The "Right to Be Forgotten": Reconciling EU and US Perspectives

Steven C. Bennett
The “Right to Be Forgotten”: Reconciling EU and US Perspectives

By
Steven C. Bennett*

Recent developments in the European Union (EU) have highlighted the potential for the development of a “right to be forgotten.” For United States (US) companies, especially those operating on the Internet, the development and enforcement of such a right could prove to be quite problematic. This Article outlines the practical implications of such a right, pointing the way toward possibilities for reconciliation of US and EU views on the application of a right to be forgotten.

I. RECENT EU DEVELOPMENTS

Viviane Reding was recently accepted to a position as European Commissioner for Justice, Fundamental Rights and Citizenship. She previously served as Commissioner for Information Society and Media. In those roles, she has served as an important spokesperson and advocate for the development of EU privacy protection.1 At an American Chamber of Commerce gathering in June 2010, Reding suggested that her “paramount goal” in her new position is to “ensure that people have a high level of protection and control over their personal infor-

* The Author is a partner at Jones Day in New York and teaches Conflicts of Law at Hofstra Law School. The views expressed are solely those of the author and should not be attributed to the author’s firm or its clients.

Reding emphasized that “[i]nternet users must have effective control of what they put online and be able to correct, withdraw or delete it at will,” labeling this right of control “a right to be forgotten.” Reding, moreover, noted that “[a]ll companies that operate in the European Union must abide by our high standards of data protection and privacy.”

Later in 2010, an EU press release announced that the European Union planned to propose “a new general legal framework for the protection of personal data in the European Union covering data processing operations in all sectors and policies of the European Union.” This “comprehensive” new legal framework would be subject to negotiation between the European Parliament and the European Council of Ministers. The EU announcement specifically mentioned the “right to be forgotten,” described as the right of individuals to “have their data fully removed when it is no longer needed for the purposes for which it was collected.”

A more comprehensive EU white paper, released simultaneously, referenced the same concept and outlined the EU plan for modernization of EU privacy law to address “globalization and new technologies. . . .” Similar EU


3. Id. Reding noted, however, that the area of data protection and privacy “needs clarity, not red tape.” She suggested that “industry self-regulation” could “work well” in this area. Id.; see generally Viviane Reding, The Upcoming Data Protection Reform for the European Union, 1 INT’L DATA PRIV. L. 3 (2011) (“Rapid technological developments and globalization have profoundly changed the world around us, and brought new challenges to the protection of personal data. . . . Globalization has seen an increasing role of third countries relating to data protection, and has also led to a steady increase in the processing of the personal data of Europeans by companies and public authorities outside the European Union.”), available at http://idpl.oxfordjournals.org/content/1/1/3.full.


6. See Data Protection Reform – Frequently Asked Questions, supra note 4 (stating that the announcement, moreover, pointed specifically at social networking site information: “People who want to delete profiles on social networking sites should be able to rely on the service provider to remove personal data, such as photos, completely”).

7. See Comprehensive Approach on Personal Data Protection, supra note 5, at 5. The EU white paper suggested a need to examine ways of “clarifying the so-called ‘right to be forgotten,’ i.e.
explanations of the “right to be forgotten” have followed.8 The European Union, moreover, has emphasized that “privacy standards for European citizens should apply independently of the area of the world in which their data is being processed.”9

Recent developments in Spain and Italy have amplified public discussion on the right to be forgotten. In early 2011, Spanish data protection authorities demanded that Google remove links to online news articles on grounds that the articles contained out-of-date information which infringed on the privacy of Spanish citizens.10 At about the same time, Italy announced that it would regu-
late Internet content sites as if they were television broadcasters and would impose an obligation to publish “corrections” to libelous content.11 These developments followed a case in Germany in 2009, where two murderers, who had completed their prison sentences, sued to remove references to their crime from Internet postings.12 In early 2010, moreover, an Italian court found several Google executives guilty of violating Italian privacy law by permitting a video of abuse of a disabled boy to persist on its online video service.13 These developments suggested the broad uses to which a comprehensive “right to be forgotten” might be implemented.

II. US RESPONSES

Many US commentators, confronted with the suggestion of development of a “right to be forgotten,” accused EU regulators of “foggy thinking”14 incon-
sistent with fundamental US values (such as freedom of expression and of the press). A representative of Facebook, for example, suggested that the EU approach was to “shoot the messenger,” in that the “source of the content” rather than the “places where the content is shared,” should be the focus of any efforts to promote privacy controls. Others suggested that the EU approach could create a property right in information (which otherwise does not exist), and pro-

sists “[t]he right to be forgotten is a figment of our imaginations;” “a right to be forgotten is about extreme withdrawal, and in its worst guise can be an antisocial, nihilistic act”), available at http://www.guardian.co.uk/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet.

15. See Timothy Ryan, The Right To Be Forgotten: Questioning The Nature Of Online Privacy, May 2, 2011 (“Sometimes, the right to information ought to outweigh the right to privacy. What incentive will there ever be for a journalist to rake muck if the information can simply be taken down upon request?”), available at http://www.psfk.com/2011/05/the-right-to-be-forgotten-questioning-the-nature-of-online-privacy.html; Spanish Claim “Right To Be Forgotten” On Web, Apr. 20, 2011 (“In the United States, we have a very strong tradition of free speech [and] freedom of expression. We would strongly caution against any interpretation of the right to be forgotten that infringes upon that.”) (quoting Justin Brookman, Center for Democracy and Technology, Privacy Project), available at http://www.cbsnews.com/2100-205_162-20055718.html; Jennifer L. Saunders, Across Jurisdictions And Web Domains, Questions Of Privacy And Online Anonymity Persist, Apr. 15, 2011 (noting “tug-of-war” involving “privacy-related question of accountability when one individual’s postings defame or expose personal information about another”), available at https://www.privacyassociation.org/publications/2011_04_15_across_jurisdictions_and_web_domains_questions_of_privacy_and; L. Gordon Crovitz, Forget Any “Right To Be Forgotten”, Nov. 19, 2010 (“Any regulation to keep personal information confidential quickly runs up against other rights, such as free speech, and many privileges, from free Web search to free email.”), available at http://abluteau.wordpress.com/2010/11/19/forget-any-right-to-be-forgotten/; L. Gordon Crovitz, Get Used To It—The Internet Is Forever, Nov. 10, 2010 (“Regulators have no reason to dictate one right answer to these balancing acts among interests that consumers are fully capable of making for themselves.”).

16. See Kelly Fiveash, Facebook Tells Privacy Advocates Not To “Shoot The Messenger:” You Have No Right To Be Forgotten, Argues Big IT, Mar. 23, 2011, http://www.theregister.co.uk/2011/03/23/facebook_shoot_messenger/; Pichayada Promchertchoo, Facebook Questions EU “Right To Be Forgotten”, Mar. 23, 2011 (right to be forgotten is “opposite of what most users want, according to Richard Allan of Facebook), http://www.techweekeurope.co.uk/news/facebook-questions-eu-right-to-be-forgotten-24509; see also Jason Walsh, When it Comes To Facebook, EU Defends The “Right To Disappear”, Apr. 6, 2011 (“criticism is coming from American technology companies and some advocates who come down on the side of freedom of expression online, over the right to privacy;” “the typical US response is to encourage more personal responsibility and education of users”), http://www.csmonitor.com/World/Europe/2011/0406/When-it-comes-to-Facebook-EU-defends-the-right-to-disappear; Ron Miller, We May Not Have A “Right To Be Forgotten” Online, Mar. 14, 2011 (“There’s really no way to remove every trace of anyone on the Internet, even if there were a law in place requiring it.”), http://www.internetrevolution.com/author.asp?section_id=1047&doc_id=204757.

17. See Larry Downes, Europe Reimagines Orwell’s Memory Hole, Nov. 16, 2010, (“Information isn’t property, at least not as understood by our industrial-age legal system or popular metaphors of ownership. Information, from an economic standpoint, is a virtual good. It can be ‘possessed’ and used by everyone at the same time. . . . And, whether the law says so or not, it can’t be repossessed, put back in the safety deposit box, buried at sea, or ‘devoured by the flames[,]’”), http://techliberation.com/2010/11/16/europe-reimagines-orwells-memory-hole/; Adam Thierer, An Internet Eraser Button To Protect Privacy? Unwise & Probably Impossible, Apr. 19, 2011, (suggest-
duce a “bureaucratic nightmare,” which might interfere with “business demands” for data.

Yet, some US commentators appeared more receptive to at least a limited version of the right to be forgotten. Some, for example, suggested that children...
should have the ability to erase information posted improvidently, out of youthful lack of judgment. Others noted that the concept of “data minimization” (a form of the right to be forgotten) has long been a central element of “fair information practices” under various US laws, and could be expanded. Still others noted that the concept of “forgive and forget” embodies a fundamental human value, and that US law (bankruptcy, credit reporting and criminal law, among others) actually does recognize at least some elements of a “right to be forgot-


22. See Justin Brockman, Europe Revisiting Privacy Law is Opportunity, not Catastrophe, CTR. FOR DEMOCRACY & TECH. (Nov. 12, 2010), available at http://cdt.org/blogs/justin-brockman/europe-revisiting-privacy-laws-opportunity-not-catastrophe (“The concept of data minimization—including deleting data no longer necessary to achieve a consumer purpose—has been a bedrock concept of Fair Information Practices . . . for years.”). A guide recently released by the Department of Homeland Security (“DHS”), for example, aims to help “federal privacy practitioners” understand how to build a “privacy culture.” Department of Health Services Privacy Office, Guide to Implementing Privacy 3 (Jun. 3, 2010), available at http://www.cio.gov/documents/DHS-Privacy-Office-Guide_June-2010.pdf. The DHS guide identifies, as an essential fair information practice, the rule that “DHS should only collect PII [personally identified information] that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).” The Fair Credit Reporting Act (“FCRA”) also provides a model for regulation to minimize the use of out-of-date and inaccurate information. Fair Credit Reporting Act, 15 U.S.C. § 1681. See Protecting Privacy in Online Identity: A Review of the Letter and Spirit of the Fair Credit Reporting Act’s Application to Identity Providers, CTR. FOR DEMOCRACY & TECH. (Feb. 26, 2010), available at http://cdt.org/policy/protecting-privacy-online-identity-review-letter-and-spirit-fair-credit-reporting-act%E2%80%99s-application (noting that the FCRA “is one source of some of the necessary protections and may already apply to entities providing or using identity-related services”).

23. See Seaton Daly, Le Droit a L’oubli—Can We Achieve “Oblivion” on the Internet? EMERGING BUS. ADVOCATE (Mar. 15, 2011), http://emergingbusinessadvocate.wordpress.com/2011/03/15/le-droit-a-loubli-can-we-achieve-oblivion-on-the-internet (“The debate over privacy has more to do with the universal right to control our image than anything else. . . . Who we perceive ourselves to be, and what people really see us for—that’s the debate, and citizens are mandating that we get some of that control back [that] companies have taken from us.”); Jeffrey Rosen, The Web Means the End of Forgetting, N.Y.TIMES (July 21, 2010), http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all (“[S]ome legal scholars have begun imagining new laws that could allow people to correct, or escape from, the reputation scores that may govern our personal and professional interactions in the future.”); VIKTOR MAYER-SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009) (noting without some form of forgetting, forgiveness may be difficult); DAVID SHENK, DATA SMOG: SURVIVING THE INFORMATION GLUT (1997) (noting risks of “information fatigue syndrome” in modern social and technical milieu); Daniel J. Solove, A TAXONOMY OF PRIVACY, 154 U. PA. L. REV. 477, 532 (2006) (“People grow and change, and disclosures of information from their past can inhibit their ability to reform their behavior, to have a second chance, or to alter their life’s direction.”).
The breadth of US reactions to developments in the European Union regarding the right to be forgotten suggests a need for serious thinking about the means available to reconcile US and EU views on the subject. The remainder of this Article focuses on both substantive and procedural mechanisms to effect such reconciliation.

III. RECONCILING SUBSTANTIVE EU AND US VIEWS

The United States and the European Union have traditionally held widely differing views on data privacy. To some degree, those differences remain unresolved. The European Union generally adheres to a high degree of government involvement in protection of this fundamental right. US privacy law has,


27. See James Gordley, When is the Use of Foreign Law Possible? A Hard Case: The Protection of Privacy in Europe and the United States, 67 LA. L. REV. 1073 (2007) (differences between the European Union and the United States may turn in part on degree to which authorities view in-
by contrast, largely developed in a “patchwork,” with a “reactive” array of state and federal statutes and common law doctrines. The United States, moreover, has traditionally emphasized freedom of expression over privacy, as a fundamental value.

Some suggest that a right to be forgotten simply cannot exist in the United States. Yet, a brief review of developments in US privacy law suggests the extent to which EU and US notions of the right to be forgotten might be reconciled. More than 120 years ago, the seminal Warren and Brandeis article on privacy focused on the degree to which “unseemly gossip,” coupled with “modern enterprise and invention” (including the telephone and photography) had contributed to “mental pain and distress,” caused by invasions of privacy. Early cases thereafter suggested at least the possibility of claims for privacy invasion based on harmful reference to out-of-date information. The Restatement (Second) of Torts, moreover, expressly recognized a potential tort claim for “publicity given to private life.”


29. See IAN BALLON, E-COMMERCE AND INTERNET LAW § 26.01 (2011) (“The US approach to data privacy is very different from that of some of our major trading partners, like the EU” and noting that “the United States has placed greater emphasis on free speech and access to information”).


33. See RESTATEMENT (SECOND) OF TORTS, § 652D ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."); Patrick J. McNulty, The Public Disclosure of Private Facts: There is Life after Florida Star, 50 DRAKE L. REV. 93 (2001); John A. Jurata, Jr., The Tort that Refuses to Go Away: The Subtle Reemergence of Public Disclosure of Private Facts, 36 SAN DIEGO L. REV. 489 (1999). These elements are largely derived from William L. Prosser, Privacy, 48 CALIF. L. REV. 383 (1960). These concepts, while based in 19th century (and even earlier) doctrine, retain their vitality in the modern technological age. See, e.g., Jordan Segall, Google Street View: Walking the Line of Privacy—Intrusion upon Seclusion and Publicity Given to Private Facts in the Digital Age, 10 U. PITT. J. TECH. L. & POL. 23 (2010); Andrew Lavoie, The Online Zoom Lens: Why
In *Melvin v. Reid*, decided in 1931, for example, a homemaker, who had once worked as a prostitute and who had been wrongly accused of murder, became the subject of a feature film ("The Red Kimono") seven years after her acquittal, based on the facts of her trial. Although not specifically referencing a right to be forgotten, the court, permitting suit against the film-maker, noted: "One of the major objectives of society as it is now constituted, and of the administration of our penal system, is the rehabilitation of the fallen and the reformation of the criminal." The court held that the unnecessary use of the plaintiff’s real name inhibited her right to obtain rehabilitation. Similarly, in *Briscoe v. Reader’s Digest Association, Inc.*, decided in 1971, the court held that a publisher’s reference to the plaintiff’s prior crimes might infringe on his ability to obtain rehabilitation.

These kinds of cases have largely been overruled based on First Amendment concerns. In a series of opinions, the US Supreme Court held that newsworthy, true stories are protected by freedom of the press, although they may conceivably cause embarrassment or other harm to the stories’ subjects. In

short, “[c]urrent interpretations of tort law do not favor granting relief under privacy tort theories to people whose once-public pasts have been resurrected by the media for public comment and discussion.” Yet, there are still some circumstances where US courts will accept privacy claims, even where the matter is worthy of media attention.

Outside the context of newsworthy stories, US courts have been less inclined to insist on unrestrained access to information. In *Nixon v. Warner Communications, Inc.*, for example, the Supreme Court recognized a general right to inspect and copy public records, but also suggested that courts must exercise their supervisory powers to preclude access to information for “improper purposes,” such as to “gratify private spite or promote public scandal.” Similarly, in *US Dep’t of Justice v. Reporters Comm. for Freedom of the Press*, the Supreme Court recognized, in the context of a Freedom of Information Act re-

38. See Allen, supra note 20, at 59 (“The First Amendment and the common law mandate wide freedom for speaking truth, accurate news reporting and artistic expression”).

39. See M.G. v. Time Warner, Inc., 107 Cal. Rptr. 2d 504 (2001) (Little League players and coaches had a privacy claim after video showed team’s group photo in a story about the team manager’s molestation of several pictured team members).

40. See Daniel J. Solove, *A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere*, 54 Wash. U. L. Rev. 1195, 1199 (2006) (“Regarding the marketplace of ideas, truth must be weighed against other values, and the truth about a private person’s personal life is often not of much importance. Therefore, a balance between free speech and privacy might achieve these interests more effectively than merely protecting speech at all costs”). The precise division between “public” and “private” information, however, has sometimes been difficult to discern. See Charles N. Davis, *Electronic Access to Information and the Privacy Paradox: Rethinking ‘Practical Obscurity’*, ArXiv (2001), http://arXiv.org/ftp/cs/papers/0109/0109083.pdf (cases show that records “rarely fall” into “neat” categories).

41. 435 U.S. 589 (1978); see also Nixon v. Adm’r of Gen. Serv., 433 U.S. 425, 457 (1977) (noting that the President probably had a privacy right in some recordings, which was over-ruled by the Presidential Recordings Act).

42. See 435 U.S. 589, 598 (1978) ("[F]iles could serve as reservoirs of libelous statements for press consumption," or as “sources of business information that might harm a litigant’s competitive standing”).

quest, that a “privacy interest” may exist in “keeping personal facts away from the public eye.” Indeed, the Court specifically noted that increased accessibility of information, as a result of “compilation of otherwise hard-to-obtain information” that “would otherwise have surely been forgotten,” threatened to affect the “privacy interest in maintaining the practical obscurity” of information.

There is, moreover, at least some suggestion in US case law that First Amendment concerns are diminished in the context of international communications. For example, in *Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L’Antisemitisme*, the Ninth Circuit, reversing a lower court decision that refused on First Amendment grounds to enforce a French court decision compelling Yahoo to halt sales of Nazi memorabilia (illegal in France) on its site, noted: “[t]he extent of First Amendment protection of speech accessible solely by those outside the United States is a difficult and, to some degree, unresolved issue. . . .” More recently, in *Holder v. Humanitarian Law Project*, the US

44. See id. at 769. Thus, the central purpose of the Freedom of Information Act (to protect the “‘citizens’ right to be informed about ‘what their government is up to’”) would “not [be] fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency’s own conduct.” Id. at 773. Indeed, the Court remarked that “both the common law and the literal understandings of privacy encompass the individual’s control of information concerning his or her person.” Id. at 763; see also Nat’l Archives & Records Admin. v. Favish, 541 U.S. 157, 166 (2004) (privacy interest “at its apex” when records concern private citizens); Whalen v. Roe, 428 U.S. 589, 599 (1977) (noting “individual interest in avoiding disclosure of personal matters”); id. at 605 (noting “threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks”); Dep’t of the Air Force v. Rose, 425 U.S. 352, 381 (1976) (republishing of information that may have been “wholly forgotten” can cause separate harm, which “cannot be rejected as trivial”).

45. See 489 U.S. at 780; id. at 763-64 (“Plainly, there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information”).

46. 433 F.3d 1199 (9th Cir. 2006) (en banc) (holding French decision unenforceable in the US), rev’d 169 F. Supp. 2d 1181 (N.D. Cal. 2001). The *Yahoo!* decisions in the US followed a French court ruling that *Yahoo!* was required to “take any and all measures of such kind as to dissuade and make impossible any consultations by [Internet] surfers calling from France to sites [that] infringe upon the internal public order of France, especially the site selling Nazi objects.” UEJF & LICRA v. Yahoo!, Inc., T.G.I. Paris, May 22, 2000, translated at http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm. The Ninth Circuit ultimately held that *Yahoo!* could not bring a claim to invalidate the French decision, but was required to wait and respond to French plaintiffs, if they sought to enforce the decision in the US. See generally Marc H. Greenberg, *A Return To Lilliput: The LICRA v. Yahoo! Case And The Regulation Of Online Content In The World Market*, 18 BERKELEY TECH. L.J. 1191 (2003) (overview of case and its jurisdiction implications).

Supreme Court upheld portions of the USA PATRIOT Act that criminalize speech when it is “coordinated” with “foreign terrorist” organizations. These, and other decisions, suggest that First Amendment protections are not absolute, at least in the context of foreign-related speech. Viewed from the other side of the Atlantic, the European Union certainly does not disregard freedom of expression and freedom of the press as essential values. Indeed, recent EU pronouncements and court decisions expressly recognize the need to balance rights of privacy with freedom of expression. Various international declarations similarly support the need for such a balance.

49. See id. at 2730 (referencing USA PATRIOT Act, 18 U. S. C. § 2339B).
50. See, e.g., Meese v. Keen, 481 U.S. 46, 48 (1987) (upholding limits on distribution of foreign political propaganda in the US); Kleindeinst v. Mandel, 408 U.S. 753, 769 (1972) (US citizens may be denied personal access to foreign speakers). In the recent case of G.D. v. Kenny, 205 N.J. 275, 15 A.3d 300 (2011), the New Jersey Supreme Court observed: “In a free society, the right to enjoy one’s reputation free from unjustified smears and aspersions must be weighed against the significant societal benefit in robust and unrestrained debate on matters of public interest.” See id., 15 A.3d at 304. Thus, the court held that, despite the existence of a conviction expungement statute, “an offender has no protected privacy interest in expunged criminal records.” Id. at 308.
52. See WERRO, supra note 30 at 289 (suggesting that “in the context of a conflict between the right to be forgotten and the freedom of the press, the European Court will balance the competing interests and may well consider that in certain cases privacy rights trump the right to publish”); Oreste Pollicino & Marco Bassini, Internet Law In The Era Of Transnational Law, EUI Working Papers RSCAS 2011/24 at 29, available at http://eadmus.eui.eu/bitstream/handle/1814/16835/RSCAS_2011_24rev.pdf?sequence=1 (noting that “[f]reedom of expression” is protected in various European conventions, and in European case law).
54. International Conference Of Data Protection and Privacy Commissioners, International
Thus, within Europe there is room for discussion of the need for balancing essential values in establishing the right to be forgotten.55

Regulators and legal theoreticians on both sides of the Atlantic, moreover, recognize that harmonizing international data protection laws may be key to maintaining the health of the world’s Internet-based economy.56 Indeed, the risk


56. See Article 29 Data Protection Working Party & Working Party On Police And Justice, The Future Of Privacy 6, Dec. 1, 2009 (“The establishment and functioning of an internal market requires that personal data should be able to flow freely from one Member State to another, while at the same time a high level of protection of fundamental rights of individuals should be safeguarded.”); Miguel P. Maduro, So Close And Yet So Far: The Paradoxes Of Mutual Recognition, 3 EUR. PUB. POLICY 814, 817 (2007) (mutual recognition of national values is key to effective Internet regulation); see also EuroISPA, Personal Data Protection In The EU, supra note 55, at 5 (“The current rigid EU rules applying to the transfer of data to third countries do not seem adequate for the cross-border data flows in a globalised economy.”); see generally Steven C. Bennett (ed.), A Privacy Primer For Corporate Counsel, Ch. 9 (2009) (discussing international business challenges in privacy arena); Yaman Akdeniz, Case Analysis Of League Against Racism And Antisemitism (LICRA), French Union Of Jewish Students v. Yahoo! Inc., Yahoo France, 1 ELEC. BUS. L. REP. 110, 6 (2001) (noting “[t]he value of the Internet as a social, cultural, commercial, educational and entertainment global communications system the legitimate purpose of which is to benefit and empower online users, lowering the barriers to the creation and the distribution of expressions throughout the world”)
that EU data restrictions might prevent US companies from doing business in the European zone led the US Department of Commerce to develop a “Safe Harbor” construct57 with the input and approval58 of the EU.59 This approach has generally been successful60 and could be expanded.61 An array of other means to promote harmonization of US and EU views on the balance between privacy and free expression exist, and governments have pursued these options in recent years.62 Additionally, the existence of long-standing concepts of “fair information practices” provides a solid base for common discussion among regulators.63

Recent political developments in the United States suggest that US regulators and law-makers may be particularly receptive to discussions on the merits (quotation omitted).


62. See generally Bernhard Maier, How Has The Law Attempted To Tackle The Borderless Nature Of The Internet?, 18 INT’L J. L. & INFO. TECH. 142 (2010) (summarizing efforts at harmonization of international law regarding the Internet); Rustad & Koenig, supra note 12 (suggesting means to promote harmonization, including ALI/UNIDROIT consultation, treaty negotiations and expansion of the Hague Convention on Jurisdiction and Foreign Judgments, and choice of law/choice of forum provisions in user agreements).

of enhanced privacy protection. 64 In December 2010, the FTC staff issued a “preliminary” report, aimed at providing a “broad privacy framework to guide policymakers, including Congress and industry.” 65 The FTC Report called for a wholesale “re-examination” of the FTC’s approach to privacy protection. 66 Shortly after the FTC released its 2010 report, the Department of Commerce issued its own report on “Commercial Data Privacy and Innovation in the Internet Economy” 67 (“Commerce Report”). The Commerce Report set out four main goals for US privacy protection policy: 68 (1) to enhance consumer trust online through the recognition of “revitalized” fair information practice principles; 69

---


66. Id. at 19.


68. Id. at 3-7.

69. The Commerce Report suggested that fair information principles should “enhanc[e] transparency, encouraged [greater detail in purpose specifications and use limitations, and foster[ the development of verifiable evaluation and accountability programs. . . .” Id. at 30. The report noted “lengthy and complex” disclosures that “fail to inform,” and suggested that “privacy rights depend on [consumer] ability to understand and act on” company privacy policies. Id. at 31 (documents written in “legalese” are “typically overwhelming” to the average consumer) (quotations omitted). The Report encouraged “reduced length and greater simplicity and clarity” in privacy disclosures. Id. at 33.
to encourage the development of “voluntary, enforceable” privacy codes of conduct through “collaborative efforts” with government;\(^70\) (3) to encourage “global interoperability;”\(^71\) and (4) to ensure “nationally consistent” privacy rules.\(^72\)

These stated goals for US data protection policy certainly recognize the global nature of information technology issues. Indeed, EU data policy developments have, to some degree, pushed the world toward uniform standards of data protection, and have spurred US regulators to action.\(^73\) Moreover, EU developments have sparked US interest in dialogue with EU authorities.\(^74\) Additional dialogue on the subject of data protection and privacy should develop.\(^75\)

70. The Commerce Report suggested the need to promote development of “flexible but enforceable codes of conduct,” to address “emerging technologies and issues not covered” by current fair information practices. Id. at 41; see id. at 42 (noting risk that privacy practices may “ossify”).

71. The Commerce Report noted that “[d]isparate approaches to data privacy can “create barriers” to trade, “harming both consumers and companies.” Id. at 53. The report reviewed a host of options for “greater harmonization and international interoperability.” Id. at 54 (citing creation of a global privacy standard, adoption of a treaty or convention to govern cross-border data flows, an enhanced US privacy framework that “can be more easily supported abroad,” increased Department Of Commerce international advocacy for US interests, more “focused and coordinated” US government advocacy of the US position internationally, creation of “accountability certifications,” such as binding corporate rules, application for “adequacy” status with the European Union, and development of a US framework that “furthers harmonization” of international privacy laws, including the EU directive). Id. at 54-55. The report suggested the possibility to take harmonization work “to the next level,” by creating “binding trade commitments” to “steer the world toward global privacy protection interoperability.” Id. at 56.

72. The Commerce Report suggested the need for a “comprehensive” commercial data security breach framework, using federal preemption, to prevent the “maze” of disparate state laws from becoming “costly and burdensome” to business. Id. at 57 (quotations omitted). Any new federal privacy framework should, however, “seek to balance the desire to create uniformity and predictability across State jurisdictions with the desire to permit States the freedom to protect consumers and to regulate new concerns” from emerging technologies that could “create the need for additional protection.” Id. at 61.

73. Ballon, supra note 29 (noting that EU adoption of data privacy Directive “pushed the [FTC] to become increasingly active in the area of internet privacy;” today, the FTC “plays a prominent role in shaping debates over privacy protection and in encouraging compliance”); Moving Forward, supra note 64, at 81-82 (noting that the FTC has joined with 12 EU regulators to launch the Global Privacy Enforcement Network, and that the FTC has been officially admitted to annual conference of data protection and privacy commissioners, and DOC officials have become “increasingly visible” in meetings with EU data protection authorities).


75. In December 2010, the EU’s Reding asserted that US officials were “unprepared” and “uninterested” in negotiating over data privacy issues. See Cyrus Farivar, EU Official Dissatisfied With American Response To Data Protection Concerns, DEUTSCHE WELLE, Dec. 12, 2010, http://www.dw.de/dw/article/0,,14729661,00.html (“They [the US] have not even appointed a negotiator.”) (quoting Reding). In January 2011, a Department of Commerce representative summarized
Given the breadth of developments in technology and usage of the Internet, and given the increasing globalization of Internet-based commerce, changes in the substantive standards for privacy appear almost inevitable.\textsuperscript{76} Thus, EU plans to revisit the data protection directive to improve harmonization within the European Union itself\textsuperscript{77} may offer a particularly good opportunity for such dialogue with US authorities.\textsuperscript{78}

At a minimum, US engagement of EU authorities can provide clarification of the EU view of the right to be forgotten.\textsuperscript{79} The development of a single EU standard for such a right could also provide greater certainty and predictability.
Substantive reconciliation of EU and US data protection law need not necessarily take on the full debate about freedom of expression versus privacy. Various minimalist solutions might emerge. For example, regulators in the European Union and United States could discuss the scope of the right to be forgotten, and at least agree on certain minimum standards in the area. Further, the discussions might include methods to support self-regulation (or “co-regulation”) to promote aspects of the right to be forgotten. The authorities might also address the specific form of

80. Industry Joint Statement On The Review Of The EU Legal Framework For Data Protection, Mar. 15, 2011 (European communications trade groups suggest that application of the EU Directive has not “resulted in the harmonised framework and level playing field necessary to establishing certainty for data controllers and individuals”); EuroISPA, Personal Data Protection in the EU, supra note 55, at 1 (noting that data protection “Directive has failed in creating a harmonized framework across the EU,” and calling for application of rules “horizontally,” to create a “level playing field”); Eric Pfanner, EU Seeks To Bolster Web Privacy; Data Protection Rules Will Be Updated With New Internet Services In Mind, INT’L HERALD TRIBUNE, Nov. 5, 2010, (“Technology companies have also been calling for an update of EU privacy rules . . . [because] there are too many different interpretations of existing legislation across the 27-country bloc.”); EU Wants To Give People Power To Vanish From Internet, AGENCE FRANCE PRESE, Nov. 4, 2010, http://www.eubusiness.com/news-eu/consumer-privacy.6sw (“The lack of harmonization of data protection rules creates enormous challenges for entrepreneurs who are trying to use emerging technologies to expand into new markets.”) (quoting Jona than Zuck, President of Association for Competitive Technology); Hill, supra note 64.

81. FTC Staff Comments, supra note 74, at 8 (noting that question of “international standards” for data protection and privacy presents “a highly complex and technical subject in which there remain significant unresolved political and policy debates”); id. at 9 (given “lack of consensus,” FTC supports “efforts to promote more consistency and inter-operability,” but suggests that “binding general international standards at this stage are premature”); EU Council Conclusions On Personal Data Protection, supra note 53, at 3, 5 (noting that protection of personal data transferred to countries outside the European Union is “one of the most complex issues in the course of the review” of the Directive; and suggesting that “development of universal principles” is “of utmost importance because of the globalised nature of data processing”).


83. See UK Advertising Association, supra note 55, at 4 (current cross-border data transfer regime is “not effective and is neither consistent nor business-friendly”) (suggesting “self-regulatory solutions” to “complement” legal framework); EFAMRO / ESOMAR, supra note 82, at 10 (“Self-regulation provides a level of detail and granularity that is impossible to achieve in national or supranational legislation and encourages sector-specific authoritative guidance and regulation.”); see also CTR. FOR DEMOCRACY & TECH., supra note 24, at 9 (suggesting use of “coregulatory approaches” to privacy governance in EU, as means to provide “international harmonization”); Ira S. Rubinstein, Privacy And Regulatory Innovation: Moving Beyond Voluntary Codes, Mar. 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1510275 (emphasizing value of Safe Harbor systems for promoting privacy protection). A large body of literature exists on the developing use of co-regulation in government. See, e.g., Peter S. Rank, Co-Regulation Of Online Consumer Personal
implementation of any right to be forgotten. Finally, to the extent that certain technical solutions (such as systems for auto-deletion of information) might address concerns underlying the right to be forgotten, regulators could (and should) discuss means to facilitate development and use of such technology.

84. Thus, for example, the European Union and the United States might agree on some form of “notice-and-takedown” of content approach, to shield website purveyors from unanticipated liability. See Center for Democracy & Technology, supra note 24, at 12 (“[A] person demanding takedown of content she did not create should be required to obtain a judicial or administrative determination that the content in question is illegal and should be removed.”); Cynthia Wong, Don’t Blame The Messenger, July 29, 2010, http://www.america.gov/st/democracyhr-english/2010/July/20100727142911enrehae0.9917871.html (noting use of “notice-and-takedown systems” to deal with copyright and other problems).

85. Systems of auto-deletion of information have been proposed. See Liam J. Bannon, Forgetting as “A Feature, Not a Bug”: The Duality of Memory and Implications for Ubiquitous Computing (2006), http://www3.unin.it/events/alpis06/download/prog/16_Bannon_2.pdf (suggesting that mechanisms of forgetting are of central concern to human psychology and that electronic tagging systems for information to “time-stamp material and contain something like a sell-by date” should be developed); Chris Conley, The Right to Delete 57 (2010), http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482 (“By building an expiration date into the content that we create, we could indeed address some of the privacy concerns that persistence presents.”); Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy & Henry M. Levy, Vanish: Increasing Data Privacy With Self-Destructing Data, PROCEEDINGS OF THE 18TH USENIX SECURITY SYMPOSIUM 299 (2009), http://vanish.cs.washington.edu/pubs/usenixsec09-geambasu.pdf; see generally Adam Thierer, Two Paradoxes of Privacy Regulation (Aug. 25, 2010), http://techliberation.com/2010/08/25/two-paradoxes-of-privacy-regulation/ (advocating “user-empowerment tools” as best means to protect privacy). The concept of auto-deletion has won supporters, both in the EU and in the US. See INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, Draft Resolution on Privacy Protection in Social Network Services 1, 3 (Oct. 17, 2008), http://www.justice.gov/ira/rdonlyres/F8A79347-170C-4EFF-A0AD-155554558A5F/24477/2008.pdf (“[I]t can be very hard – and sometimes even impossible – to have information thoroughly removed from the internet once it is published.”) (suggesting that providers of social network services should “allow users to easily terminate their membership, delete their profile and any content or information that they have published on the social network”); CTR. FOR DEMOCRACY & TECH., supra note 24, at 11 (Center “supports empowering individuals to delete data they themselves have created” but would strongly resist measures to “delete comments on other websites” as presenting “a high risk that one user’s right to be forgotten will unduly hamper others’ free expression rights and leave intermediaries with the difficult, potentially impossible, task of ‘dis-entangling’ individuals’ data”). Auto-deletion systems, however, may present certain technical problems for implementation. See Fleischer, supra note 14 (noting technical problems with auto-delete systems).

86. See EuroISPA, Personal Data Protection in the EU, supra note 55, at 1 (noting “it is important to address the impact that future innovations can produce on privacy through non-legislative measures, such as the use of privacy-enhancing technologies, privacy-by-design and industry self-
IV. RECONCILING EU AND US VIEWS OF JURISDICTION

Despite the progress to date, and prospects for additional efforts at harmonization, the fact remains that US and EU views of privacy protection (and the right to be forgotten, in particular) are currently in conflict. So long as such conflict exists, a significant procedural question arises: What is the scope of the jurisdiction of EU authorities to regulate and adjudicate the activities of actors operating outside the European Union, where some effects of that activity arguably arise within the European Union? In an inter-connected world, such a scenario inevitably arises. Effective enforcement of any right, including the regulation which are the most effective means to deal with fast-moving technology markets”), see generally Harry Surden, Structural Rights In Privacy, 60 S.M.U. L. Rev. 1605, 1629 (2007) (noting that changes in technology may have greater effects on society than changes in law); Steven C. Bennett, Government Options for Encouraging Use of On-Line Privacy-Enhancing Technologies, IAPP PRIVACY ADVISOR (Feb. 22, 2011), https://www.privacyassociation.org/publications/2011_03_01 government_options_for_encouraging_use_of_online_privacy-enhancing; Sonia Verma & Upvan M. Prakash, Jurisdictional Disputes and Intermediary Liability in Cyberspace, at 15 (Apr. 1, 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1800837 (drafting international agreements to regulate Internet is “complicated;” solution may appear in development of regulations by “Internet community”).

87. Uta Kohl, Jurisdiction and the Internet: Regulatory Competence over Online Activity 264-65 (2007) (national approaches to “privacy-encroaching or reputation-damaging” speech have produced a “diversity” of views such that “[x]substantive harmonization has not occurred” coupled with an “inherent resistance to making an external legal commitment” in the form of treaties or other agreements); Christopher Kuner, Data Protection Law and International Jurisdiction on the Internet, 18 Int’l J.L. & INFO. TECH. 176, 177 (2011) (noting that “while fundamental, high-level principles of data protection law are similar across regions and legal systems, the details of the law differ substantially” from one jurisdiction to another); Monique Altheim, The Review of the EU Data Protection Framework v. The State of Online Consumer Privacy in the US (Mar. 17, 2011), http://ediscoverymap.com/2011/03/the-review-of-the-eu-data-protection-framework-v-the-state-of-online-consumer-privacy-in-the-us/ (recent discussions in EU and US highlight how “very different” the two systems of data protection are).

88. Technically, questions of jurisdiction involve at least three separate issues: jurisdiction to prescribe, jurisdiction to adjudicate and jurisdiction to enforce. See generally RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 401 (1987). Even where a nation’s courts or regulators claim jurisdiction over a person or matter, conflicts may appear, in that the enforcement of any judgment rendered may require cooperation from the courts and authorities in other nations. See generally Yulia A. Timofeeva, Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis, 20 Conn. J. Int’l L. 199 (2005) (“There is no general obligation of states to enforce foreign judgments under international law”). As a result, concerns for comity and reciprocity of treatment may tend to encourage national authorities to harmonize their laws and regulations. See Reid, supra note 59, at 493 (noting concern that, “no matter how successful the mechanics of the Directive may be, weak regulation of such transnational transfers will render the provisions worthless when trying to guard online privacy”); see generally GARY BORN & DAVID WESTIN, INTERNATIONAL CIVIL LITIGATION IN UNITED STATES COURTS 564-604 (1989); Joel R. Reidenberg, Technology And Internet Jurisdiction, 153 U. Pa. L. Rev. 1951, 1958 (2005) (noting that international conventions on recognition of foreign judgments include exceptions where “the public order of the enforcing state” may be affected).

89. EuroISPA, Personal Data Protection in the EU, supra note 55, at 2 (“most frequent sce-
right to be forgotten, depends upon a system of jurisdiction that permits effective enforcement of that right. However, the problem of conflicting jurisdictions over Internet activity presents an enormous conundrum, which commentators have long recognized.

Traditionally, the exercise of jurisdiction was based on the concept of “sovereignty” over territory. Modern conflicts of law theory, however, recognizes the potential for expansion of jurisdiction based on the nationality of the defendant, protection of national interests, universal jurisdiction for offenses harmful to humanity, and the “passive personal” theory of adverse effects on a citizen subject to a state’s jurisdiction. In the essentially borderless region of cyberspace, the concept of sovereignty over specific physical territory becomes particularly problematic. Under these conditions, unless nations generally agree on a “law nario” in current environment is “collection and processing of data belonging to European citizens by extra-EU entities . . . Users now sit in a complex web of relationships with service providers often scattered around the world and sometimes operating from jurisdictions with non-compatible or non-existent data privacy legal frameworks”).

90. Sarudzai Chitsa, Name Calling on the Internet: The Problems Faced by Victims of Defamatory Content in Cyberspace, Paper No. 48, CORNELL LAW SCHOOL INTER-UNIVERSITY GRADUATE STUDENT CONFERENCE PAPERS (2011), http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1077&context=lps_clacp (noting potential “conflict of laws nightmare” in context of Internet content regulation); Rustad & Koenig, supra note 12 (quotation omitted) (“The global Internet’s legal environment makes it inevitable that one country’s laws will conflict with another’s—particularly when a Web surfer in one country accesses content hosted or created in another country.”); Timofeeva, supra note 88 (noting “heated” discussion regarding “multiple overlapping conflicting jurisdictions” claiming authority over Internet activities).

91. From the outset, US commentators recognized that the EU Directive presented challenges to US regulatory authorities. See generally Fred H. Cate, Data Protection Law and the European Union Directive: The Challenge for the United States, 80 IOWA L. REV. 431 (1995); see also Alexander Gigante, Ice Patch on the Information Superhighway: Foreign Liability for Domestically Created Content, 14 CARDOZO ARTS & ENT. L.J. 523 (1996); Kuner, supra note 87 (“While the fundamental, high-level principles of data protection law are similar across regions and legal systems, the details of the law differ substantially. Given these differences, it is not surprising that data protection law has been the subject of an increasing number of jurisdictional disputes, many of them involving [the European Union and the United States]”).


93. See United States v. Yunis, 681 F. Supp. 896 (D.D.C. 1988) (reviewing theories); Timofeeva, supra note 88, at 201 (quotation omitted) (although international law “sets little or no limit on the jurisdiction which a [particular] state may arrogate to itself[,]” several “established principles are more or less recognized in all jurisdictions”).

94. See Am. Libraries Ass’n v. Pataki, 969 F. Supp. 160, 168-69 (S.D.N.Y. 1997) (“The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent states that the actor never intended to reach and
of the Internet, a consistent, understandable “effects” standard of jurisdiction naturally becomes the most likely substitute for a strict “sovereignty” approach. An unlimited “effects” doctrine, however, could be used to justify virtually unlimited jurisdiction. Online intermediaries such as social networks and other facilitators of Internet content are “at the front lines” of this problem, as their content may be viewed from a computer anywhere on the planet.

The divergence of views on Internet-based jurisdiction appears in US case law and EU official pronouncements. To a large extent, US courts have fol-

possibly was unaware were being accessed. Typically, states’ jurisdictional limits are related to geography; geography, however, is a virtually meaningless construction on the Internet.

95. See generally David R. Johnson & David G. Post, Law and Borders – The Rise of Law in Cyberspace, 48 STAN. L. REV. 1367 (1996) (arguing for development of Internet law independent of individual countries). But see Frank H. Easterbrook, Cyberspace and the Law of the Horse, 1996 U. CHI. LEGAL F. 207 (1996) (suggesting no need exists for creation of separate law of the Internet); Timothy S. Wu, Cyberspace Sovereignty? – The Internet and the International System, 10(3) HARV. INT’L. & INFO. TECH. 647, 649 (1997) (arguing that Johnson and Post’s descriptive assumptions – “that the ‘territorial’ powers of the world will, or already do, respect an emergent cyberspace sovereignty” and that “state regulation of the Internet will be impossible or futile” – are incorrect) (“Internet regulation, although difficult, is possible and stands to become increasingly so regardless of its desirability on normative grounds”).

96. Bernhard Maier, How Has the Law Attempted to Tackle the Borderless Nature of the Internet?, 18(2) INT’L J. INFO. TECH. 142, 142 (2010) (regulations must address fact that actions may not physically take place in territory, but still have effects there).

97. Jessica R. Friedman, A Lawyer’s Ramble Down the Information Superhighway: Defamation, 64 FORDHAM L. REV. 794, 803 (1995) (defendants potentially liable for suit in every jurisdiction where access to defamatory content may be had from the Internet); Kulesza, supra note 94 (the fact of “enabling contents to be available within a certain territory cannot be [a] basis” for the exercise of the “prerogatives of the ruling sovereign;” rather, the “result of such [a] practice would be the ultimate insecurity of the Net”); Uerpmann-Wittzack, supra note 55, at 1256 (“[J]urisdiction based on an unqualified effects doctrine would not only infringe the sovereignty of other states, but it would also collide with the principle of Internet freedom.”); Policino & Bassini, supra note 52, at 9 (“[I]f the Internet makes websites accessible anywhere, and proper jurisdiction [arises] in any state where a harm occurs due to their contents, two paths are feasible: either the contents must comply with all the relevant jurisdictions where the website can be accessed, or access to such contents may be limited to those countries which has [sic] not outlawed them”).


100. See Toys “R” Us, Inc. v. Step Two, S.A., 318 F.3d 446, 452 (3rd Cir. 2003) (noting that
followed the reasoning in *Zippo Mfr. Co. v. Zippo Dot Com, Inc.*,101 in which the court referenced a “sliding scale” for determining whether Internet activity could form the basis for personal jurisdiction.102 At one end of the spectrum, according to the *Zippo* court, are situations where a defendant clearly does business over the Internet by entering into contracts with residents of a foreign jurisdiction.103 At the other end of the spectrum are situations where a defendant has simply posted information on an Internet site.104 In the middle are cases where an interactive website permits the user to exchange information with the host computer.105 In those cases, “the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs...”106 Although the *Zippo* test has not proved infallible in its application,107 its essential notion, that purely “passive” operation of a website should not form the sole basis for exercise of personal jurisdiction, seems relatively well established in US law.108

In contrast, EU interpretations on the reach of European privacy law (and


102. Id. (“[T]he likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet”).

103. Id. (jurisdiction is proper where contacts involve “knowing and repeated transmission of computer files over the Internet”).

104. Id. (“passive” website “does little more than make information available”).

105. Id.

106. Id.


related concepts such as defamation) appear to extend beyond the bounds of the prevailing US test for jurisdiction. 109 The EU Data Protection Directive (the “Directive”)110 adopted in 1995 does not expressly state that its provisions apply to the activities of non-EU entities111 but does purport to apply EU substantive law to any organization that uses means within the European Union to collect or process personal data.112 In 2000, the European Union issued a further directive “on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market,” which again did not expressly touch on the reach of EU jurisdiction.113 In 2002, the Article 29 Data Protection Working Party (the “Working Party”), an advisory group associated with the European Union, issued its “working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites.”114 The Working Party suggested that an online interaction between a website operator with no legal establishment in the European Union and an individual residing in the European Union may suffice to trigger coverage under EU data protection law.115 The full reach of this Working Party

109. Chen, supra note 107, at 436 (EU approach to Internet jurisdiction “markedly different” from US approach; EU is “highly regulatory”); id. at 445 (EU “country-of-destination” approach may be “overly broad and an unfair burden on [internet] sellers”).


111. See Lokke Moerel, Back To Basics: When Does EU Data Protection Law Apply?, 1 INT’L DATA PRIV. L. 92, 92 (2011) (“It is much debated when the data protection laws of the EU Member States apply in international situations. . . . The lack of guidance in the Directive on key concepts of applicable law and jurisdiction has lead to unacceptable differences in the manner in which the provision is implemented in the Member States.”); see generally Eleni Kosta, Christos Kalloniatis, Lilian Mitrou and Evangelia Kavakli, The “Panopticon” of Search Engines: The Response of the European Data Protection Framework, 15 REQUIREMENTS ENGINEERING 2 (2010) (noting “heated debate” among European privacy professionals on whether EU data protection framework applies to search engine providers that process data from outside the EU).


115. See id. at 15 (noting that the Working Party is convinced that a high level of protection of individuals can only be ensured if web sites established outside the European Union but using equipment in the European Union as explained in this working document respect the guarantees for
opinion has not been tested, but on a technical reading of the EU Directive, anyone who posts personal information about another person on his or her own social networking profile or uses personal information from another person’s profile could be deemed a “data controller” subject to the data protection obligations of the Directive. In that event, recognition of a “right to be forgotten” could have very broad consequences.

Indeed European case law tends to extend well beyond US views on the reach of jurisdiction, based on Internet activity. In substance, so long as actions on the Internet have known “effects” in a European state, EU courts (and, by implication, EU regulators) may exercise jurisdiction. In addition to the Yahoo! case, where a French court held Yahoo! responsible for permitting sale of Nazi-themed materials in France, and a host of other similar cases, in the personal data processing, in particular the collection, and the rights of individuals recognized at European level and applicable anyway to all web sites established in the European Union).

116. See Lokke Moerel, The Long Arm Of EU Data Protection Law: Does The Data Protection Directive Apply To Processing Of Personal Data Of EU Citizens By Websites Worldwide?, 1 Int’l Data Privacy L. 28 (2011) (“The conclusion is that the interpretation given by the Working Party is contrary to the legislative history of [the Data Protection Directive]. . . . Although the attempt of the Article 29 Working Party to provide protection to EU nationals is commendable, this result should be achieved by amendment of the applicability rule. . . .”); Wang, supra note 99, at 240 (“[T]here is still no clear indication of the creation of a special regime of jurisdiction rules for e-commerce cases. . . . Even if efforts were made to draft a specific regulation or convention, it would still take time and efforts to come into force.”); see also Kuner, supra note 87; Chen, supra note 107.

117. Daniel B. Garrie, Hon. Maureen Duffy-Lewis, Rebecca Wong & Richard L. Gillespie, Data Protection: The Challenges Facing Social Networking, 6 BYU Int’l L. & MGMT. REV. 127, 131-32 (2010) (to require “every user” to comply with Directive is “unrealistic objective”); id. at 133 (“impractical,” and “not customary” for users to “ask permission before posting another’s personal information, such as a photo or video”). The key under EU law, may turn out to be the extent to which information is accessible beyond a group of “self-selected contacts.” See id. at 143 (citing Sweden v. Lindquist, 2003 E.C.R. 1-12971 (holding that personal use exception to EU Directive does not apply where personal information is accessible by anyone on the Internet, rather than a limited number of self-selected contacts); Denis T. Rice, Jurisdiction Over Privacy Issues On The Internet, (Jul. 15, 2003), http://www.martindale.com/business-law/article_Howard-Rice-Nemerovski-Canady-Falk_17400.htm (“the notion of accessibility as the basis for jurisdiction is far from dead” in EU law, citing Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F.3d. 1199 (9th Cir. 2006)).


119. Chris Brunner, Territoriality As A Regulatory Technique: Notes From The Financial Crisis, 79 U. Cinn. L. REV. 101, 109 (2010) (“[R]egulators can assert jurisdiction extraterritorially wherever foreign companies engage in conduct that has effects in the country asserting jurisdiction; “this kind of strategy has been used to most spectacular effect” in EU antitrust actions); Marike Verme, Unfair Competition Online And The European Electronic Commerce Directive, 7 ANN. SURVEY INT’L & COMP. L. 87, 94-96 (2001) (noting that European law will often point to “lex loci delicti,” or “market” effects rule; these rules are not “effective,” as they permit “too many national laws” to apply).

120. See generally Timofeeva, supra note 88 (noting examples of cases in Germany, France and Italy, and suggesting that “the effects principle as applied in asserting jurisdiction in Internet content controversies is employed most broadly, capable to justify almost anything”).
recent criminal prosecution of Google executives in Italy,\textsuperscript{121} the Italian court held that, because at least some of the processing of information (a video of a child with Down’s Syndrome being abused by other youths) took place in Italy, the court could properly exercise jurisdiction. Thus, if “processing” of “personal data” through EU “equipment”\textsuperscript{122} includes a user’s downloading of Internet content somewhere in Europe,\textsuperscript{123} the European Union theoretically could exercise world-wide jurisdiction over Internet actors.\textsuperscript{124}

The disparity of views on the reach of jurisdiction over Internet-related activities can produce uncertainty, additional cost (in responding to varying standards) and unnecessary barriers to trade (as firms may be deterred from activities that place them at risk of regulation in unfavorable jurisdictions).\textsuperscript{125} In addition, the risk that judicial and administrative orders in one jurisdiction may not be enforced in other countries may tend to deter effective implementation of rules.\textsuperscript{126}

\begin{itemize}
\item \textsuperscript{121} Tribunale Ordinario di Milano, 24 febbraio 2010, Foro it. II 2010, 5, 279 (It.), http://speciali.espresso.repubblica.it/pdf/Motivazioni_sentenza_Google.pdf.
\item \textsuperscript{122} Christopher Kuner, \textit{Data Protection Law And International Jurisdiction On The Internet Part 2}, at 3, 2009, www.ssrn.com[Note: the link is temporarily down. I would say just leave it as this]. (EU concepts of “personal data” and “data processing” are “interpreted very expansively, which “increases their jurisdictional scope”).
\item \textsuperscript{123} See Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking 01189/09/EN WP 163 (June 12, 2009), ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (“The provisions of the Data Protection Directive apply to [social networking systems] providers in most cases, even if their headquarters are located outside of the EEA. The Article 29 Working Party refers to its earlier opinion on search engines for further guidance on the issues of establishment and use of equipment as determinants for the applicability of the Data Protection Directive and the rules subsequently triggered by the processing of IP addresses and the use of cookies”).
\item \textsuperscript{124} See Kuner, \textit{supra} note 122, at 3 (noting that EU use of “equipment” as basis for exercise of jurisdiction “most controversial,” because connection to the European Union may be very limited).
\item \textsuperscript{125} See Brummer, \textit{supra} note 119, at 112 (“extraterritorial regulation, even when justifiable, generates costs,” as foreign firms “must adjust to new standards or move to other jurisdictions to avoid a law’s regulatory effect;” extraterritorial regulation also “often erodes a country’s reputation in the international community;” as a result, other regulators and courts “may decide to refrain from cooperating with [the regulating country] or helping it achieve its strategic objectives,” as by refusing to enforce judgments); Kuner, \textit{supra} note 122, at 4 (jurisdictional uncertainties about data protection law “may dissuade individuals and companies from engaging in electronic commerce,” and may “impose burdens” on commerce); Timofeeva, \textit{supra} note 88 (prospect for assertion of worldwide jurisdiction “contributes to legal uncertainty”); Chen, \textit{supra} note 107, at 423 (“The unpredictability of jurisdiction makes it difficult for companies with web sites to limit their legal liability and inhibits the growth of e-commerce.”); Adam Thierer & Clyde Wayne Crews, Jr., \textit{Everybody Wants To Rule The Web} (Dec. 17, 2003), http://www.cato.org/pub_display.php?pub_id=3343 (noting that “patchwork” of international law may be “confusing, costly, and technically impossible for all but the most well-heeled firms” to navigate).
\item \textsuperscript{126} See Chris Reed, \textit{Think Global, Act Local: Extraterritoriality in Cyberspace} (2010), papers.ssrn.com/sol3/papers.cfm?abstract_id=1620129 (“A state is unlikely to attempt to enforce its laws against foreign defendants where it is known that their home country will probably refuse to enforce a judgment”). In such instances, however, both jurisdictions have an interest in developing a solution, to promote “comity” (equal treatment of laws) between nations. See \textit{Restatement (Third) Of Foreign Relations Law Of The United States, § 403(1) (1987)} (noting that comity
Ideally, the United States and the European Union could develop some form of an agreed international standard on jurisdiction. But even if agreement upon a general standard is impossible, or at least unlikely to develop in the immediate future, the United States and the European Union could still achieve less ambitious improvements in international understanding. Recently, for example, the EU Article 29 Working Party issued an opinion on “applicable law” under the EU Directive, which suggested that “additional criteria” should be developed to determine when EU data protection law applies to a “controller established outside the EU. . . .” The Working Party suggested that these criteria could include the “targeting” of individuals within the European Union.

The notion of “targeting” as a standard for the exercise of jurisdiction has relatively wide support among commentators. US courts have developed ex-
perience in applying such a standard and, to a lesser extent, the notion is recognized in the European Union. Furthermore, both US and EU courts are likely to agree that, on an intuitive level, a country almost certainly enjoys jurisdiction over the “territory” of its top-level Internet domain. Courts can also recognize other indicia of “targeting,” such as language, specific content and references to the particular country. The International Organization of Securities Commissions adopted just such a test for national jurisdiction over securities offerings. In the United States, the FTC applies similar standards in determining whether websites are addressed at children. A further example appears in the EU Convention on Cybercrime. Such standards, of course, rely to some


131. Haynes, supra note 100, at 159-60 (noting that many US courts have added a “targeting” element to the Zippo test, which provides “a means of focusing on a defendant’s action—those directed toward a particular jurisdiction, rather than actions directed at all jurisdictions simultaneously”); Timofeeva, supra note 88 (noting that targeting-based analysis is “not a novel doctrine,” although, in the Internet setting, “the United States alone favors its application”); Reidenberg, supra note 88, at 1955 (US courts “have looked to online targeting and to deleterious effects within the forum to determine if personal jurisdiction is appropriate”). The issue of targeting has also arisen in US First Amendment jurisprudence. See United States v. Playboy Entertainment Grp., 529 U.S. 803, 804 (2000) (“[T]he Government cannot ban speech if targeted blocking is a feasible and effective means of furthering its compelling interests”).


133. Uerpmann-Wittzack, supra note 55, at 1258 (suggesting that countries may “assert full jurisdiction” over matters within their own “top level domain,” which “becomes a state’s territory in cyberspace”); Timofeeva, supra note 88 (noting “authority of a country to administer its own Country-Code Top-Level Domain”) (“[T]he manager of the German ccTLD ‘.de’ would not register the domain name http://www.heil-hitler.de or the like”).

134. See supra notes 128-129 (Article 29 Working Party suggestions for targeting criteria); see generally Matthew L. Perdoni, Revising The Analysis Of Personal Jurisdiction To Accommodate Internet-Based Personal Contacts, 14 U.D.C. L. REV. 159 (2011).

135. Factors include: whether the offeror accepts orders from or provides services to residents in the jurisdiction, whether the offeror uses email or other media to “push” information to residents, and (contrariwise), whether the offeror clearly states that it does not intend to make an offering in specific jurisdictions. See IOSCO, Securities Activities On The Internet (1998), http://www.iosco.org/library/pubdocs/pdf/IOSCOPD83.pdf; IOSCO, Securities Activities On The Internet II (2001), http://www.iosco.org/library/pubdocs/pdf/IOSCOPD120.pdf.

136. See FTC, What Determines Whether Or Not A Website Or Online Service Is Directed To Children?, http://www.ftc.gov/privacy/coppafaqs.shtm (FAQ section) (factors may include subject matter, language, use of animated characters, and whether advertising appeals to children).

degree on subjective and ambiguous factors\textsuperscript{138} and may introduce new complications.\textsuperscript{139} But a workable standard is at least theoretically possible.\textsuperscript{140}

Similarly, the development of “geo-location” technologies for the Internet potentially opens the way to development of new standards for jurisdiction.\textsuperscript{141} Website purveyors often tailor their content to specific markets and use geolocation technology to assist them in delivering targeted messages.\textsuperscript{142} Indeed,
technologies for location identification, based on Internet usage, mobile device usage, or both, may offer tremendous opportunities for “personalization of services and contextualization of information.” These geo-location technologies have their limits, of course. Such technologies, sometimes used to establish “content zoning,” present serious privacy concerns, may adversely affect innovation, may unduly place burdens on Internet intermediaries, and have

formation on the Internet becoming steadily weaker, as technology advances); Timofeeva, supra note 88, at 220 (“Various tools exist to identify the geographical location of the user and many companies routinely employ these tools for targeted advertising purposes.”).


144. See Justice S. Muralidhar, Jurisdictional Issues In Cyberspace, 6 INDIAN J. L. & TECH. 1, 3 (2010) (“Even while it was thought that one could fix the physical location of the computer from where the transaction originates and the one where it ends, that too can be bypassed or ‘masked’”).

145. See Yulia A. Timofeeva, Establishing Legal Order in the Digital World: Local Laws and Internet Content Regulation, 1 J. INT’L COMMERCIAL L. 41, 43 (2006) (content “zoning” consists of technical procedures to “direct information flows to particular users only; “[m]etaphorically, it can be described as creating zones in cyberspace that are open for some categories of users and closed for others”).


148. Etienne Montero & Quentin Van Enis, Enabling Freedom of Expression in Light of Filtering Measures Imposed on Internet Intermediaries: Squaring the Circle?, 27 COMPUTER L. & SEC. REV. 21 (2011) (“It is not always simple to identify the authors of illegal or harmful content in an open digital environment, global in scale, where it is easy to operate from abroad and/or anonymously. On the other hand, intermediary providers involved in transmitting or storing the disputed content
been used in some instances in the service of government repression. At least in theory, such concerns could be addressed by a jurisdictional standard that also considers whether the use of geo-location technology is mandatory or merely permissible. Concerns regarding geo-location technology may also be addressed via the development of appropriate technology.

V. CONCLUSION

Despite cultural divisions between the European Union and the United States on the substance of privacy rights and the reach of jurisdiction over Internet

are known and clearly identified, close to the victim, and generally solvent.”); Mark MacCarthy, What Internet Intermediaries Are Doing About Liability and Why It Matters, 25 BERKELEY TECH. L.J. 1039 (2010) (noting examples of implementation of Internet regulations through payment intermediaries).

149. Laura DeNardis, The Emerging Field of Internet Governance, Yale Info. Soc. Working Paper at 11, Sept. 17, 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678343 (“Freedom of expression and association are increasingly exercised online and institutional, governmental, and private decisions about Internet architecture can determine the extent of these freedoms as well as the degree to which online interactions protect individual privacy and reputation. . . . Technical measures such as content filtering, digital rights management techniques, and blocking access to web sites are techniques that repressive governments can use to ‘govern’ the flow of information on the Internet.”); Jessica E. Bauml, It’s a Mad, Mad Internet: Globalization and the Challenges Presented by Internet Censorship, 63 FED. COMM. L.J. 697 (2010) (reviewing censorship problems associated with Internet technologies that permit identification of location of Internet users). But see Patricia Moloney Figliola, Casey L. Addis & Thomas Lum, U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy and Technology, CRS Rep. 7-5700 at Appendix B, Apr. 5, 2011, http://fpc.state.gov/documents/organization/140637.pdf (listing and explaining technical means to circumvent government censorship of web-based communications, including use of proxy servers).

150. Reidenberg, supra note 88, at 1956 (suggesting that website purveyor may be “purposely availing” itself of entry into jurisdiction “whenever content is posted without geolocation filtering”); Adam D. Thierer & Clyde Wayne Crews Jr., Internet Libel Ruling: Talk About a Kangaroo Court, Dec. 16, 2002, http://www.cato.org/publications/techknowledge/internet-libel-ruling-talk-about-kangaroo-court (suggesting that Internet vendors and publishers may be able to avoid confrontations with foreign courts and regulators by “using new geographic location technologies to better target their services instead of just blasting their materials out to the planet”).

151. On one view, if a website purveyor makes use of geo-location technology to target specific countries, it may be subject to jurisdiction. See Henn, supra note 140, at 175 (“[A] web site that uses software technology to target advertising toward the specific user should also be considered to have submitted to the jurisdiction of the specific user”). On another view, if a website purveyor does not use geo-location technology to exclude specific countries, then it might be subject to general jurisdiction in all countries. See Reidenberg, supra note 88, at 1959 (“[M]ore sophisticated computing enlists the processing capabilities and power of users’ computers. This interactivity gives the victim’s state a greater nexus with offending acts and provides a direct relationship with the offender for purposes of personal jurisdiction and choice of law”).

net-related activities, a process of “convergence” in views seems almost inevitable.153 The means for implementing consensus views on subjects such as the right to be forgotten may vary according to the perceived needs and political practicalities of the two regions.154 Often, consensus is best developed, at least in the first instance, through “soft law” guidelines.155 Such guidelines may permit experimentation, feedback, and revision to respond to developments in technology and business practices.156

The Internet and regulations surrounding it have matured greatly over the past generation.157 The wide range in types of data transfers across international borders that occur daily might give rise to different problems that require differ-

153. See Reed, supra note 126, at 6 (noting “natural process of convergence” in international law, supported by a “desire to achieve the benefits of global communication and commerce,” and developed in part through comparisons between laws, where one country may use another’s law as a “template” for parallel legislation). The “convergence” process, however, can be lengthy, “particularly for new and fast-moving areas of technology like cyberspace.” Id. at 7; see also, Gehan Gunasekara, The “Final” Privacy Frontier? Regulating Trans-Border Data Flows, 17 INT’L J. L. & INFO. TECH. 147, 149 (2007) (“Despite significant convergence in global information privacy norms, the difficulties resulting from trans-border data flows represents a further concern insuffi- ciently dealt with by existing privacy norms”).


155. See Andrew Power & Oisin Tobin, Soft Law for the Internet, Lessons from International Law, 8 SCRIPT-ED 1, 32, 35 (2011) (“soft law consists of those informal rules that are non-binding, but, due to cultural norms or standards of conduct, have practical effect;” “[s]oft law offers an effective way to deal with uncertainty, especially when it initiates processes that allow actors to learn about the impact of agreements over time;” areas in the international arena where a soft law approach has worked include forestry, labor rights and sustainable development); François Nawrot, Katarzyna Syska & Przemyslaw Switalski, Horizontal Application of Fundamental Rights: Right to Privacy on the Internet, May 2010, http://en.zpc.wpia.uw.edu.pl/wp-content/uploads/2010/04/9_Horizontal_Application_of_Fundamental_Rights.pdf (1980 OECD guidelines, outlining “core principles to protect privacy and personal data,” which are considered “soft-law”).


157. See John Palfrey, Four Phases of Internet Regulation, 77 SOC. RES. 3 (2010) (tracing development of Internet regulation, from “open” Internet to today’s structure, where “access [may be] contested” by regulators and private parties); Debra L. Spar, Ruling the Waves: Cycles Of Discovery, Chaos, and Wealth from the Compass to the Internet (2001) (noting sequence of innovation, commercial exploitation, creative anarchy, and eventual government regulation, in systems of new technology, including the Internet).
ent solutions at different times. In the end, an approach to regulation based on careful attention to technology and business developments, coupled with genuine respect for cultural differences, is most likely to produce satisfactory, workable international solutions. Inaction, however, is not an option as the conflict has already manifested itself in the tensions that exist between the approach to regulation taken in the European Union and the approach taken in the United States.


159. Cass R. Sunstein, Constitutional Caution, 1996 U. CHI. LEGAL F. 361, 374-75 (1996) (“In [periods] of rapid change and technological uncertainty, in which those schooled in law are likely to be ignorant, there is much room for tentative, narrow judgments.”)


161. See Frayer, supra note 10 (“These problems will absolutely continue to come up, until one of two things happens: either the technology companies begin to build architectures that enable compliance with existing law, or the law begins to change.”) (quoting Joel Reidenberg of Fordham Law School).
VI.

POST SCRIPT

As this Article went to press, the European Commission (the executive body within the European Union) issued a proposal to revise the 1995 EU Data Protection Directive. The proposal included a provision for recognition of the “right to be forgotten.”162