Berkeley Journal of International Law

Volume 30 | Issue 1 Article 4

2012

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

Steven C. Bennett

Recommended Citation

Steven C. Bennett, *The "Right to Be Forgotten": Reconciling EU and US Perspectives*, 30 Berkeley J. Int'l Law. 161 (2012).
Available at: http://scholarship.law.berkeley.edu/bjil/vol30/iss1/4

Link to publisher version (DOI)
http://dx.doi.org/doi:10.15779/Z38V08Z

This Article is brought to you for free and open access by the Law Journals and Related Materials at Berkeley Law Scholarship Repository. It has been accepted for inclusion in Berkeley Journal of International Law by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact jcera@law.berkeley.edu.

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.

1. *See* Peter Hustinx, *The Strategic Context and the Role of Data Protection Authorities in the Debate on the Future of Privacy*, Apr. 29, 2010 (EU Data Protection Supervisor notes that Reding has "made data protection her top priority"), *available at* http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Future_Pricacy_EN.pdf; *see also Q&A: Viviane Reding*, Mar. 27, 2006 (interview, summarizing Reding's background and interests), *available at* http://www.egovmonitor.com/node/5302. Reding is well known for brokering a deal with various social networking providers to adopt "Safer Social Networking Principles" for their operations in the EU. *See* Felix Hofer, *Privacy Issues in Social Networking: The European Perspective*, Mar. 21, 2010, *available at* http://www.mondaq.com/article.asp?articleid=95756.

Published by Berkeley Law Scholarship Repository, 2012

mation."[2] 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."[3]

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."[4] This "comprehensive" new legal framework would be subject to negotiation between the European Parliament and the European Council of Ministers.[5] 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."[6] 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. . . ."[7] Similar EU

---

2. *See* Press Release, June 22, 2010, (text of Reding speech), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/327.

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.*; s*ee 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.

4. *See Data Protection Reform –Frequently Asked Questions,* Nov. 4, 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/542; *see also EU Publishes Draft Strategy to Strengthen Data-Protection Laws,* Nov. 5, 2010 (EU "has been targeting a strengthening of privacy laws for some time and says strong data legislation will help boost business and consumer confidence across the bloc"), *available at* http://www.i-policy.org/2010/11/eu-publishes-draft-strategy-to-strengthen-data-protection-laws.html.

5. *See European Commission, Communication from the Commission to the European Parliament, the Council, The Economic and Social Committee and the Committee on the Regions, A Comprehensive Approach on Personal Data Protection in the European Union*, Nov. 4, 2010 [hereinafter Comprehensive Approach on Personal Data Protection] (EU launched review of legal framework in Data Protection Directive in 2009 and has "confirmed that the core principles of the Directive are still valid," but determined that several "problematic" challenges must be addressed, including "the impact of new technologies," "[e]nhancing the internal market dimension of data protection," addressing "globalization and improving international data transfers," and providing "a stronger institutional arrangement for the effective enforcement of data protection rules"), *available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

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.

DOI: doi:10.15779/Z38V08Z

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-

---

the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period [for data] has expired." *Id.* at 8.

8. *See, e.g.*, Viviane Reding, *Speech-Brussels,* Nov. 30, 2010 ("[I]ndividuals need to be able to maintain control over their data. This is particularly important in the [online] world . . . . I want to introduce the 'right to be forgotten.' Social network sites are a great way to stay in touch with friends and share information. But if people no longer want to use a service, they should have no problem wiping out their profiles. The right to be forgotten is particularly relevant to personal data that is no longer needed for the purposes for which it was collected. This right should also apply when a storage period, which the user agreed to, has expired."), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700; *see also* Viviane Reding, *Speech – Brussels*, Mar. 16, 2011 (discussing how the "right to be forgotten" includes "a comprehensive set of existing and new rules to better cope with privacy risks online. When moderni[z]ing the [EU privacy] legislation, I want to explicitly clarify that people shall have the right – and not only the 'possibility' – to withdraw their consent to data processing. The burden of proof should be on data controllers – those who process your personal data. They must prove that they need to keep the data rather than individuals having to prove that collecting their data is not necessary."), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183; *see also* Steve Olenski, *You Have the Right to be Forgotten Online*, Mar. 24, 2011 ("Maybe you've been at a party, up until four in the morning and you or someone you know posts photos of you. Well, it's a harmless bit of fun, but being unable to erase this can threaten your job or access to future employment.") (quoting spokesman for Reding), *available at* http://socialmediatoday.com/steve-olenski/280649/you-have-right-be-forgotten-online ; *see also* uTRUSTit, *Legal Requirements For Trust In The IoT [Internet of Things]* at 26 (Apr. 12, 2011) (report co-funded by European Commission) ("To counter what can be referred to as the perpetual memory of the [I]nternet, one could think of a right to be forgotten as a complement to the right to privacy, traditionally referred to as the 'right to be let alone.' Such would enable the data subject to personally determine that their data is no longer processed and deleted when they are no longer needed for legitimate purposes.").

9. Viviane Reding, *Speech – Brussels*, Mar. 16, 2011 ("Any company operating in the EU market or any online product that is targeted at EU consumers must comply with EU rules. For example, a US-based social network company that has millions of active users in Europe needs to comply with EU rules. . . . To enforce the EU law, national privacy watchdogs shall be endowed with powers to investigate and engage in legal proceedings against non-EU data controllers whose services target EU consumers."), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183.

10. *See* Greg Sterling, *Google Confronting Spain's "Right to be Forgotten",* Mar. 8, 2011 (giving example of Spanish surgeon who was featured in critical newspaper profile in 1991; where dispute with patient was resolved, but news story remained available on the Internet), *available at* http://searchengineland.com/google-confronting-spains-right-to-be-forgotten-67440; *see also* Greg Sterling, *Spanish Want Google to Police Libel on the Internet*, Jan. 17, 2011, http://searchengineland.com/spanish-want-google-to-police-libel-on-the-internet-61418; Lauren

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-

---

Frayer, *In Madrid Court, Google Challenges Europe's Privacy Laws*, Feb. 1, 2011 (noting that Spanish authorities filed 90 court orders against Google, based on the "derecho al olvido," the right to be forgotten), *available at* http://www.voanews.com/english/news/In-Madrid-Court-Google-Challenges-Europes-Privacy-Laws-115012364.html; Ciaran Giles, *Internet "Right To Be Forgotten" Debate Hits Spain*, Apr. 20, 2011 (noting that Spanish national court has asked EU Justice officials to provide advice on the cases), *available at* http://www.boston.com/news/world/europe/articles/2011/04/20/internet_right_to_be_forgotten_debate_hits_spain/.

11. *See* Greg Sterling, *Italy to Regulate YouTube & Other Video Sites Like TV Stations*, Jan. 3, 2011 (Italian authorities noting potential liability for any content appearing on a website), *available at* http://searchengineland.com/italy-to-regulate-youtube-other-video-sites-like-tv-stations-60098.

12. *See* 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; David Kravets, *Convicted Murderer Sues Wikipedia, Demands Removal Of His Name*, Nov. 11, 2009 (The plaintiffs reportedly prevailed in their suits against some German publishers, although not against Wikimedia), *available at* http://www.wired.com/threatlevel/2009/11/wikipedia_murder/; *see The "Right To Be Forgotten," Germany, and the Wikimedia Case*, Feb. 2, 2011 (summarizing developments in several German cases), *available at* http://www.pogowasright.org/?p=20228. For a Wikipedia account of the cases, *see Wolfgang Werle and Manfred Lauber*, http://en.wikipedia.org/wiki/Wolfgang_Werl%C3%A9_and_Manfred_Lauber. This sense of the "right to be forgotten" is apparently well-established in certain elements of European law. *See* Martine Herzog-Evans, *Judicial Rehabilitation in France: Helping with the Desisting Process and Acknowledging Achieved Desistance*, 3 EURO. J. OF PROBATION 4, 10 (2006) (noting "strong" element of French legal culture, recognizing a "droit a l'oubli," or "right to be forgotten," as a means to aid rehabilitation). For descriptions of additional European cases on the obligation of Internet service providers to remove defamatory material promptly, *see* Michael L. Rustad & Thomas H. Koenig, *Harmonizing Cybertort Law for Europe and America*, 5 J. HIGHTECH. L. 13 nn. 9, 193-97 (2005).

13. *See* Danny Sullivan, *Italian Court Finds Google Execs Guilty of Violating Privacy Code*, Feb. 24, 2010, http://searchengineland.com/italian-court-finds-google-execs-guilty-of-violating-privacy-code-36813; *see also* Joshua Sibble, *Recent Developments in Internet Law*, 23 INTELL. PROP. & TECH. L.J. 12 (2011) (noting that case is on appeal and has been "widely criticized").

14. *See* Peter Fleischer, *Foggy Thinking About The Right To Oblivion*, Mar. 9, 2011 (Google global privacy counsel suggests that right to be forgotten may be "used to justify censorship"), *available at* http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html; *see also* Tessa Mayes, *We Have No Right To Be Forgotten Online*, Mar. 19, 2011 (UK commentator

DOI: doi:10.15779/Z38V08Z

sistent with fundamental US values (such as freedom of expression and of the press).[15] 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.[16] Others suggested that the EU approach could create a property right in information (which otherwise does not exist),[17] and pro-

---

suggests "[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.internetevolution.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,"[18] which might interfere with "business demands" for data.[19]

Yet, some US commentators appeared more receptive to at least a limited version of the right to be forgotten.[20] Some, for example, suggested that children

---

ing that right to be forgotten turns in part on "[w]ho actually owns the data collected by online sites and services"), http://techliberation.com/2011/04/19/an-internet-eraser-button-to-protect-privacy-unwise-probably-impossible/. In general, as one commentator has noted, "much of the current electronic publishing legal landscape remains an unsettled and uncertain frontier." Lateef Mtima, *Tasini And Its Progeny: The New Exclusive Right Or Fair Use On The Electronic Publishing Frontier?*, 14 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 369, 373 (2004); Jed Scully, *A Conversation And Colloquia Concerning "Who Owns Your Digital Creations?"*, 35 MCGEORGE L. REV. 179 (2004) (noting "cataclysmic effect" of web publishing on "settled notions of property, jurisdiction, national borders and boundaries").

18. *See* Greg Sterling, *Google Confront Spain's "Right To Be Forgotten"*, Mar. 8, 2011 ("The EU should tread carefully so as not to create a bureaucratic nightmare where individuals, and by extension, companies could exercise censorship over what appears about them online and in search results. On balance, the 'right to know' (especially where entities and public figures are involved) should trump the novel 'right to be forgotten.'"), http://searchengineland.com/google-confronting-spains-right-to-be-forgotten-67440.

19. *See Internet Privacy And The "Right To Be Forgotten",* Mar. 19, 2011 (Reding proposals will "cause concern in parts of the United States, where many of the biggest and most successful search engines and social media companies are based;" noting that "Europe and the [US] have traditionally differed on privacy issues, with the EU taking a stronger approach and US officials more mindful of the need to balance entrepreneurship and business demands with data protection"), http://www.thefreelibrary.com/Internet+privacy+and+the+%22right+to+be+forgotten%22.-a0251824741; Adam Thierer, *The Conflict Between A "Right To Be Forgotten" & Speech/Press Freedoms*, Nov. 5, 2010 ("Enshrining a "right to be forgotten" into law would necessitate a fairly significant expansion in the rules and regulations governing information sectors and actors. Enforcement would certainly be challenging. As always, there is no free lunch, something has to give."), http://techliberation.com/2010/11/05/the-conflict-between-a-right-to-be-forgotten-speech-press-freedoms/.

20. *See* Valentina Pop, *EU To Press For "Right To Be Forgotten" Online*, Nov. 4, 2010 ("Privacy experts and consumer rights' groups were thrilled at the [EU] proposal."), http://euobserver.com/851/31200. There is extensive psychological and other literature on the means by which "[d]redging up the past can hurt feelings, stir negative emotions, and ruin lives." *See* Anita L. Allen, *Dredging Up The Past: Lifelogging, Memory And Surveillance*, 75 U. CHI. L. REV. 47, 58 (2008) (citing literature). These problems only grow larger, as data grows in volume, and low-cost memory and search techniques make such data increasingly available. *See* Sheila Molnar, *Privacy, Surveillance, And The Persistence Of Data*, Apr. 27, 2009 (society may be close to "total surveillance," where "piles of data will eventually become one collective intelligence) (citing IBM data expert Jeff Jonas), http://www.sqlmag.com/article/data-management/privacy-surveillance-and-the-persistence-of-data; Lauren Gelman, *Privacy, Free Speech, And "Blurry Edged" Social Networks*, 50 B.C. L. REV. 1315, 1318 (2009) ("Most information on the Internet is captured, indeed, saved, and searchable."); Andrew Haberman, *Policing The Information Super Highway: Custom's Role In Digital Piracy*, 2 AM. U. INTELL. PROP. BRIEF 17 (Summer 2010) ("Today, anyone can look virtually anywhere to find virtually anything on the virtual marketplace of the web, shifting the economic power from the sellers to the masses."). Increasing indifference to privacy concerns, at least in certain segments of the population, may also have an effect. *See* Daniel Solove, *The Future Of Reputation: Gossip, Rumor, And Privacy On The Internet* 5-6 (2007) (summarizing privacy impacts of Internet social networking); Jenn Web, *The Truth About Data: Once It's Out There, It's Hard To Control*, Apr. 4, 2011 (noting trend that "involves the willingness of consumers to give up all kinds of personal data in return for some benefit—free email or a fantastic social network site") (quoting

DOI: doi:10.15779/Z38V08Z

should have the ability to erase information posted improvidently, out of youthful lack of judgment.[21] 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.[22] Still others noted that the concept of "forgive and forget" embodies a fundamental human value,[23] 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-

---

Jeff Jonas of IBM), http://radar.oreilly.com/2011/04/jeff-jonas-data-privacy-control.html.

21. *See Common Sense Media Calls For New Policy Agenda To Protect Kids And Teens' Privacy Online*, Dec. 2, 2010 (calling for an "erase button," so that "parents and kids should be able to delete online information"), http://www.commonsensemedia.org/about-us/news/press-releases/common-sense-media-calls-new-policy-agenda-protect-kids-and-teens-priva; David Zax, *Will There Ever Be An "Internet Erase Button?"*, Apr. 27, 2011 (suggesting that regulation might be appropriate where "personal information [is] voluntarily submitted to websites," or where information is posted by children; in those cases, "the calls for an erase button seem reasonable"), http://www.technologyreview.com/blog/helloworld/26700/.

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-brookman/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-appli (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-doit-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-SCHÖNBERGER, 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.").

ten."[24]

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.[25] To some degree, those differences remain unresolved.[26] The European Union generally adheres to a high degree of government involvement in protection of this fundamental right.[27] US privacy law has,

---

24. *See Comments to the European Commission in the Matter of Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union*, CTR. FOR DEMOCRACY & TECH. (Jan. 15, 2011), http://ec.europa.eu/justice/news/consulting_public/0006/contributions/not_registered/nhs_en.pdf (in context of "passive data sharing," right to be forgotten already exists in US law) (citing Fair Credit example); Jean-Francois Blanchette & Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 18 THE INFO. SOC'Y 1, 4 (2002) ("[T]he U.S. has traditionally understood itself to be a place where individuals could get a 'second chance.'") (referencing bankruptcy law, juvenile crime records, and credit reporting as examples of US policies that embody "forgetfulness" as a value); Viktor Mayer-Schönberger, *Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing,* (Harvard Belfar Ctr. for Sci. & Int. Aff.Working Paper RWP07-022, 2007), http://belfercenter.ksg.harvard.edu/publication/3083/useful_void.html (suggesting need for "a simple rule that reinstates the default of forgetting our societies have experienced for millennia"); Martin Dodge & Rob Kitchin, *'Outlines of a World Coming into Existence': Pervasive Computing and the Ethics of Forgetting*, 34 ENV'T & PLAN. 431 (2007) ("Rather than seeing forgetting as a weakness or a fallibility . . . it is an emancipator process that will free pervasive computing from burdensome and pernicious disciplinary effects").

25. Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU, and Canada: The Allure of the Middle Ground,* 2 U. OTTOWA L. & TECH. J. 357 (2005); David L. Baumer, Julia B. Earp & J.C. Poindexter, *Internet Privacy Law: A Comparison Between the United States and the European Union*, 23 COMPUTERS & SEC. 400, 411 (2004) ("Compared with the EU . . . there is far less legal protection of online privacy in the US."); Steven R. Salbu, *The European Union Data Privacy Directive and International Relations*, 35 VAND. J. TRANSNAT'L L. 655, 665 (2002) (describing EU versus US philosophies and approaches to privacy); Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 718 (2001) (noting "clash" between the European Union and the United States "over the protection of personal information").

26. *See* Eric Pfanner, *G-8 Leaders to Call for Tighter Internet Regulation*, N.Y. TIMES (May 24, 2011), http://www.nytimes.com/2011/05/25/technology/25tech.html (noting debate at G-8 meeting on how best to balance privacy and other rights with an open Internet structure); *Internet Freedom Will Lead to Anarchy, Claims Sarkozy in Extraordinary Outburst*, May 25, 2011, THE DAILY MAIL, http://www.dailymail.co.uk/sciencetech/article-1390610/Mark-Zuckerberg-Facebook-going-children.html (noting "deep rifts" in views of policymakers and Internet executives at G8 meeting, and "deep" cultural differences between American and European approaches).

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-

DOI: doi:10.15779/Z38V08Z

by contrast, largely developed in a "patchwork," with a "reactive" array of state and federal statutes and common law doctrines.[28] The United States, moreover, has traditionally emphasized freedom of expression over privacy, as a fundamental value.[29]

Some suggest that a right to be forgotten simply cannot exist in the United States.[30] 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.[31] 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.[32] 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."[33]

---

formation as "public"); W. Kuan Hon, Christopher Millard & Ian Walden, *The Problem of "Personal Data" in Cloud Computing—What Information is Regulated?*, SOC. SCI. RESEARCH NETWORK (Apr. 13, 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577 (definition of data "processing" under EU Directive is "very broad").

28. *See* Horace A. Anderson, *The Privacy Gambit: Toward a Game Theoretic Approach to International Data Protection*, VAND. J. ENT. & TECH. L. 1, 17-18 (2006); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

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").

30. *See* Franz Werro, *The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash* 286 (Georgetown Ctr. for Transnat'l Legal Studies Research Paper No. 2, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357 (suggesting that "the right to be forgotten is unprotected" in the United States); *id.* at 298-99 (noting "fairly dramatic transatlantic schism in the law of privacy," regarding right to be forgotten, and explaining cultural and historical sources of divergence).

31. US views on the importance of privacy protection have changed greatly in recent years. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 101, 105-06 (2011) (noting "profound transformation" in corporate privacy management efforts in the United States in past 15 years, resulting from consumer expectations, and the "rise" of the Federal Trade Commission ("FTC") as an "activist privacy regulator").

32. *See* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

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*,[34] 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.*,[35] 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.[36] 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.[37] In

---

Internet Street-Level Mapping Technologies Demand Reconsideration of the Modern-Day Tort of 'Public Privacy', 43 GA. L. REV. 604 (2009); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, SOC. SCI. RESEARCH NETWORK (Nov. 2004), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=629283 (question of what is "private" information cuts across many areas of American law, including Fourth Amendment, trade secrets, patents, evidence, the constitutional right of information of information privacy, and the Freedom of Information Act); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure*, 53 DUKE L.J. 967, 976 (2003) ("Even in the current age, when information is king, sometimes less access to information is the soundest policy choice").

34. 297 P. 91 (Cal. Ct. App. 1931).

35. 483 P.2d 34 (Cal. 1971).

36. *See*, *e.g.*, Gates v. Discovery Comms., Inc., 101 P.3d 552 (Cal. 2004) (corporation not liable to offender for publishing facts obtained from public records); Wilan v. Columbia County, 280 F.3d 1160, 1163 (7th Cir. 2002) (noting that "the *Melvin* case, paternalistic in doubting the ability of people to give proper rather than excessive weight to a person's criminal history, is dead"); Ostergren v. McDonnell, 643 F. Supp. 2d 758 (E.D. Va. 2009), (permitting republication of public documents containing sensitive information), *rev'd,* Ostergren v. Cuccinelli, 615 F.3d 263 (4th Cir. 2010); *see generally* ALLEN, *supra* note 20 ("Current 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. The First Amendment and the common law mandate wide freedom for speaking truth, accurate news reporting and artistic expression."); Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. L. 73, ¶ 21 (2007) (in US, "causes of action that primarily protect one's reputation, dignity, or privacy . . . have traditionally been both anemic and anomalous"). A variety of concerns other than the First Amendment may also affect views on the wisdom of expanding the right to privacy into a right to be forgotten. *See generally* Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2 (encouraging "rational review" of the benefits and costs of information exchange); Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking about You*, 52 STAN. L. REV. 1049 (2000) (suggesting that "a right to have the government stop people from speaking about you" may have "unintended consequences").

37. *See, e.g.*, The Florida Star v. B.J.F., 491 U.S. 524, 532 (1989) ("[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not consti-

DOI: doi:10.15779/Z38V08Z

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."[38] Yet, there are still some circumstances where US courts will accept privacy claims, even where the matter is worthy of media attention.[39]

Outside the context of newsworthy stories, US courts have been less inclined to insist on unrestrained access to information.[40] In *Nixon v. Warner Communications, Inc.*,[41] 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."[42] Similarly, in *US Dep't of Justice v. Reporters Comm. for Freedom of the Press*,[43] the Supreme Court recognized, in the context of a Freedom of Information Act re-

---

tutionally punish publication of the information, absent a need to further a state interest of the highest order."); Smith v. Daily Mail Publishing Co., 443 U.S. 97 (1979) (justification for prior restraint of publication requires showing that the state's action furthers a state interest of the "highest order"); Oklahoma Publishing Co. v. District Court, 430 U.S. 308 (1977) (invalidating district court order enjoining newspapers from publishing name and picture of juvenile offender); Cox Broad. v. Cohn, 420 U.S. 469 (1975) (press could not constitutionally be exposed to tort liability for truthfully publishing name of rape and murder victim released to public in official court records); *see generally* Arminda Bradford Bepko, *Public Availability or Practical Obscurity: The Debate over Public Access to Court Records on the Internet*, 49 N.Y.L. SCH. L. REV. 967 (2005). Despite these opinions, even court records are not universally available to the public. *See* Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 WASH. L. REV. 307, 309 (2004) (noting various criminal procedure rules that protect reputations, such as secrecy of grand jury proceedings, search warrant applications, and pre-sentence reports); *id.* at 311 ("[C]ourts tend to protect personal information when the purpose of access is not related to facilitating public scrutiny of the judicial process").

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*, 84 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-ridden 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").

43. 489 U.S. 749 (1989).

quest, that a "privacy interest" may exist in "keeping personal facts away from the public eye."[44] 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.[45]

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*,[46] 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. . . ."[47] More recently, in *Holder v. Humanitarian Law Project*,[48] 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'g* 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).

47. *Yahoo!*, 433 F.3d at 1217; *see also* Desai v. Hersh, 719 F. Supp. 670, 679-80 (N.D. Ill. 1989) (noting that not all speech published by US citizens in foreign forums is covered by the First Amendment); Robert D. Kamenshine, *Embargoes On Exports Of Ideas And Information: First Amendment Issues*, 26 WM. & MARY L. REV. 863, 867 (1985) (questioning whether First Amendment values apply to speech by aliens); Suzlon Energy Ltd. v. Microsoft Corp., No. 10-35793, 2011 WL 4537843 at *4 (9th Cir. Oct. 3, 2011) (discussing how foreigners may have privacy interest in the United States).

DOI: doi:10.15779/Z38V08Z

Supreme Court upheld portions of the USA PATRIOT Act that criminalize speech when it is "coordinated" with "foreign terrorist" organizations.[49] These, and other decisions,[50] suggest that First Amendment protections are not absolute, at least in the context of foreign-related speech.[51]

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.[52] Indeed, recent EU pronouncements and court decisions expressly recognize the need to balance rights of privacy with freedom of expression.[53] Various international declarations similarly support the need for such a balance.[54]

---

48. 130 S. Ct. 2705 (2010).

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.

51. *See* Timothy Zick, *The First Amendment And Territoriality: Free Speech At—And Beyond—Our Borders*, 85 NOTRE DAME L. REV. 1543 (2010); Burt Neuborne & Steven R. Shapiro, *The Nylon Curtain: America's National Border And The Free Flow Of Ideas*, 26 WM. & MARY L. REV. 719 (1985).

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://cadmus.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).

53. Article 10(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221 recognizes a right to "receive and impart information and ideas without interference by public authority and regardless of frontiers." Recent EU pronouncements have referenced that principle. *See* Council of the European Union, *Council Conclusions On The Communication From The Commission To The European Parliament And The Council – A Comprehensive Approach On Personal Data Protection In The European Union*, pmbl. ¶ 8, Feb. 24-25, 2011[hereinafter EU Council Conclusions On Personal Data Protection], http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/jha/119461.pdf (noting that "other relevant fundamental rights," including "the right to freedom of expression and information" must be "fully taken in to account while ensuring the fundamental right to the protection of personal data"); Opinion 5/2009 Online Social Networking at 6 (June 12, 2009) ("[B]alance needs to be struck between freedom of expression and the right to privacy."), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf; Case C-101/01, In re: Bodil Lindqvist, 2003 ECR I-12971 ¶ 90, http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=161968 (noting need for "fair balance" between rights established by EU, including freedom of expression); Case C-275/06, Productores de Música de España v. Telefónico de España SAU. 2008 ECR I-271 ¶ 68 (member states must consider "fair balance" between fundamental rights).

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

---

Standards On The Protection Of Personal Data And Privacy ¶ 2, Nov. 5, 2009, http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24464/20091.pdf(representatives from 50 countries suggest "consensus" views on privacy standards); *Statement On The Necessity Of International Frameworks In Support Of The Protection Of Privacy And Personal Data*, Oct. 27, 2009, http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24465/20092.pdf (Microsoft, IBM, Google and other companies support "protection of personal information while providing legal certainty for the data flows [that] are essential to economic growth"); International Conference of Data Protection and Privacy Commissioners, *Draft Resolution On The Urgent Need For Protecting Privacy In A Borderless World, And For Reaching A Joint Proposal For Setting International Standards On Privacy And Personal Data Protection* 2, Oct. 17, 2008, http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24474/20083.pdf (noting "promising efforts" to develop "effective and universally accepted international privacy standards as a mechanism for assisting parties to establish and demonstrate compliance with legal requirements").

55. EuroISPA, *Consultation On The Commission's Comprehensive Approach On Personal Data Protection In The European Union* 8, Jan. 2011[hereinafter EuroISPA, *Personal Data Protection in the EU*], http://www.euroispa.org/files/1101_euroispa_data_protection_consultation.pdf (imposition of intermediary liability for content would require intermediaries to "constantly monitor all content," leading to "massive censorship," which could "seriously hamper the viability of the Internet"); UK Advertising Association, *Response To The European Commission Paper: "A Comprehensive Approach On Personal Data Protection In The European Union,"* 1, Jan. 14, 2011, http://www.adassoc.org.uk/write/Documents/AA%20DPD%20response%20Jan2011.pdf (data protection should "strike[] a balance between protecting the rights of citizens and the objectives of the single market" as well as "economic development" concerns, to prevent regulations from becoming "a barrier to market entry").Importantly, jurists, lawyers and academics in the EU and the US interact with increasing frequency, producing ever-greater opportunities for such discussions. *See* Pollicino & Bassini, *supra* note 5252, at 27 (noting "global judicial dialogue" that "very often occurs" to avoid "risk of collision" with regard to "the standard of protection of fundamental rights"); Robert Uerpmann-Wittzack, *Principles Of International Internet Law*, 11 GERMAN L.J. 1245, 1246 (2010) (suggesting development of "emerging principles of I[nternational] I[nternet] L[aw]," including both freedom of expression and privacy).

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*, J. 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")

DOI: doi:10.15779/Z38V08Z

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" construct[57] with the input and approval[58] of the EU.[59] This approach has generally been successful[60] 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).

57. *See* US Department of Commerce, *Safe Harbor Overview*, http://www.export.gov/safeharbor.

58. *See* Commission Of The European Communities, *Commission Decision Pursuant To Directive 95/46/EC Of The European Parliament And Of The Council On The Adequacy Of The Protection Provided By The Safe Harbour Privacy Principles And Related Frequently Asked Questions Issued By The US Department Of Commerce*, (July 26, 2000), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

59. *See* Virginia Boyd, *Financial Privacy In The United States And The European Union: A Path To Trans-Atlantic Regulatory Harmonization*, 24 BERKELEY J. INT'L L. 939, 969 (2006) (summarizing development of Safe Harbor program); Stephen J. Kobrin, *Safe Harbours Are Hard To Find: The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction And Global Governance*, 30 REV. INT'L STUD. 111, 113 (2004); Alexander Zinser, *The Safe Harbor Solution: Is It An Effective Mechanism For International Data Transfers Between The United States And The European Union?*, 1 OKLA. J. L. & TECH. 11 (2004). *But see* Paul Reid, *"Regulating" Online Data Privacy*, 1 SCRIPT-ED 488, 495-96 (2004) (noting that Safe Harbor is "a marriage of convenience" between the European Union and the United States; and the measure has garnered "poor take up" by businesses).

60. *See* Peter P. Swire, *Elephants And Mice Revisited: Law And Choice Of Law On The Internet*, 153 U. PA. L. REV. 1975, 1986-87 (2005) (Safe Harbor has produced a "limited, but significant, degree of harmonization of privacy standards" between the United States and the European Union, and has "been fairly successful at meeting two strategic goals: avoiding a trans-Atlantic trade war and providing a reasonable baseline for privacy protection in transborder activities"); Nikhil S. Palekar, *Privacy Protection: When Is "Adequate" Actually Adequate?*, 18 DUKE J. COMP. & INT'L L. 549, 573 (2008) (Safe Harbor program allows US companies to "look not to the Directive when evaluating notice and privacy practices but rather to the Safe Harbor provisions").

61. *See* Gregory Shaffer, *Reconciling Trade And Regulatory Goals: The Prospects And Limits Of New Approaches To Transatlantic Governance Through Mutual Recognition And Safe Harbor Agreements*, 9 COLUM. J. EUR. L. 29 (2002).

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).

63. *See* David Banisar, *The Right To Information And Privacy: Balancing Rights And Managing Conflicts*, at 7, 2011, http://wbi.worldbank.org/wbi/Data/wbi/wbicms/files/drupal-acquia/wbi/Right%20to%20Information%20and%20Privacy.pdf ("Since the 1960s, principles governing the collection and handling of [private] information (known as 'fair information practices') have been developed and adopted by national governments and international bodies").

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]

---

64. *See* Katie Kindelan, *Will Europe's Online Privacy Laws Jump The Pond To The US?*, SOCIAL TIMES, Mar. 21, 2011, http://socialtimes.com/will-europes-online-privacy-laws-jump-the-pond-to-the-u-s_b42528 (noting that calls for reform of data protection in the European Union come at a time when both the President and Congress are "calling for tougher online privacy regulations" in the United States); Christopher Kuner, Fred H. Cate, Christopher Millard & Dan Jerker B. Svantesson, *Moving Forward Together*, 1 INT'L DATA PRIV. L. 81, 81 (2011) [hereinafter *Moving Forward*] (noting "growing convergence in transatlantic thinking about data protection issues;" and noting that "elements of" recent FTC, DOC and EU reports each "sound themes historically associated with regulators on the other side of the Atlantic"); CTR. FOR DEMOCRACY & TECH., *supra* note 24, at 2 (noting that discussions with US Department of Commerce and FTC raise "many of the same issues" raised by the EU Commission with regard to Directive reform); *see also* Steven C. Bennett, *The Politics Of Privacy*, NAT'L L.J., Jan. 31, 2011, http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202479696504&slreturn=1 (discussing recent US agency reports and congressional developments related to privacy enhancement); Kashmir Hill, *Could Europe's Tough Privacy Protection Proposals Influence Washington, D.C.?*, FORBES, Oct. 22, 2010, http://www.forbes.com/sites/kashmirhill/2010/10/22/will-europes-tough-privacy-protection-proposals-influence-washington-d-c/; James E. Weber & Richard Paulson, *The EU's Data Protection Directive: Headed For The Rocks?*, 4 ISSUES IN INFO. SYS. 748, 752 (2003) ("It is possible that the [EU Data Protection] Directive may even spark demands by US citizens for privacy coverage equal to the treatment their employers are giving EU citizens."); Todd A. Nova, *The Future Face Of The Worldwide Data Privacy Push As A Factor Affecting Wisconsin Businesses Dealing With Consumer Data*, 22 WIS. INT'L L.J. 769, 769-70 (2001) (noting "ratcheting" effect on US privacy legislation, as a result of economic pressure from EU Directive).

65. *See* Preliminary FTC Staff Report, *Protecting Consumer Privacy In An Era Of Rapid Change: A Proposed Framework for Businesses And Policymakers* 79 (Dec. 2010) [hereinafter FTC 2010 Report].

66. *Id.* at 19.

67. *See* Department of Commerce, Internet Policy Task Force, *Commercial Data Privacy In The Internet Economy: A Dynamic Policy Framework*, NAT'L TELECOMM. & INFO. ADMIN. Dec. 2010 [hereinafter Commerce Report], http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework. The central purpose of the Commerce Report was to "articulate certain core privacy principles," and "assure baseline consumer protections." *Id.* at 1 (introductory message from Commerce Secretary Gary Locke).

68. *Id.* at 3-7.

69. The Commerce Report suggested that fair information principles should "enhanc[e] transparency, encourage[ ] 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.

DOI: doi:10.15779/Z38V08Z

(2) 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).

74. *U.S. Federal Trade Commission Staff Comments On The European Commission's November 2010 Communication On Personal Data Protection In The European Union* 1-2, Jan. 13, 2011 [hereinafter FTC Staff Comments] http://www.ftc.gov/os/2011/01/111301dataprotectframework.pdf (noting "ongoing communication" between the FTC and the European Union on data protection issues, which is "one of the FTC's highest priorities"); *id.* at 3 (noting that FTC contributes to privacy work within OECD and APEC organizations).

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.[76] Thus, EU plans to revisit the data protection directive to improve harmonization within the European Union itself[77] may offer a particularly good opportunity for such dialogue with US authorities.[78]

At a minimum, US engagement of EU authorities can provide clarification of the EU view of the right to be forgotten.[79] The development of a single EU standard for such a right could also provide greater certainty and predictability

---

recent meetings with EU authorities, and announced a plan to hold a conference on Safe Harbor issues in November 2011. *See Department of Commerce Official Holds Briefing on EU Data Protection Forum: Privacy & Information Security Law Blog*, LEGAL TECH. TODAY, Jan. 12, 2011, http://www.legaltechtoday.com/2011/01/12/department-of-commerce-official-holds- briefing-on-eu-data-protection-forum-privacy-information-security-law-blog/; March 2011, the US announced a plan to create a formal "mandate" for negotiations with EU authorities on data protection issues. *See* Toby Vogel, *US Preparing For Talks On Data Protection*, EUROPEAN VOICE, Mar. 10, 2011, http://www.europeanvoice.com/article/imported/us-preparing-for-talks-on- data-protection/70488.aspx.

76. *See* Peter Hustinx, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions—"A Comprehensive approach on personal data protection in the European Union"*, Jan. 17, 2011, http://ediscoverymap.com/2011/01/opinion-of-the-european-data-protection- supervisor-on-the-communication-from-the-commission-to-the-european-parliament-the-council-the-economic-and-social-committee-and-the-committee- of-the-regions/ ("a review of the present legal framework for data protection in the EU is necessary, in order to ensure effective protection in a further developing information society;" and "in the longer term, changes of Directive 95/46/EC seem unavoidable" at para 3; review of the Directive "occurs at a crucial historical moment," at para 13-15 where "technology is not the same," and "globalisation" has become a major force); Mark Rasdale, *New Working Party Opinion Relevant To Cloud And Social Network Providers*, Jan. 21, 2011, http://www.irelandip.com/2011/01/articles/information-technology/new-working- party-opinion-relevant-to-cloud-and-social-network-providers/ (suggesting that recent Working Party opinion is a "clear sign that legislative change (in the mid to longer term) to deal with these developments is inevitable"); Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri, *Review Of The European Data Protection Directive*, vii, May 2009, *available at* http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf (Rand Europe report) ("the Directive as it stands will not suffice in the long term;" noting "growing challenge of globalization and international data flows").

77. Hon, Millard & Walden, *supra* note 27 (noting "important national differences in data protection laws" within EU, including degree of civil liability and penalties for violations).

78. *See* EU Council Conclusions On Personal Data Protection, *supra* note 53, at 1-2 (noting that "emerging business and technological developments" in years since 1995 Directive "require a thorough evaluation" of the Directive, and suggest need for "better harmonization" of rules to allow "free movement of data"); Hustinx, *supra* note 76.

79. It is possible, of course, that EU regulators may conclude that no single, useful standard for the right to be forgotten can be formulated, and that the issue might be better left for further discussion as law, technology and Internet usage develop. *See* Stuart Robertson, *Hasty Legislation Will Make A Mess Of Europe's "Right To Be Forgotten;" The Ethics Of Online Deletion,* THE REGISTER, Nov. 12, 2010, http://www.theregister.co.uk/2010/11/12/privacy_legislation/ ("[T]he problems [with a right to be forgotten] are technical, ethical and legal. Most of all they are complex, and EU legislators would be fools to write laws covering such sensitive ground in any kind of hurry").

DOI: doi:10.15779/Z38V08Z

to foreign businesses operating in the European Union.[80] Substantive reconciliation of EU and US data protection law need not necessarily take on the full debate about freedom of expression versus privacy.[81] 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.[82] Further, the discussions might include methods to support self-regulation (or "co-regulation") to promote aspects of the right to be forgotten.[83] 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 PRESSE, 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 Jonathan 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").

82. *See* EFAMRO / ESOMAR, *Consultation On The Commission's Communication "A Comprehensive Approach On Personal Data Protection In The European Union,"* 3, Jan. 14, 2011, http://www.efamro.eu/Files/2011-01-14%20EC%20Data%20Protection%20Consultation%20Response-FINAL.pdf (concept of right to be forgotten should emphasize "responsible data collection, data minimization, and purpose limitation"); *see also* Gregory C. Shaffer & Mark A. Pollack, *Hard vs. Soft Law: Alternatives, Complements, And Antagonists In International Governance*, 94 MINN. L. REV. 706 (2010) (harmonization of EU law may lead to world standards).

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.[84] Finally, to the extent that certain technical solutions (such as systems for auto-deletion of information)[85] might address concerns underlying the right to be forgotten, regulators could (and should) discuss means to facilitate development and use of such technology.[86]

Health Records: Breaking Through The Privacy Logjam To Increase The Adoption Of A Long-Overdue Technology, 2009 WIS. L. REV. 1169 (reviewing co-regulation experience and suggesting application); Richard M. Marsh, *Legislation For Effective Self-Regulation: A New Approach To Protecting Personal Privacy On The Internet*, 15 MICH. TELECOMM. & TECH. L. REV. 543 (2009); Natascha Just & Michael Latzer, *Self And Co-Regulation In The Mediamatics Sector*, 17 KNOW. TECH. POL. 38 (2004) (proliferation of electronic services requires guidance beyond market, but government intervention only justified where indispensable); Daniel E. Newman, *European Union And United States Personal Information Privacy, And Human Rights Philosophy—Is There A Match?*, 22 TEMP. INT'L & COMP. L.J. 307 (2008) (suggesting means of reconciling EU and US views on data privacy).

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/20100727142911enelrahc0.9917871.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.unitn.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; s*ee 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.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24477/20086.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 'disentangling' 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-

DOI: doi:10.15779/Z38V08Z

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.[87] 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?[88] In an inter-connected world, such a scenario inevitably arises.[89] Effective enforcement of any right, including the

---

regulation which are the most effective means to deal with fast-moving technology markets"); s*ee 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-enhanci; 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 "[s]ubstantive 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,[90] which commentators have long recognized.[91]

Traditionally, the exercise of jurisdiction was based on the concept of "sovereignty" over territory.[92] 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.[93] In the essentially borderless region of cyberspace, the concept of sovereignty over specific physical territory becomes particularly problematic.[94] 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]").

92. Hannah L. Buxbaum, *Conflict of Economic Laws: From Sovereignty to Substance*, 42 VA. J. INT'L L. 931, 933 n.3 (2002) (the power to "exercise supreme authority over a territory carved on the physical map of the world" [is] a primary aspect of sovereignty); Daniel Philport, *Sovereignty: An Introduction and Brief History*, 48(2) J. INT'L AFF. 353, 356-57 (1995) ("Sovereignty is authority, within a discrete land, bounded by borders . . . [and the] legitimate authority within a territory."); *see generally* Andrea Slane, *Tales, Techs, and Territories: Private International Law, Globalization, and the Legal Construction of Borderlessness on the Internet*, 71 LAW & CONTEMP. PROBS. 129, 130 (2008).

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

DOI: doi:10.15779/Z38V08Z

of the Internet,"[95] a consistent, understandable "effects" standard of jurisdiction naturally becomes the most likely substitute for a strict "sovereignty" approach.[96] An unlimited "effects" doctrine, however, could be used to justify virtually unlimited jurisdiction.[97] 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.[98]

The divergence of views on Internet-based jurisdiction appears in US case law and EU official pronouncements.[99] To a large extent,[100] 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."); Digital Equip. Corp. v. AltaVista Tech., Inc., 960 F. Supp. 456, 462 (D. Mass. 1997) ("The Internet has no territorial boundaries. To paraphrase Gertrude Stein, as far as the Internet is concerned, not only is there perhaps 'no there there,' the 'there' is *everywhere* there is Internet access."); *see generally* Georgios I. Zekos, *State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction*, 15 INT'L J.L. & INFO. TECH. 1 (2007) (the Internet operates through networks, not through specific geography); Joanna Kulesza, *Internet Governance and the Jurisdiction of States: Justification of the Need for an International Regulation of Cyberspace* (Dec. 2, 2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1445452 (noting that the Internet is "aterritorial" in that it does not conform to "statehood in its traditional sense;" statehood generally connotes "complete and exclusive" sovereignty "exercised at a particular territory, shaped by the organs of state power").

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. J.L. & 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. L. 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."); Pollicino & 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").

98. *See* Reidenberg, *supra* note 88, at 1960.

99. *See generally* Faye Fangfei Wang, *Obstacles and Solutions to Internet Jurisdiction: A Comparative Analysis of the EU and US Laws*, 3 J. INT'L COMMERCIAL L. & TECH. 233 (2008) (contrasting EU and US jurisdiction tests and suggesting use of "targeting" standard).

100. *See* Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, 452 (3rd Cir. 2003) (noting that

lowed 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

---

Zippo "has become a seminal authority" regarding jurisdiction based upon "the operation of an Internet web site"); Allyson W. Haynes, *The Short Arm of the Law: Simplifying Personal Jurisdiction Over Virtually Present Defendants*, 64 U. MIAMI L. REV. 133, 154-55 (2009) ("The *Zippo* test has been praised and criticized, but never ignored."); A. Benjamin Spencer, *Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network-Mediated Contacts*, 2006 U. ILL. L. REV. 71, 74 ("Unfortunately, the prevailing analysis in contemporary *Zippo*-based approaches is fundamentally unsound").

101. 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

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*.

107. *See* Timofeeva, *supra* note 88 (noting that "[n]ot all cases are consistent" in application of *Zippo* test); Cindy Chen, *United States And European Union Approaches To Internet Jurisdiction and Their Impact On E-Commerce*, 25 U. PA. J. INT'L ECON. L. 423, 435-36 (2004) (noting that some US courts apply "effects-based" test in lieu of *Zippo* standard).

108. *See*, *e.g.*, GTE New Media Serv. v. BellSouth Corp., 199 F.3d 1343, 1346 (D.C. Cir. 2000) (personal jurisdiction could not be based upon "mere accessibility to an Internet site" within jurisdiction); Cybersell, Inc. v. Cybersell Co., 130 F.3d 414, 418 (9th Cir. 1997) (internet advertising alone insufficient for jurisdiction); English Sports Betting v. Tostigan, No. CIV.A. 01-2202, 2002 WL 461592 (E.D. Pa. 2002) (internet publication allegedly defaming Pennsylvania resident insufficient to justify jurisdiction); *In re* Magnetic Audiotape Antitrust Litig., 171 F. Supp. 2d 179 (S.D.N.Y. 2001) (foreign company's passive website did not support a finding of minimum contacts sufficient for jurisdiction); Machulsky v. Hall, 210 F. Supp. 2d 531 (D.N.J. 2002) (buyer's single transaction on eBay did not confer specific jurisdiction in seller's forum state); Barrett v. Catacombs Press, 44 F. Supp. 2d 717 (E.D. Pa. 1999) (posting to listserv too passive for personal jurisdiction); Timofeeva, *supra* note 88, at 205 (noting that US law includes a "reasonableness" requirement as part of a "threshold" for application of national law to extraterritorial activities) (citing Restatement (Third) of Foreign Relations Law § 403(1) (1987)).

DOI: doi:10.15779/Z38V08Z

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 entities[111] 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").

110. *See* Council Directive 95/46/EC, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (defining in Article 2, paragraph (b) "processing of personal data" to include "any operations or set of operations which is performed upon personal data," regardless of whether the data is processed by automatic means); *see generally* Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of "Controller" and "Processor", 00264/10/EN WP 169 (Feb 16, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (outlining broad definitions of information processing for use in connection with Directive).

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).

112. *See* Reidenberg, *supra* note 88, at 1957 (noting "expansive" rule in Directive).

113. Council Directive 2000/31/EC, On Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), 2000 O.J. (L178), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML .

114. Article 29 Data Protection Working Party, Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites 5035/01/EN/Final, WP 56 (May 30, 2002), *available at* http://www.interlex.it/testi/pdf/wd5035.pdf.

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,[116] 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.[117] 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.[118] 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.[119] 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,[120] 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. I-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)).

118. *See* Matthew Fagin, *Regulating Speech Across Borders: Technology vs. Values*, 9 MICH. TELECOMM. & TECH. L. REV. 395, 434 (2003) (noting "troubling" trend of EU regulators and courts to use "effects-based analysis" to exercise jurisdiction).

119. Chris Brummer, *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 Vermeer, *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").

DOI: doi:10.15779/Z38V08Z

recent criminal prosecution of Google executives in Italy,[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"[122] includes a user's downloading of Internet content somewhere in Europe,[123] the European Union theoretically could exercise world-wide jurisdiction over Internet actors.[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).[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.[126]

---

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.

122. Christopher Kuner, *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").

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").

124. *See* Kuner, *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).

125. *See* Brummer, *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, *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, *supra* note 88 (prospect for assertion of worldwide jurisdiction "contributes to legal uncertainty"); Chen, *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., *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).

126. *See* Chris Reed, *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* 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.[127] 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,[128] 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.[129]

The notion of "targeting" as a standard for the exercise of jurisdiction has relatively wide support among commentators.[130] US courts have developed ex-

---

consists of "the recognition which one nation allows within its territory to the legislative, executive, or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protections of its law").

127. *See* Burke T. Ward & Janice C. Sipior, *Where In The World Is Internet Jurisdiction: A US Perspective*, 4 INT'L J. VALUE CHAIN MGMT. 5 (2010) (noting need to develop "globally agreed" standard for jurisdiction related to Internet activity); Timofeeva, *supra* note 88 (international agreement on jurisdiction standards for Internet-related issues "certainly" best choice, if possible to achieve); Chen, *supra* note 107, at 447 ("obvious solution" to divergence in approaches to Internet jurisdiction is for the United States and the European Union to "cooperate and develop an international framework"); *see also* Julia Marter, *When and Where Does an Internet Posting Constitute Publication? Interpreting Moberg v. 33T LLC*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 495 (2011) ("Surprisingly, the legal community has not yet answered this question").

128. *See* Opinion 8/2010 On Applicable Law, 0836-02/10/EN WP 179 (Dec. 16, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

129. *See id.* at 24 ("A more specific connecting factor, taking the relevant 'targeting' of individuals into account, as a complement to the 'equipment/means' criteria could be useful in terms of legal certainty[.] Such a criterion is not new and has been used in other contexts in the EU, and by the United States' legislation on the protection of children on-line."); *see id.* at 31 ("The following examples illustrate what targeting could consist of: the fact that a data controller collects personal data in the context of services explicitly accessible or directed to EU residents, via the display of information in EU languages, the delivery of services or products in EU countries, the accessibility of the service depending on the use of an EU credit card, the sending of advertising in the language of the user or for products and services available in the EU").

130. Pollicino & Bassini, *supra* note 52, at 9-10 (suggesting that "common denominator" in authorities is that "as long as websites do not target nor produce harm to certain individuals or entities, a domestic jurisdiction cannot be asserted on the sole ground that website contents do not comply with the laws of that state"); Lorna E. Gilles, *Addressing the "Cyberspace Fallacy": Targeting the Jurisdiction of an Electronic Consumer Contract*, 16 INT'L J. L. & TECH. 242 (2008) (suggesting use of "intentional targeting" standard as basis for jurisdiction); Timofeeva, *supra* note 88 ("Targeting-based analysis could be a solution to the unlimited application of the effects principle if the courts could agree to accept it in a consistent form."); Thomas Schultz, *Carving Up The Internet: Jurisdiction, Legal Orders, And The Private/Public International Law Interface*, 19 EURO. J. INT'L L. 799 (2008) (noting risk that Internet will be "fragmented" into discrete legal spheres, by local law, and suggesting a "principle of targeting" and "effects doctrine" as solution); Brian D. Boone, *Bullseye! Why A "Targeting" Approach To Personal Jurisdiction In The E-Commerce Context Makes Sense Internationally*, 20 EMORY INT'L L. REV. 241 (2006); Greenberg, *supra* note 46, at 1253-54 (suggesting that agreement on international convention on jurisdiction may be "impossible," but "targeting" test can be developed with existing standards); Michael A. Geist, *Is There A There*

DOI: doi:10.15779/Z38V08Z

perience in applying such a standard[131] and, to a lesser extent, the notion is recognized in the European Union.[132] 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.[133] Courts can also recognize other indicia of "targeting," such as language, specific content and references to the particular country.[134] The International Organization of Securities Commissions adopted just such a test for national jurisdiction over securities offerings.[135] In the United States, the FTC applies similar standards in determining whether websites are addressed at children.[136] A further example appears in the EU Convention on Cybercrime.[137] Such standards, of course, rely to some

---

There? Toward Greater Certainty For Internet Jurisdiction, 16 BERKELEY TECH. L.J. 1345, 1378 (2001) (suggesting use of targeting test as basis for rulings on jurisdiction).

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").

132. *See* Council Regulation 44/2001 of Dec. 22, 2000 on Jurisdiction and the Recognition and Enforcement of Judgments and Commercial Matters, 2001 O.J. (L12) (referencing country-of-destination as basis for jurisdiction).

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).

137. Council of Europe, Committee of Ministers, Convention on Cybercrime, Explanatory Report, Nov. 8, 2001, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (noting authority of state to regulate "where the computer system [attacked] is within its territory, even if the attacker is not"); Cristos Velasco San Martin, *Jurisdictional Aspects Of Cloud Computing*, Feb. 28, 2009, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf (noting that the jurisdiction provision of the Convention on Cybercrime "represents the consensus of traditional accepted principles of jurisdiction under public international law"); Michael L. Rustad, *Private Enforcement Of Cybercrime*

degree on subjective and ambiguous factors[138] and may introduce new complications.[139] But a workable standard is at least theoretically possible.[140]

Similarly, the development of "geo-location" technologies for the Internet potentially opens the way to development of new standards for jurisdiction.[141] Website purveyors often tailor their content to specific markets and use geo-location technology to assist them in delivering targeted messages.[142] Indeed,

---

On The Electronic Frontier, 11 S. CAL. INTERDIS. L.J. 63 (2001) (discussing enforcement of Cybercrimes Convention); Nancy E. Marion, *The Council Of Europe's Cyber Crime Treaty: An Exercise In Symbolic Legislation*, 4 INT'L J. CYBER CRIM. 699, 701 (2010) (noting that negotiation of convention included representatives of US, Japan and other non-EU nations).

138. Timofeeva, *supra* note 88 (targeting test based on language of site "problematic," given that English, Spanish and other languages are commonly used in many jurisdictions); *id.* at 213 ("Targeting is relatively easy to detect when commercial activity takes place but when a passive website merely provides information on objectionable subjects the targeting of a particularly jurisdiction is far from obvious."); *see also*, Allison MacDonald, *YouTubing Down The Stream Of Commerce: Eliminating The Express Aiming Requirement For Personal Jurisdiction In User-Generated Internet Content Cases*, 19 ALB. L.J. SCI. & TECH. 519 (2009) (suggesting that proof, under targeting standard, may be difficult to sustain).

139. The use of "targeting" criteria for the exercise of jurisdiction does not necessarily solve all the problems of uncertainty and burden that may attend to EU exercise of jurisdiction over foreign data controllers. *See* Gail Crawford, *Article 29 Working Party Comments On Applicable Law Highlight The Need For Greater Harmonisation*, Jan. 5, 2011, http://www.globalprivacyblog.com/privacy/article-29-working-party-comments-on-applicable-law-highlight-the-need-for-greater-harmonisation/ (noting that "targeting" rule could actually increase burdens, because the data protection laws of EU member states vary) ("Businesses established in Europe would only have to comply with the laws of the territory of their main establishment, whilst those established outside Europe and targeting European consumers would need to comply with the laws of each state in which they target individuals.").

140. Julie L. Henn, *Targeting Transnational Internet Content Regulation*, 21 B.U. INT'L L.J. 157, 174 (2003) (suggesting standards for "targeting" test for jurisdiction based on Internet activities); Holger P. Hestermeyer, *Personal Jurisdiction For Internet Torts: Towards An International Solution*, 26 NW. J. INT'L L. & BUS. 267, 269 (2006) ("[I]nsecurity about Internet jurisdiction could be reduced significantly if countries were to commit themselves in an international convention to abide by a targeting approach along with guidelines for relevant criteria").

141. These technologies are widely available. The questions of whether (and how) they should be used amounts to a matter of political philosophy. *See* Horatia Muir Watt, *Yahoo! Cyber Collision Of Cultures: Who Regulates?*, 24 MICH. J. INT'L L. 673, 683 (2003) ("[G]eographical indeterminacy on the Internet is not inevitable, but results from ideological choice").

142. Patricia Moloney Figliola, Kennon H. Nakamura, Casey L. Addis & Thomas Lum, *U.S. Initiatives To Promote Global Internet Freedom: Issues, Policy and Technology*, CRS Rep. 7-5700 at i, Jan. 3, 2011, http://fpc.state.gov/documents/organization/140637.pdf ("Internet services are often tailored for deployment to specific countries."); Kevin F. King, *Personal Jurisdiction, Internet Commerce, And Privacy: The Pervasive Legal Consequences Of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61, 63, 66 (2011) ("Modern geolocation technologies allow Internet sites to automatically and accurately identify a user's geographical location. . . . [G]eolocation tools have already become an essential part of many electronic commerce business models."); Reidenberg, *supra* note 88, at 1956 ("While online technologies were initially designed for geographically indifferent access, nothing fixed the technology in stone. Commercial pressures and the dynamic nature of the Internet have resulted in geolocation and the re-creation of geographic origin and destination."); Jack L. Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EURO. J. INT'L L. 135, 159 (2000) (assumption that content provider cannot monitor or control geographic flow of in-

DOI: doi:10.15779/Z38V08Z

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."[143] These geo-location technologies have their limits, of course.[144] Such technologies, sometimes used to establish "content zoning,"[145] present serious privacy concerns,[146] may adversely affect innovation,[147] may unduly place burdens on Internet intermediaries,[148] 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.").

143. Yiming Liu & Erik Wilde, *Personalized Location-Based Services* (2011), *available at* http://dret.net/netdret/docs/wilde-iconf2011-horizontal-lbs.pdf.

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").

146. *See* Janice Y Tsai, Patrick Gage Kelley, Lorrie Faith Cranor & Norman Sadeh, *Location-Sharing Technologies: Privacy Risks and Controls*, 6 I/S: A J. OF L. & POLICY FOR THE INFO. SOC. 119 (2010). (a recent Department of Justice proposal to enhance the ability of law enforcement to determine the locations of wireless device users, for example, drew immediate (and negative) commentary). *See* Lisa Greim, *DOJ Wants More Wireless Location Tracking*, May 11, 2011, http://www.pcworld.com/article/227580/stop_the_presses_department_of_justice_wants_more_wireless_location_tracking.html (noting congressional inquiry); *see also*, Tony Bradley, *Who Else Is Tracking Your Location?*, Apr. 29, 2011, http://www.pcworld.com/businesscenter/article/226699/who_else_is_tracking_your_location.html (noting "privacy concerns" from geo-location by wireless providers, GPS navigation systems, ATM and credit cards, and more); Tony Bradley, *iPhone Tracking Not News, Not Unique, and Not Ominous*, Apr. 23, 2011, http://www.pcworld.com/article/226127/iphone_tracking_not_news_not_unique_and_not_ominous.html (noting "panic among the media and privacy advocates" over revelations of geo-tracking). The EU apparently views geo-location data as private. *See* Jennifer Baker, *Location Data is Personal and Private Confirms EU Watchdog*, May 17, 2011, http://www.pcworld.com/businesscenter/article/228034/location_data_is_personal_and_private_confirms_eu_watchdog.html ("Location data is certainly, in many instances, private data[.]") (quoting Peter Hustinx, European Data Protection Supervisor).

147. Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart*, 42 U.C. DAVIS L. REV. 343, 348 (2008) (potential for "balkanization" of the Internet "poses grave threats to the Internet as an engine of innovation, economic growth, and creative expression"); Timofeeva, *supra* note 88, at 221 ("zoning" of the Internet would "render valuable content inaccessible and significantly raise the costs of Internet activities for all concerned"); Llewellyn Joseph Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL J. L. & PUB. POL'Y 475, 479 (1997) ("greatest danger" in Internet development is "balkanization of information (content)").

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.[149] At least in theory, such concerns could be addressed by a jurisdictional standard[150] that also considers whether the use of geo-location technology is mandatory or merely permissible.[151] Concerns regarding geo-location technology may also be addressed via the development of appropriate technology.[152]

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 Inter-

---

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 1953 ("[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").

152. Timofeeva, *supra* note 88 (noting potential for introduction of geographical indicator, associated with individual computer, to "enable an easy check of the location of every site visitor," which "could make the site inaccessible for users from specific jurisdictions"); Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 399 (1999) (describing system for Internet access controls).

DOI: doi:10.15779/Z38V08Z

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) ("[D]espite significant convergence in global information privacy norms, the difficulties resulting from trans-border data flows represents a further concern insufficiently dealt with by existing privacy norms").

154. *See* Ivana Deyrup, *Responses to Questions Posed by CNAS on International Law & Internet Freedom*, Mar. 2011, http://www.law.harvard.edu/students/orgs/nsrc/CNAS-Final%20Draft-3.pdf ("There are many different potential models for international normative regimes to promote Internet freedom, including existing international human rights norms, international treaties and organizations, industry self-regulation, and domestic legislation that directs the conduct of American corporations internationally."); *see also*, Sean Flynn, *ACTA's Constitutional Problem: The Treaty That Is Not a Treaty (Or An Executive Agreement)*, Mar. 1, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1982091 (noting variety of international agreement forms that US may constitutionally use).

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 Świtalski, *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").

156. *See* Charles F. Sabel & Jonathan Zeitlin, *Experimentalism in Transnational Governance: Emergent Pathways and Diffusion Mechanisms*, Mar. 2011, http://www2.law.columbia.edu/sabel/papers.htm (noting that "experimentalist regimes" for transnational regulation appear to be emerging and suggesting means to encourage this phenomenon).

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); Debora 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.[158] In the end, an approach to regulation based on careful attention to technology and business developments,[159] coupled with genuine respect for cultural differences, is most likely to produce satisfactory, workable international solutions.[160] 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.[161]

158. *See* Dan Jerker B. Svantesson, *A Legal Method for Solving Issues of Internet Regulation: Applied to the Regulation of Cross-Border Privacy Issues*, EUI Working Paper Law 2010/18 at 5, http://cadmus.eui.eu/bitstream/handle/1814/15344/LAW_2010_18.pdf?sequence=1 (noting differences between intentional versus unintended communications, and personal versus commercial communications).

159. Cass R. Sunstein, *Constitutional Caution*, 1996 U. CHI. LEGAL F. 361, 374-75 (1996) ("In [] period[s] 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.")

160. Nicola Lucchi, *Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression*, 19 CARDOZO J. INT'L & COMP. L. 1, 3 (2011) (attempts to regulate Internet content are "often criticized for the inability to reconcile technological progress, protection of economic interests and other interests that might conflict"); Evgeny Morozov, *Whither Internet Control?*, 22 J. DEMOCRACY 62 (2011) (Internet control schemes may threaten both privacy and freedom of expression; caution appropriate); Philip A. Wells, *Shrinking the Internet*, 5 N.Y.U. J. L. & LIB. 531, 532 (2010) (noting "strong temptation to fill the enforcement vacuum [on the Internet] with enhanced government intervention;" that approach may be "misguided" in producing "costly, oppressive" regulations).

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).

DOI: doi:10.15779/Z38V08Z

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]

162. *See* Press Release, European Commission, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses (Jan. 25, 2012), www.europa.eu*; Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*, COM (2012) 10 final (Jan. 25, 2012) (proposed form of revisions to directive), www.europa.eu.