullivan*.[183] At the same time, actual malice *per se* has been adopted "wholesale" only in the Philippines[184] and has been rejected in Commonwealth countries and elsewhere.[185] Representatively, Canada concluded that *Sullivan* put too much weight on the free expression side of what the Canadian Supreme Court decided should be a balance with a person's reputational rights.[186] However much good *Sullivan* has done as a beacon for human rights around the world, the procedural and substantive hurdles of the doctrine remain, every day, insurmountable obstacles to justice for genuinely injured persons in the United States. It can hardly take free expression advocates by surprise if the doctrine begins to show wear amid dramatic and not altogether inspiring changes in the nature, character, and conduct of the media business.

B. *The Rule of* Daily Mail

> *"[T]he first virtue is to restrain the tongue; he approaches nearest to gods who knows how to be silent, even though he is in the right."*
>
> —Marcus Porcius Cato, a.k.a. Cato the Censor

The rule of *Smith v. Daily Mail*[187] was never meant to be ironclad. The *Daily Mail* rule prohibits penalty for the dissemination of truthful information lawfully obtained.[188] The rule is a logical corollary of the rule against prior restraint, a fundamental principle derived from historic British common law, married with the veneration of truth as expressed through the *Sullivan* doctrine. The U.S. Supreme Court has described the *Daily Mail* rule as excepted by "a need to further a state interest of the highest order,"[189] but has not found a case it likes to demonstrate the exception.

Presumably the publication of wartime troop movements that com-

183. *Id.* at 26-30.

184. *Id.* at 6-7 (analyzing Borjal v. Court of Appeal, G.R. No. 126466, 301 S.C.R.A. 1 (Jan. 14, 1999) (Phil.)).

185. *E.g.*, Youm, *supra* note 121, at 28.

186. Hill v. Church of Scientology, [1995] 2 S.C.R. 1130 (Can.). *See generally* Thomas A. Hughes, *The Actual Malice Rule: Why Canada Rejected the American Approach to Libel*, 3 COMM. L. & POL'Y 55 (1998).

187. 443 U.S. 97 (1979).

188. *Id.* at 103.

189. *Id.*

prises the classic exception to the rule against prior restraints[190] would suffice as exception from *Daily Mail*. There seems to be little serious doubt that plaintiffs who are neither public officials nor public figures may win damages for invasion of privacy without constitutional impediment. But like in defamation, the judicial power in private-plaintiff tort cases usually does not sufficiently satisfy the state action doctrine to implicate constitutional constraints.[191] Similarly, constitutional considerations are rendered moot when free speech hurdles already have been surmounted, as when criminal penalties or civil fines penalize true speech delivered in violation of a valid time, place, and manner regulation,[192] or true representations of obscenity.[193]

An exception to the *Daily Mail* rule, though, might be found in circumstances well short of unveiled wartime secrets that endanger the nation. The 2004 criminal trial of professional basketball player Kobe Bryant—against whom charges later were dropped[194]—offers a recent and compelling case.[195] In the course of the prosecution, the court held a hearing pursuant to the Colorado rape shield law, which authorizes closed-door screening of victim testimony on intimate matters such as sexual history.[196] Then only testimony deemed relevant and essential to prosecution or defense may be introduced in open court.[197] Media followed *Bryant* intently, and the Eagle County, Colorado court staff had, to their credit, developed efficient means to maximize access to the proceeding by disseminating court records to media via e-mail. Unfortunately, in one daily mass dissemination, court officials inadvertently e-mailed the accuser's sealed testimony.[198]

The court quickly tried to unring the bell by ordering recipients to delete or destroy the mistakenly released records.[199] Violators would

---

190. New York Times Co. v. United States, 403 U.S. 713, 726 (1971) (Brennan, J., concurring) (citing Near v. Minnesota *ex rel.* Olson, 283 U.S. 697, 716 (1931)).

191. *See, e.g.*, Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 757-61 (1985).

192. *See, e.g.*, Ward v. Rock Against Racism, 491 U.S. 781, 790-91, 795 n.5 (1989).

193. *See, e.g.*, Alexander v. United States, 509 U.S. 544, 549-58 (1993).

194. *E.g.*, T.R. Reid, *Rape Case Against Bryant Is Dropped*, WASH. POST (Sept. 2, 2004), http://www.washingtonpost.com/wp-dyn/articles/A52941-2004Sep1.html.

195. People v. Bryant, 94 P.3d 624 (Colo. 2004) (en banc), *stay denied by* Associated Press v. Dist. Court for Fifth Judicial Dist. of Colo., 542 U.S. 1301 (2004) (Breyer, J.).

196. *See* COLO. REV. STAT. ANN. § 18-3-407(2) (West 2012); *Bryant*, 94 P.3d at 626. *See generally* Richard I. Haddad, *Shield or Sieve?:* People v. Bryant *and the Rape Shield Law in High-Profile Cases*, 39 COLUM. J.L. & SOC. PROBS. 185 (2005).

197. *See* COLO. REV. STAT. ANN. § 18-3-407 (West 2012).

198. *Bryant*, 94 P.3d at 626.

199. *Id.*

have been held in contempt.[200] Mainstream media were not keen to publish the confidential records, but objected powerfully to the prior restraint.[201] Nevertheless, the Colorado Supreme Court substantially upheld the trial court order. Though vacating the destruction order in favor of a narrower order against republication of only content deemed irrelevant and immaterial, the state high court acknowledged the prior restraint and concluded that it properly furthered victim privacy, incentives to report sexual assault, and prosecution and deterrence of sexual assault.[202]

Media were optimistic in a subsequent federal appeal to the moderately liberal Justice Stephen Breyer, sitting in circuit justice capacity.[203] They expected that he would recognize the *Daily Mail* problem and redress it unequivocally.[204] After all, the inadvertent release of the confidential court records very closely tracked fact patterns in previous *Daily Mail* cases. *Daily Mail* itself involved media ascertainment from police-band radio of the identity of a juvenile suspect.[205] In *Florida Star v. B.J.F.*, the Court had refused to permit criminal penalty for a newspaper that published, apparently unwittingly, the identity of a rape victim who was inadvertently named in a public police log.[206] In *Bartnicki v. Vopper*, a radio station came into possession of a recording of a politically sensitive telephone conversation, which was apparently obtained in violation of wiretap laws, but without media complicity.[207] There were grounds in *Bryant* to distinguish prior cases. The time between release and retraction of the confidential information was much shorter than in previous cases, so the state court prior restraint had issued before publication. And the records released in *Bryant* had been marked confidential, so no recipient could plead ignorance as to the private character of their content. But those grounds for distinction

200. *Id.*

201. *See* Reporters Committee for Freedom of the Press, Media Petitions Supreme Court over Prior Restraint in Bryant Case (June 28, 2004), http://www.rcfp.org/browse-media-law-resources/news/media-petitions-supreme-court-over-prior-restraint-bryant-case.

202. *Id.*

203. *See, e.g.*, Press Release, Reporters Committee for Freedom of the Press, Reporters Committee Urges Breyer to Intercede in Kobe Bryant Case (July 23, 2004), http://www.rcfp.org/reporters-committee-urges-breyer-intercede-kobe-bryant-case.

204. *See id.*

205. 443 U.S. at 99-100.

206. 491 U.S. 524, 526-28 (1989).

207. Bartnicki v. Vopper, 532 U.S. 514, 517-19 (2001). *See generally* Eric B. Easton, *Ten Years After:* Bartnicki v. Vopper *as a Laboratory for First Amendment Advocacy and Analysis*, 50 U. LOUISVILLE L. REV. 287 (2011).

were thin. In the Internet age, the time between release and publication could not be expected to matter much in future cases. And arguably the editors in *Florida Star* had at least constructive knowledge of the mistake, because state law forbade the release of the name of a sexual assault victim.[208]

Hopes that Justice Breyer would void the prior restraint were disappointed.[209] Justice Breyer noted that the trial court had made its relevancy determinations and predicted that they would "significantly change the circumstances."[210] Denying relief without prejudice, Justice Breyer opined that release of the disputed records was "imminent."[211] He therefore remanded the case for reconsideration in light of the developing record, managing to duck the prior restraint question.[212]

The outcome ostensibly represented a media victory, but free press advocates understood Breyer's faint ruling as a ruinous blow to the rule against prior restraints in the Tenth Circuit.[213] The implication of Breyer's reluctance to void categorically the prior restraint order was that, had push have come to shove, he might have been receptive to the argument that the accuser's privacy demanded an exception to the *Daily Mail* rule. The case seemed to fit squarely within the rule in that media had done nothing wrong. They were lawful recipients of the confidential records, just as WILK Radio had been in *Bartnicki*. The thin possible grounds for factual distinction of *Bryant* had not seemed to matter as much as the intimate nature of the content at issue. Thus, it seemed, Breyer signaled that for even the Court's left wing, historically the font of civil rights jurisprudence à la Justice Brennan in *Sullivan*, individual privacy might rate with survival of the republic in outweighing free speech.

C. *New Rule of American Privacy*

"What I dream of is an art of balance . . . ."
—Henri-Émile-Benoît Matisse

---

208. 532 U.S. at 528.

209. Associated Press v. Dist. Court for Fifth Judicial Dist. of Colo., 542 U.S. 1301, 1303-03 (2004) (Breyer, J.).

210. *Id.* at 1303.

211. *Id.* at 1304.

212. *Id.* ("[A] brief delay will permit the state courts to clarify, perhaps avoid, the controversy at issue here.").

213. *See, e.g.*, Kimberley Keyes, *Kobe's Legal Legacy*, 28 NEWS MEDIA & L. 17 (2004), *available at* http://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-fall-2004/kobes-legal-legacy (quoting media attorney Tom Kelley).

American free speech absolutism is giving way to ambivalence; meanwhile, ambivalence is increasingly expressed through approaches more akin to European-style rights balancing than to the free speech-imperative model of presumption and rebuttal. This balance appears in areas of law in which free speech never was enshrined as the paramount value, whether because it is balanced with an established and competing constitutional interest, as in the case of intellectual property, or because the courts rejected a free speech dimension in the equation, as in the case of the freedom of information.

Twentieth-century U.S. law saw the emergence of a balance between the free speech guarantee of the Constitution's First Amendment and the federal power of the Constitution's First Article to protect intellectual property. The balance is well expressed in the familiar fair use analysis of copyright law, which was codified in the 1976 Copyright Act,[214] and which, to some unknown measure, the First Amendment compels.[215] Because of the textual constitutional underpinning for both sides in a free speech-intellectual property dispute,[216] intellectual property is one of those exceptional areas in which free speech never was elevated to the presumptively paramount status it usually enjoys in American law.

Despite the uneasy truce between free speech and intellectual property, the Internet age has fostered a hard push against the free speech side of the equation. Early signs of this shift were contemporaneous with the 1995 DPD. The European Union followed up the DPD with a further directive, the Database Directive, which authorized *sui generis* European copyright protection for databases based on the labor of compilation, notwithstanding the creativity in data selection and arrangement that copyright usually requires.[217] Where the DPD sat uneasily with free speech and the *Daily Mail* rule, the Database Directive ran up against the U.S. Supreme Court's free speech-protective rejection of the "sweat of the brow" doctrine in U.S. copyright law. In *Feist Publications, Inc. v. Rural Telephone Service Co.*, the U.S. Supreme Court in 1990 had rejected the Copyright Act's purported protection for compilations that lacked "originality," or "some creative spark," a slim but necessary characteristic of copyrightable work, regardless of

214. 17 U.S.C. § 107 (2006).

215. *See, e.g.*, New Era Publ'ns Int'l, ApS v. Henry Holt & Co., 873 F.2d 576, 583-84 (2d Cir. 1989).

216. *Compare* U.S. CONST. art. I, § 8, cl. 8, *with* U.S. CONST. amend. I.

217. Directive 96/9/EC of the European Parliament and of the Council, 1996 O.J. (L 77) 20, 22.

the investment of labor in the project.[218]

The U.S. insistence on minimal creativity for copyright in data compilations is consistent with the TRIPs Agreement[219] and WIPO Copyright Treaty.[220] But both those instruments meant to liberalize database protection, so the Database Directive represents a further step in the same direction. Intellectual freedom advocates in the United States have been unwilling to follow suit. Librarians especially have protested copyright protection for data compilations. The American Library Association maintained (and maintains) that copyright in databases unduly restricts the global flow information and thereby diminishes world knowledge without the corresponding benefit posited by intellectual property protection, that is, without stimulating creation and innovation in database products.[221]

Despite the continuing vitality of the free speech position, U.S. congressional efforts to adopt EU-imitative database protection legislation have come in waves.[222] And U.S. courts have found that the slim creativity requirement sometimes can be made to protect databases.[223] Thus, in a Second Circuit case, the court found that vehicle valuation listings obtained copyrightable originality from authors' informed predictions of future value.[224]

American lawmakers meanwhile have found other means to shift the free speech-intellectual property balance to the latter's favor. Librarians also opposed the anti-circumvention provisions[225] of the Digital Millennium Copyright Act (DMCA),[226] which became effective in

---

218. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345-48 (1991).

219. Agreement on Trade-Related Aspects of Intellectual Property Rights art. 10(2), Apr.15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

220. WIPO Copyright Treaty art. 5, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 65.

221. *See* American Library Ass'n, Resolution in Opposition to "Sui Generis" Database Protection (Jan. 25, 2006), http://www.ala.org/offices/sites/ala.org.offices/files/content/wo/reference/colresolutions/PDFs/012506-CD20.6.pdf; American Library Ass'n, Database Protection, http://www.aallnet.org/main-menu/Advocacy/copyright/database.html (last visited July 28, 2012). *See generally* U.S. COPYRIGHT OFFICE, REPORT ON LEGAL PROTECTIONS FOR DATABASES (1997), *available at* http://www.copyright.gov/reports/dbase.html.

222. *See* American Ass'n of Law Libraries, Database Protection, http://www.aallnet.org/main-menu/Advocacy/copyright/database.html.

223. *See, e.g.*, CCC Info. Servs., Inc. v. Maclean Hunter Market Reports, Inc., 44 F.3d 61, 65-68 (2d Cir. 1994), *cited in* Jennifer Askanazi, et al., *The Future of Database Protection in U.S. Copyright Law*, 2001 Duke L. & Tech. Rev. 17 (2001).

224. *CCC Info Servs.*, 44 F.3d at 68.

225. 17 U.S.C. § 1201(a)(1) (2006).

226. Pub. L. No. 105-304, 112 Stat. 2860 (1998).

2000.[227] The circumvention of technological protection measures (TPMs) for intellectual property had been a means to exploit copyright's failure to protect mere facts and data, which intrinsically lacked creativity. The DMCA closed the loophole by imposing liability for conduct that is merely preliminary to infringement—and, libraries worried, might not be, despite purported statutory preservation of fair use.[228] The DMCA furthermore banned circumvention devices and prohibited the removal of copyright management information that facilitates TPM.[229] Reverse engineering TPM is permitted only to achieve interoperability with independently created systems.[230]

In a paradigmatic test of these provisions of the DMCA, the Motion Picture Association of America successfully stopped dissemination of TPM-decryption software for DVDs.[231] Free speech (and freedom of information) advocates again objected that the law put too much power in the hands of rights-holders as against lawful uses of copyrighted content, thereby shrinking the body of publicly accessible content. Amici opposing DMCA enforcement fretted in vain that liability for merely linking to decryption software, steps removed from and absent any evidence of actual copyright infringement, offended the First Amendment and impermissibly derogated from fair use.[232] In fairness, there is a troublesome dystopian undercurrent to a prohibition on the mere analysis of decryption software so as to protect corporate control of information.[233] But the DMCA, for better and worse, reflects the present balance in American law and represents a digression from an expansive, First Amendment-fueled fair use doctrine.

---

227. *E.g.*, American Library Ass'n, DMCA, http://www.ala.org/advocacy/copyright/dmca (last visited July 28, 2012); Electronic Frontier Found., DMCA https://www.eff.org/issues/dmca/ (last visited July 28. 2012). *See generally* Chilling Effects, Anticircumvention (DMCA) FAQs, http://www.chillingeffects.org/anticircumvention/faq.cgi (last visited June 19, 2012).

228. 17 U.S.C. § 1201(c) (2006); *see also id.* § 1201(d) (limited protection for non-profit libraries).

229. *Id.* § 1201(b). There is a distinction not worth belaboring between access and copy controls, which in practice may be one and the same. The DMCA allows the circumvention of copy controls only, but bans devices that would facilitate the circumvention of either. *Id.*

230. *Id.* § 1201(f).

231. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 458-60 (2d Cir. 2001).

232. Brief of Amici Curiae Am. Civil Liberties Union, et al., at 13-27, Universal City Studios, 273 F.3d 429 (No. 00-9185), *available at* https://w2.eff.org/IP/Video/MPAA_DVD_cases/20010126_ny_lib_amicus.pdf.

233. *See generally* Isaac Asimov, *The Dead Past*, ASTOUNDING SCI. FICTION, Apr. 1956, at 6, *cited in* Alex Kozinski, *The Dead Past*, 64 STAN. L. REV. ONLINE 117 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/dead-past.

Though for the time unsuccessful, recent bills in the U.S. Congress, such as the Stop Online Piracy Act[234] and the PROTECT Intellectual Property Act,[235] show that efforts to press against free speech in the online balance have not abated. The laws in essence would have authorized orders against legitimate Internet service providers to cut off access to websites identified as—or arguably merely accused of being—problem intellectual property infringers. Protests by major online information providers including Google and Wikipedia fomented worldwide opposition to the measures.[236] But proponents had strong allies among content creators in Hollywood.[237] And while the European Parliament was squeamish on the bills' particulars,[238] the resemblance of these proposals to the European "right to be forgotten" is striking: both would compel Internet service providers to "forget" content deemed to offend someone's rights, whether a copyright owner or an offended data subject.[239] Especially considering Hollywood's celebrated association with free speech and liberal causes,[240] even the unsuccessful support in the United States for Internet regulation of this kind signals a sea change from the free speech outlook of the civil rights era.

Meanwhile American ambivalence over free speech can be found in the curiously corollary area of freedom of information (FOI). FOI is corollary to the freedom of speech because without a right to receive information, there is nothing to speak about.[241] FOI is curious because only recently has it been recognized as a "right" or "freedom" in the

234. H.R. 3261, 112th Cong. (introduced Oct. 26, 2011). *See generally* Declan McCullagh, *How SOPA Would Affect You: FAQ*, CNET NEWS (Jan. 18, 2012), http://news.cnet.com/8301-31921_3-57329001-281/how-sopa-would-affect-you-faq/.

235. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, S. 968, 112th Cong. (2011).

236. *See* Julie Samuels & Mitch Stoltz, *The Internet at Its Best*, ELECTRONIC FRONTIER FOUNDATION (Jan. 18, 2012), https://www.eff.org/deeplinks/2012/01/internet-its-best.

237. *See, e.g.*, Press Release, Motion Picture Ass'n of Am. (Jan. 17, 2012), https://www.eff.org/sites/default/files/MPAA_statement.pdf.

238. *See* European Parliament Resolution on the EU-US Summit of 28 November 2011, EUR. PARL. DOC. RC-B7-0577/2011(2011), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0510&language=EN&ring=P7-RC-2011-0577.

239. Jerry Brito, *What Europe's "Right to Be Forgotten" Has in Common with SOPA*, TIME (Jan. 30, 2012), http://techland.time.com/2012/01/30/what-europes-right-to-be-forgotten-has-in-common-with-sopa/.

240. *See, e.g.*, Paul Blumenthal, *SOPA Forces Obama to Pick Sides Between Donors from Hollywood, Silicon Valley*, HUFFINGTON POST (Jan. 18, 2012), http://www.huffingtonpost.com/2012/01/18/sopa-obama-donors-hollywood-silicon-valley_n_1213159.html.

241. *See, e.g.*, Richmond Newspapers v. Virginia, 448 U.S. 555, 575-78 (1980).

human rights sphere.[242] The Universal Declaration of Human Rights (UDHR)[243] and the International Covenant on Civil and Political Rights[244] both assert a right to receive information, but are vague on the particulars, such as whether the information is coming from the state and whether the state has an obligation to provide information at all.[245]

FOI nevertheless has been recognized and advocated for. Organizations such as Article 19, which derives its name from the UDHR provision that references both expression and information, includes "the right to know" alongside "the right to speak" and "freedom of the press" as a principal mission objective.[246] Decisions in the European Court of Human Rights in 2009 and in the Inter-American Court of Human Rights in 2006 have recognized a human rights dimension to the freedom of information.[247] And in 2009, the Council of Europe opened for signature the Convention on Access to Official Documents.[248] FOI as right to know, more than mere right to receive what is made available, seems just now to be in its naissance as a fundamental human right.

The timing for these developments is less than ideal for FOI in the United States because it failed to fully exploit the growth opportunity of the civil rights era. Justice Potter Stewart famously wrote in 1975 that the Constitution "is neither a Freedom of Information Act nor an Official Secrets Act."[249] FOI squeaked through the civil rights movement with important but only statutory recognition through the federal Freedom of Information Act (FOIA)[250] and a slow wave of matching

242. *See generally* CHERYL ANN BISHOP, ACCESS TO INFORMATION AS A HUMAN RIGHT (2012).

243. G.A. Res. 217A (III), art. 19, U.N. Doc. A/810, at 71 (Dec. 10, 1948).

244. Art. 19(2), Dec. 16, 1966, S. Treaty Doc. 95-20, 999 U.N.T.S. 171.

245. *See also* Right 2 Know, International Instruments and Standards, http://right2info.org/resources/international-instruments (last visited July 28, 2012) (listing relevant declarations around the world).

246. Article 19, *Who We Are*, http://www.article19.org/pages/en/who-we-are.html (last visited July 28, 2012).

247. Szabadságjogokért v. Hungary, App. No. 37374/05, 53 Eur. H.R. Rep. 3, ¶¶ 26-27, 35-38 (2011); Claude-Reyes v. Chile, Merits, Reparations, and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C), No. 151, ¶¶ 75-87 (Sept. 19, 2006).

248. CETS No. 205, *available at* http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=205&CM=8&DF=29/07/2012&CL=ENG. The treaty will enter into force upon ten ratifications and at the time of research, July 29, 2012, was ratified in Bosnia and Herzegovina, Hungary, Montenegro, Netherlands, and Sweden.

249. Potter Stewart, *"Or of the Press,"* 26 HASTINGS L.J. 631, 636 (1975).

250. 5 U.S.C. § 552 (2006).

state reforms.[251] With the quirky exception of courtroom access to criminal trials,[252] the U.S. Supreme Court drew a bright line between, on the one hand, news reporting and information dissemination, protected by the freedom of expression, and, on the other hand, news gathering and information acquisition, which are not protected. Through key cases such as *Branzburg v. Hayes*,[253] regarding the reporter's privilege, and *Houchins v. KQED*,[254] regarding access to prisons, the Court marked a boundary beyond which the Constitution has no command.

Statutory access in state and federal law in the United States is modeled on common law.[255] After that example, sunshine laws universally preserve the common law model of broad, presumptive access that may be rebutted only upon enumerated exemptions or supervening rights.[256] In accordance with that language, presumptive access is a central concept that defines access in the United States through both statutory and continuing common law mechanisms.[257]

But statutory access and exemptions sometimes meet at soft and controverted borders, as where exemptions for personal privacy are concerned. At those intersections in both federal and state law, the formality of presumption and rebuttal that favors access tends to yield to a balancing approach that would be right at home in any of the world's human rights courts.

The balancing approach was well illustrated recently in a June 2012 decision of the New York Court of Appeals construing the state open records law.[258] The court denied a historian access to the names of communist informers whom state officials had promised anonymity in the 1950s.[259] (The case is a modest American analog to the debate in the Eastern Bloc over access to Stasi records that identify informers and

---

251. *See generally* RICHARD J. PELTZ-STEELE, THE LAW OF ACCESS TO GOVERNMENT 127, 129, 293, 343 (2012).

252. *E.g. id.* at 3-5; *see also* Richmond Newspapers v. Virginia, 448 U.S. 555 (1980).

253. 408 U.S. 665 (1972).

254. 438 U.S. 1 (1978).

255. PELTZ-STEELE, *supra* note 251, at 125-27.

256. *Id.* at 129-30; *see also* Nixon v. Warner Communications, 435 U.S. 589, 597-99 (1978).

257. PELTZ-STEELE, *supra* note 251, at 129-30; *see also* United States v. Peterson, 627 F. Supp. 2d 1359, 1373 (M.D. Ga. 2008).

258. Harbatkin v. New York City Dep't of Records & Info. Servs., No. 91, 2012 N.Y. Slip. Op. 04277, 2012 WL 1986509 (June 5, 2012).

259. *Id.* at *3.

collaborators in earlier decades.[260]) Decisive in the case, the New York law exempts information from public disclosure when an "unwarranted invasion of privacy" would result,[261] a root test that appears also in federal FOIA exemption 6 for personnel, medical, and similar files, and in exemption 7 for law enforcement records.[262] Ample case law at state and federal levels has established that "unwarranted" analysis calls for a balancing of privacy against public interest.[263] In the instant case, historical investigation carried weight on the public interest side of the balance.[264] But the court ultimately looked to the state's promise of confidentiality and the risk of embarrassment to informers' descendants to find the privacy side of the balance the weightier.[265]

An older federal FOIA case arising from the destruction of the space shuttle Challenger also well demonstrates balancing in FOI and privacy. The decision in *New York Times Co. v. National Aeronautics and Space Administration (NASA)*[266] exemplifies privacy in FOI reduced to a balancing test with a humanist thumb on the privacy side of the balance. Since Challenger exploded soon after launch in 1986, controversy has surrounded the question of whether and for how long astronauts might have been conscious and aware of their predicament before they died.[267] NASA released to the public a transcript of the last communication from the craft, but refused to release the audio recording.[268] *The New York Times* sought the recording under the FOIA.[269] Applying the "unwarranted invasion of privacy" standard,[270] federal courts recognized a "substantial privacy interest" on behalf of astronauts' families.[271] The courts moreover concluded that "the very sounds of the astronauts' words," apart from the published transcript, comprised an

---

260. *See, e.g.*, Inga Markovits, *Selective Memory: How the Law Affects What We Remember and Forget About the Past—The Case of East Germany*, 35 LAW & SOC'Y REV. 513, 533-40 & n.29 (2001).

261. N.Y. PUB. OFF. Law §§ 87(2)(b), 89(2)(b) (McKinney 2012).

262. 5 U.S.C. § 552(b)(6), (b)(7)(C) (2006).

263. *E.g.*, Goyer v. New York State Dep't of Envtl. Conservation, 813 N.Y.S.2d 628, 635 (Sup. Ct. 2005).

264. *Harbatkin*, 2012 WL 1986509, at *3.

265. *Id.*

266. 782 F. Supp. 628 (D.D.C. 1991).

267. *See, e.g.*, *Astronauts Likely Survived Challenger Explosion* (WESH-TV news broadcast Jan. 28, 2011), *available at* http://www.youtube.com/watch?v=uqcd_3daPQ8.

268. *NASA*, 782 F. Supp. at 630.

269. *Id.*

270. 5 U.S.C. § 552(b)(6) (2006).

271. *NASA*, 782 F. Supp. at 631-32, *after remand from* 920 F.3d 1002, 1004-05 (D.C. Cir. 1990).

"intimate detail" worthy of protection against public consumption.[272] The trial court found speculative any public accountability function in disclosure of the recordings, thus insufficient public interest to counterbalance privacy.[273]

A transformative development in American access law in the first years of the twenty-first century has been the advent of regulatory systems to govern access to records in state and federal courts.[274] Because these new systems have been incubated in a post-September 11th context, they make for a compelling barometer of contemporary American sentiments on access and privacy. The picture is not what it was in the 1960s. Like their progenitors in FOI statutory and common law access, court record access systems tend formally to adopt the presumption-exemption approach. But in adapting historic court practices to the electronic age, the debates over court record access have acknowledged a far more nuanced reality.

A charismatic figure in the early development of court record access systems was the "jammie surfer."[275] The jammie surfer represented every person's gut aversion to the probing of his or her personal information in court records by a home-computer user who apparently lacked the decency to put on proper clothes and visit the courthouse.[276] The problem of the jammie surfer is really just one facet of the "practical obscurity" debate.[277] Derived from the seminal federal FOIA case *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*,[278] the term practical obscurity described the reality that courthouse records in the paper age were often effectively confidential because of their geographic dispersion in local courthouses, the difficulties of finding and copying papers, and possible obstruction by court clerks against inquiries they perceived as illegitimate. To the delight of FOI advocates and to the horror of privacy advocates, the migration of court records to online platforms promised largely to obviate those barriers. In recent years, privacy advocates have lobbied vigorously for "intentional inconveniences" that simulate or restore practical obscu-

272. *NASA*, 782 F. Supp. at 631-32, *after remand from* 920 F.3d at 1006, 1009-10.

273. *NASA*, 782 F. Supp. at 632-33.

274. *See generally* Richard J. Peltz, Joi L. Leonard & Amanda J. Andrews, *Arkansas Proposal on Access to Court Records*, 59 ARK. L. REV. 555, 557-59, 611-14 (2006).

275. *Id.* at 716-21.

276. *Id.* at 716-17.

277. *See id.* at 718-26.

278. 489 U.S. 749, 762, 780 (1989).

rity.[279] One modest redress, adopted by the federal court record access system, is to require users online to register, so that any misuses of information harvested from court records can be tracked.[280] More bluntly, many states simply have limited online case information to docket entries, or relegated some classes of cases, such as juvenile or other domestic matters, to courthouse paper only.[281]

Intentional inconvenience marks a substantial departure from FOI statutory norms rooted in the civil rights tradition. In statutory FOI, the overwhelming rule is to reject record access decisions predicated on the identity of the requester,[282] on the medium or format in which the record is maintained,[283] or on the risk of obviating merely practical obscurity.[284] That these distinctions are newly important in the drafting of judicial access mechanisms in the twenty-first century says something about the rise of privacy as a viable norm to compete with the freedom of information in the absence of any constitutional compulsion.

Another salient distinction to appear in access policies in the last fifteen years is based upon the motive of the requester, especially as between commercial and non-commercial motives. This distinction again departs from a civil rights era FOI norm, namely motive neutrality, which forbade discrimination based on requester motive.[285] Adoption of the distinction is meant in part to redress perceived profiteering in information compiled at taxpayer expense.[286] But a significant and growing objective is to protect personal privacy exactly as the European Union has through the DPD, and as the European Union would through the proposed regulation.

For example, in the procedure adopted by Arkansas in 2007, a court record requester was compelled to assert a noncommercial purpose, or else submit to a rigorous request procedure that vests substantial discretion in court administrators to set terms and conditions on access.[287] The Arkansas rule does not rival the data protections in EU

---

279. Richard J. Peltz-Steele, *Electronic Court Records*, *in* TRANSPARENCY 2.0 (Charles N. Davis ed., forthcoming 2013) (copy on file with author while pending publication).

280. *Id.*

281. *Id.*

282. Peltz, Leonard, & Andrews, *supra* note 274, at 705-15.

283. *Id.* at 721-26, 731-32.

284. *Id.* at 721-26.

285. *Id.* at 705-15.

286. *See, e.g.*, *id.* at 728-29.

287. ARK. SUP. CT. ADMIN. ORDER 19, § VI (as promulgated in 2007), *available at* https://courts.arkansas.gov/rules/admin_orders_sc/admord19.pdf. In 2012, the Arkansas Supreme Court amended the rule to further limit access to protect personal privacy. Bulk distributions, meaning

law, but it does contemplate that court administrators will impose privacy-protective conditions to control downstream data disseminations.[288] For example, regulators can ensure that revised dispositions such as dropped charges, exonerations, and expungements are included in criminal-information databases. Administrators might not have the kind of control over downstream data transfers that a European "right to be forgotten" would entail, but at least they can ensure accuracy in the first generation of data transfer, and they can compel data brokers at least to offer updates to downstream consumers.

The commercial versus non-commercial distinction had precedent in statutory FOI law, as the Supreme Court in 1999 rejected a constitutional challenge to a California statute favoring non-commercial users of certain police records.[289] But with vast courthouse stores of data in property and vital records, worries over data-broker abuse, and fears of high-tech crime such as identity theft, the demand has multiplied for measures such as intentional inconveniences that impede the free flow of information. With no constitutional backstop, access and privacy in the area of court records are feeling their way to an artful balance that abhors free expression or FOI absolutism.

IV. RECONSTRUCTING PRIVACY

Thinking about privacy is in vogue now in academic circles around the world. Unexceptionally, U.S. scholars and advocates have been eager to systematize diffuse musings and reconstruct privacy as rational and sturdy scaffolding for law and regulation. Exceptionally, U.S. policymakers must fit this reconstructed privacy into an existing superstructure of civil and economic liberties. That superstructure has been molded and in places made rigid by the same social developments that shaped U.S. constitutional law in the twentieth century. The problem is more one of legal architecture than of public will, and U.S. researchers

---

wholesale record dumps, are permitted now only upon fee-based licensing. ARK. SUP. CT. ADMIN. ORDER 19, § VI(C) (as amended in 2012), *available at* https://courts.arkansas.gov/rules/admin_orders_sc/index.cfm#19. Compiled distributions, meaning records responsive to a search query, are permitted upon actual costs in consonance with statutory FOI principles; however, personal identities in the records must be redacted unless the requester demonstrates that personal identification is essential for a sworn non-commercial ("scholarly, journalistic, political, governmental, research, evaluation, or statistical") purpose. *Id.* § VI(B).

288. ARK. SUP. CT. ADMIN. ORDER 19, § VI cmt. (as amended in 2012, without material change in this regard since original promulgation in 2007).

289. Los Angeles Police Dep't v. United Reporting Publ'g Co., 528 U.S. 32 (1999) (analyzing CAL. GOV'T CODE § 6254(f)(3) (West 2012)).

such as Helen Nissenbaum and Daniel Solove are laying the groundwork to tackle the project.

Professor Solove posited a sixteen-category taxonomy of information activities that can harm data subjects.[290] He theorized that if privacy harms can be clearly articulated, then lawmakers can work back to define and disincentivize the information practices that result in those harms.[291] Among the potentially injurious activities, and key areas of policy discussion in the information age, are oft hand-in-hand surveillance and secondary use.[292] Both were at issue, for example, in the recent uproar over Google's privacy policy revision, by which Google dropped information-sharing barriers across its various platforms, such as search engine, electronic mail, and location mapping.[293] This "surveillance" of user activity allows Google to construct profiles of its users with a level of intimate familiarity that makes some uncomfortable. Searches for information about sexual fetishes or venereal diseases are not the kind of data a user might wish to have associated with her or his personal identity and home and electronic addresses.

Amplifying qualms over surveillance is the fear of secondary use (and tertiary use, etc.), that is, the use of information for purposes unrelated to its initial harvesting. A user might not object to Google's use of location mapping to enhance search results for a "florist."[294] But the user might be surprised and uncomfortable when an advertising bot a week later proposes a dating service upon the perceptive gamble that the twenty-year-old who sought a florist in August would soon be in the market for a new romantic partner. The situation is not much improved by knowing that the aforementioned intimate details are part of

290. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 10-11, 103-70 (2008).

291. *Id.* at 171-74.

292. *Id.* at 106-12 (surveillance), 129-33 (secondary use).

293. *See* GOOGLE POLICIES & PRINCIPLES, http://www.google.com/policies/ (last visited July 28, 2012); *see also, e.g.*, Elec. Privacy Info. Ctr. v. Fed. Trade Comm'n, 844 F. Supp. 2d 98 (D.D.C. 2012), *aff'd*, No. 12-5054, 2012 WL 1155661 (D.C. Cir. Mar. 5, 2012) (dismissing effort to compel administrative investigation of Google, Inc., for lack of statutory basis for judicial review); Jaikumar Vijayan, *36 State AGs Blast Google's Privacy Policy Change*, COMPUTERWORLD (Feb. 24, 2012), http://www.computerworld.com/s/article/9224590/36_state_AGs_blast_Google_s_privacy_policy_change; Karen Evans & Jeff Gould, *Google's New Privacy Policy is Unacceptable and Jeopardizes Government Information in the Cloud*, SAFEGOV (Jan. 25, 2012), http://safegov.org/2012/1/25/google's-new-privacy-policy-is-unacceptable-and-jeopardizes-government-information-in-the-cloud.

294. A less mundane example of social utility through information cross-referencing is Google's endeavor to use ill health reporting to track the spread of infectious disease. *See* Hendel, *In Europe*, *supra* note 107.

the same data profile. Google itself is not in the data brokering business at present, but surveillance and secondary use may result in painful and invasive privacy violations with real social and financial consequences when intimate personal profiles are sold wholesale for unrestricted downstream applications—say, to a potential employer or insurer.

Professor Nissenbaum posited a more elaborate theory of "contextual integrity" that examines the context in which privacy is implicated relative to the norms that animate the information use.[295] Her complex and thoughtful taxonomy defies easy summary. To oversimplify nevertheless, she outlined four constructs that define context: the role of the actor in context, such as journalist; the activity in context, such as news reporting; the social norms that govern in the context, such as the use of quotation marks to indicate a subject's own words; and the values that operate in the context, such as objectivity.[296] Nissenbaum further outlined four parameters of informational norms: context, such as a newspaper's front page; actors, that is, the identity of the information senders, the receiver, and the data subject; attributes of the information, such as the physical appearance of a data subject; and most importantly, transmission principles, including customary and articulated constraints on information transmission, such as a reporter's promise of non-attribution.[297]

The analytical trigger in the Nissenbaum approach is a change in the context of information use, as determined by a change in the constructs that define context.[298] A change—say the journalist decides to use a deep-background interview with a corporate whistleblower to put words in the mouth of a fictional character in a screenplay—requires that the new use be tested for consistency with the original parameters of informational norms.[299] The deep-background agreement, a transmission principle in the initial disclosure of information, contemplated *no* use of the data subject's words, regardless of the speaker. For that and various other reasons, contextual integrity is compromised. Lawmakers may choose to define an invasion of privacy according to such a compromise of contextual integrity.[300]

Solove's and Nissenbaum's creative approaches point to similar

295. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY & THE INTEGRITY OF SOCIAL LIFE 127-28 (2010).

296. *Id.* at 132-40.

297. *Id.* at 140-47.

298. *Id.* at 148-50.

299. *Id.*

300. *Id.* at 236-37.

results because both are merely tools to articulate existing value systems. A public library's database of patron checkouts furthers free intellectual inquiry and efficient management of a shared resource. Thus transfer of personal information for national security investigations (surveillance), or sale of data for commercial profiling (secondary use), violates privacy rights, whether framed as an aversion of injurious consequence or as a compromise of contextual integrity. Within any one cultural tradition, be it American, French, or another, the proper employment of each approach aids in the detection of a violation of social norms. The violation then may or may not be used to demarcate a violation of law or civil rights.

Crucially, Solove and Nissenbaum both reject what Solove termed "the secrecy paradigm"[301] in favor of a contextual approach. This divergence from convention exemplifies the resemblance of these approaches to those of the DPD and proposed regulation in the European Union. The secrecy paradigm, which is a controlling norm in trade secret law,[302] posits that only secrets are legally protectable; information once disclosed is fair game in the public sphere.[303] The DPD similarly rejected the deceptively simple dichotomy of the secrecy paradigm by persisting in the regulation of data use after a subject's voluntary disclosure. The context of initial disclosure and the ongoing contexts of information use, including downstream injury, are defining features of both Solove's and Nissenbaum's analyses. Just as the DPD newly emphasized disclosure and consent for information practices when persons remain identifiable, Nissenbaum posited that factors such as notice, consent, and redaction may serve to maintain contextual integrity.[304] In toughening the requirement of explicit consent and allowing a sort of consent revocation through the device of the right to be forgotten, the proposed regulation is only further consistent with the concepts of harm-aversion and contextual integrity.

Solove acknowledged that an approach to privacy predicated on extant values might require that the Supreme Court reconsider its commitment to the secrecy paradigm[305]—which it might. In present

---

301. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1140-41 (2002) [hereinafter Solove, *Access and Aggregation*]; *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 42-44 (2004).

302. *E.g.*, GABRIEL M. RAMSEY, VICKIE L. FEEMAN, WILLIAM S. COATS & MARIA ATHANASIOU, 1A INTERNET LAW AND PRACTICE § 18:5 (West 2012).

303. Solove, *Access and Aggregation*, *supra* note 301, at 1140.

304. NISSENBAUM, *supra* note 295, at 145.

305. Solove, *Access and Aggregation*, *supra* note 301, at 1176-84.

jurisprudence under the U.S. Fourth Amendment,[306] the font of constitutional privacy, the government can dip deeply into personal information held by third parties, such as banks and telephone companies, because the data are regarded as already disclosed.[307] The concept carries over into the civil context where, for example, the secrecy paradigm is expressed through the tortious invasion of privacy requirement that information have been guarded as secret (like in trade secret law).[308] Voluntary disclosure furthermore may manifest in tort through a defense of consent (to intentional torts) or comparative fault (to negligence torts).[309] But in a recent case in which the Court, on narrow grounds, reproved the covert installation of a GPS tracking device,[310] Justice Sotomayor hinted that a reconsideration of the dichotomy might be in the cards. The decision in general confirmed the Court's willingness to adapt the Fourth Amendment to new technologies,[311] and GPS tracking is plainly "surveillance" in Solove's terms. Writing in concurrence, Justice Sotomayor acknowledged that GPS tracking can accumulate "a wealth of detail about [a subject's] familial, political, professional, religious, and sexual associations," and that such power is "susceptible to abuse"[312]—which is to say, compromised contextual integrity may result in injury. She concluded: "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[313]

The Fourth Amendment of course comes into play only in the presence of state action, and the DPD and proposed EU regulation, along with Solove and Nissenbaum, are not so limited in their outlook. Though proposed regulatory models in the U.S. Congress have not yet gained traction, there is a movement afoot in the White House to get the ball rolling.

The Obama Administration in February 2012 unveiled the Con-

306. U.S. CONST. amend. IV.

307. *E.g.* Katz v. United States, 389 U.S. 347, 350-53 (1967).

308. *E.g.*, 77 C.J.S. *Right of Privacy and Publicity* § 35 (West 2012).

309. *E.g. id.* § 36 (consent or release); *see also* Snavely v. AMISUB of South Carolina, Inc., 665 S.E.2d 222, 226 (S.C. Ct. App. 2008) (comparative fault).

310. United States v. Jones, 132 S. Ct. 945 (2012). *See generally* Peter Swire, *A Reasonableness Approach to Searches After the* Jones *GPS Tracking Case*, 64 STAN. L. REV. ONLINE 57 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/searches-after-jones.

311. *See Jones*, 132 S. Ct. at 959, 963-64 (Alito, J., concurring, joined by Ginsburg, Breyer & Kagan, JJ.).

312. *Id.* at 956 (Sotomayor, J., concurring).

313. *Id.* at 957 (Sotomayor, J., concurring).

sumer Privacy Bill of Rights.[314] The initiative, which charges the Commerce Department with further development,[315] is a poor relation to EU controls. Self-regulation, voluntary participation, and technological architecture are front-line strategies in the plan,[316] and the scope is limited to data disclosed in a commercial context.[317] But the initiative does contemplate Federal Trade Commission enforcement of industry-developed standards and eventual codification of a broader regulatory framework.[318]

Moreover, the values articulated in the initiative better reflect the scope of the proposed EU regulation than the scope of the conventional secrecy paradigm. The initiative calls for continuing consumer control over data, including a means to revoke or limit consent.[319] Remarkably, the initiative enumerates "respect for context" as a core value, calling on companies to use or disclose data consistently with consumer expectations, or at least to mitigate secondary uses with control and transparency norms.[320]

The Obama initiative is a modest foray into the regulation of data collection and use, but the initiative portends a regulatory framework that would move U.S. law leagues in the direction of European privacy. As U.S. commercial businesses and data brokers warily eye the development of the proposed regulation in the European Union, they must realize too that this election-year White House initiative coincides with Supreme Court misgivings about technology and privacy and with scholarly approaches to privacy that reject the secrecy paradigm in favor of subject-driven contextual analyses.

V. CONCLUSION

The EU proposed regulation demonstrates a balancing approach to free expression and privacy that has become characteristic of European human rights law and has diverged from the U.S. bent toward free speech absolutism. Even with safeguards to protect the freedom of expression, the proposed regulation seems likely to widen the scope of

---

314. WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 11-22 (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

315. *Id.* at 45.

316. *See id.* at 2, 12, 15, 19, 27, 29.

317. *See id.* at 1.

318. *See id.* at 35-36.

319. *Id.* at 11.

320. *Id.* at 15-19.

an EU data protection regime that is vastly more solicitous of the right of personal privacy than U.S. and other non-EU businesses are accustomed to.

Nevertheless, 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. American devotion to free speech absolutism is not what it was in the civil rights era. The doctrine of *New York Times Co. v. Sullivan*, with its powerful prophylactic protection for truth, shows wear. Its chill on legitimate as well as illegitimate causes of action, having outlived past the exigencies of the civil rights era, highlight ways in which the doctrine might be ill fit for further expansion in tort law, especially as would limit liability for invasion of privacy and expressive interference. Meanwhile the doctrine of *Smith v. Daily Mail*, though a direct descendant of the rule against prior restraints, also has met a rocky reception on privacy's shores. In areas of information law that were not constitutionalized to accommodate freedom of expression in the civil rights era, such as fair-use copyright and the freedom of information, new developments represent a solicitousness of privacy that often has more in common with contemporary European-style balancing than with the free speech imperative of American civil rights era jurisprudence.

Finally, this shift in approach to the relationship between free expression and privacy is reflected in the leading re-conceptualizations of privacy that have appeared in the literature in the last decade. These new approaches reject privacy as an all-or-nothing proposition and endeavor to build frameworks for privacy law that reflect contemporary social norms. These attractive formulations portend a sea change in the way U.S. law and policy approach free expression and privacy in a direction consistent with the drift away from the free speech imperative.

At some point, emerging American privacy norms—which value individual expectations, construe privacy in context, and ultimately might countenance a right to be forgotten—will run up against the rigid constitutional constraints of the First and Fourth Amendments, profoundly shaped as they were by the civil rights movement. But with the hard rules in those areas showing signs of softening, and non-constitutionalized areas of law, such as FOI, modeling paths of compromise and balance, the prophesied cultural collision might yet unfold less as conflict and more as convergence in a new American privacy.