SO CLOSE, YET SO FAR APART: THE EU AND U.S. VISIONS OF A NEW PRIVACY FRAMEWORK

(Summer, 2012)

So Close, Yet So Far Apart: The EU and U.S. Visions of a New Privacy Framework

BY CHRISTOPHER WOLF AND WINSTON MAXWELL

TECHNOLOGICAL ADVANCEMENTS have made it easier and more cost effective for businesses to collect, use, share, and store vast amounts of personal information about consumers and employees alike. As a result, privacy is becoming an ever-important issue for businesses of all types and sizes. The media increasingly are turning their attention to privacy-related issues, raising the stakes for businesses that maintain personal information, as one instance of mishandling personal information could harm the public's perception of a business. There are almost daily headlines about privacy abuses and mistakes. The continuing, Pulitzer Prize-nominated, *Wall Street Journal* series entitled "What They Know" has focused national and international attention on the often-undisclosed uses of Internet tracking technology to collect and share consumer information obtained from computers and mobile devices.[1] Thus, it is not surprising that policymakers around the world are re-examining the legal framework that regulates the collection, use, sharing, and storing of personal information—making more robust the protections afforded to such information, and increasing the legal obligations of business.

The privacy frameworks recently proposed by the European Commission, the White House, and the FTC seek more protection of individuals, and are founded on the same underlying principles of fairness. However, despite a common foundation, the privacy regimes from opposite sides of the Atlantic exhibit fundamental differences in approach and substance.

The Global Nature of Privacy

As a result of the ubiquitous nature of the Internet, data rarely stays in only one jurisdiction. Rather, the Internet, social media, and Cloud computing cross national borders, allowing data to be transmitted to any location in the world. As such, the privacy problem is not restricted to any one jurisdiction. Indeed, the wonder of modern technology is the ability of people to access information and entertainment from virtually anywhere, and to send information globally. Thus, one would expect nations of the world to focus on a global standard of protection, and to harmonize existing laws.

In that connection, at a recent conference held simultaneously in Washington and in Brussels, the EU Commissioner for Justice, Fundamental Rights and Citizenship and the U.S. Secretary of Commerce issued a joint statement declaring that "[t]his is a defining moment for global personal data protection and privacy policy and for achieving further interoperability of our systems on a high level of protection."[2]

One basis for the hoped-for interoperability is the wide agreement around the world, as there has been for decades, on the basics of what it means to protect privacy in an information age. The so-called "Fair Information Practice Principles," or "FIPPs," focus on empowerment of people to control their personal information and on safeguards to ensure adequate data security.[3] FIPPs form the core of the 1980 OECD privacy guidelines on which both the U.S. and European models are based, and that were adopted "to harmonise national privacy legislation and, while upholding [ ] human rights, [ ] prevent interruptions in international flows of data."[4]

The Targeted Approach to Privacy in the United States

Historically, the EU and United States have taken divergent approaches to implementing the FIPPs. In the United States, where privacy interests are balanced with the right to free expression and commerce, and where the legal framework assumes that—as a practical matter—not every piece of personal information can be protected and policed, the framework provides the highest levels of protection for sensitive personal information, such as financial, health, and children's data. For example, the Gramm-Leach-Bliley (GLB)

Christopher Wolf is a partner in Hogan Lovells US LLP, resident in Washington, DC, where he leads the global Privacy and Information Management practice. Winston Maxwell is a partner in the Paris office of Hogan Lovells Int'l LLP, where he focuses on data protection, technology, media, and telecoms. *The authors acknowledge with thanks the assistance of their Hogan Lovells colleague Steve Spagnolo in the preparation of this article.*

Act regulates how financial institutions collect, disclose, share, and protect personally identifiable financial information.[5] The Health Insurance Portability and Accountability Act (HIPAA) regulates the use and disclosure of "protected health information" by such entities as physicians, hospitals, and health insurers.[6] And the Children's Online Privacy Protection Act of 1998 (COPPA), regulates websites' collection and use of the personally identifiable information of children.[7]

A major, if not defining characteristic of U.S. privacy law, comes from the targeted enforcement actions against bad (or negligent) actors—principally by the U.S. Federal Trade Commission—which has created a "common law" of what is expected from business when it comes to the collection, use, and protection of personal information. The FTC has authority to take enforcement action against "unfair or deceptive" practices. In the privacy context, this has resulted in enforcement actions against companies that have promised something in their privacy policies about the collection, use, or protection of personal information but, in practice, handled the personal information in ways that differed from the promised treatment. Early examples include enforcement actions against Eli Lilly,[8] Microsoft Passport,[9] and Gateway,[10] when each company made representations concerning its data practices—such as how data will be collected, shared, and protected—which were contrary to what actually happened.

Data security breach notification laws require public notification of information security mishaps. The laws motivate companies to improve their data security to avoid having to report breaches publicly since publicity invites legal challenges. With the advent of the breach notification laws[11] the FTC developed new targets for enforcement—inadequate information security programs. A number of FTC enforcement actions have resulted in consent decrees requiring comprehensive data security programs regularly assessed and reported upon by independent outside auditors. For example, the FTC brought enforcement actions against BJ's Wholesale Club[12] and DSW,[13] both of which were victimized by hackers who tapped into their computer systems to obtain their customers' credit card information, alleging that each company failed to provide reasonable security for the sensitive customer information that it collected and maintained. The FTC required both companies to implement, establish, and maintain comprehensive security programs.

The 2011 settlements by Facebook[14] and Google[15] with the FTC contained, for the first time, requirements for comprehensive (and auditable) privacy programs, patterned on the FTC requirements in the data security area. These program requirements are seen as creating a new and heightened FTC standard for protection of consumer data.

In addition, Chief Privacy Officers (CPOs) are proliferating and gaining in importance in U.S. businesses, adding to the level of American privacy protection. CPOs ensure that there are documented and enforceable compliance and training programs in place within businesses to provide physical, administrative, and technical protections for personal data, and to ensure that new products and services take privacy considerations into account.

In a revealing 2011 *Stanford Law Review* article, University of California at Berkeley Professors Kenneth Bamberger and Deirdre Mulligan presented findings from the first study of corporate privacy management in fifteen years.[16] Bamberger and Mulligan effectively responded to the criticism of the U.S. privacy regime as lacking sufficient legal protections (what they termed "privacy on the books") with a descriptive account of privacy "on the ground." They explored the emergence of the Federal Trade Commission as a privacy regulator; the increasing influence of privacy advocates; market and media pressures for privacy protection; and the rise of privacy professionals, and concluded that, together, these factors played a major role in preventing violations of consumers' expectations of privacy in the United States.

The EU's Across-the-Board Approach to Privacy

In the EU, by contrast, a region-wide Directive, with national laws in twenty-seven jurisdictions to implement the requirements of the Directive, purports to regulate every piece of personal information and is predicated on the notion that privacy is a fundamental human right.[17] Thus, under the approach of across-the-board regulation, there are strict limits on the collection and use of information, although enforcement of those limits has been episodic. Some of the enforcement actions have been criticized, such as a criminal case against Google executives on the grounds of invasion of privacy for a video posted by a YouTube user that depicted a group of Italian students bullying a disabled classmate—a video that Google took down within hours of being notified about it.[18] After removing the video, Google fully cooperated with Italian police to help identify the individual who uploaded the video, and the video was used to convict that individual. Google stated in its official blog that "[i]n these rare but unpleasant cases, that's where our involvement would normally end," but four Google executives were subsequently arrested and charged with violating Italian privacy laws for not blocking the video, and three of them were convicted of the charge.[19]

Another example of controversial enforcement of privacy laws in the EU is a case currently before the European Court of Justice in which the Court has been asked to decide whether Google must honor requests from Spanish citizens who wish to have their data removed from Google's search engine, even when Google is not the creator of the content.[20] These unusual cases are distinct from the FTC's enforcement actions, whose consent decrees have the effect of setting certain standards of conduct for American businesses.

Still, the EU firmly believes its framework is superior to that of the United States, and it has been steadfast in the belief that because the United States does not have an across-

the-board privacy law, its protections are inadequate and transfers of personal data from the EU to the United States must be controlled and subject to special regulation. Viviane Reding, Vice President of the European Commission and Commissioner for Justice, Fundamental Rights and Citizenship, is skeptical of anything less than comprehensive U.S. privacy legislation akin to that in the EU.[21]

The belief on the European side that the United States lacks adequate protections for personal data theoretically could mean that personal data could not be transferred across EU borders to the United States, bringing trans-Atlantic commerce to a grinding halt. To address that unthinkable result, legal mechanisms have been established, requiring expense and burden, to transfer data from the EU to the United States. These mechanisms are the EU-U.S. Safe Harbor,[22] which requires eligible businesses to certify compliance with the Safe Harbor principles of notice, choice, onward transfer, data integrity, security, access, and verification and enforcement; Model Contracts,[23] which are standard contractual clauses approved by EU authorities that must be included in agreements that involve the transfer of personal data outside the EU; and Binding Corporate Rules,[24] which are a set of comprehensive internal policies and procedures that allow for intra-company cross-border transfers, and that must conform to standards approved by EU authorities.

Some had speculated, or perhaps merely hoped, that the current focus on improving the privacy frameworks in the United States and the EU would bring the parties closer to international harmonization or comity. In the past few months recent proposals for privacy reform were announced in Brussels and Washington, but it remains to be seen whether those reforms will act to ease the tensions between the EU and the United States over their respective approaches to privacy, so that there will be convergence and greater cooperation between the two regimes.

[The EU] has been steadfast in the belief that because the United States does not have an across-the-board privacy law, its protections are inadequate and transfers of personal data from the EU to the United States must be controlled and subject to special regulation.

The Proposal for an EU Privacy Regulation

In January, the European Commission unveiled a new proposal for privacy in the EU, calling for a region-wide Regulation that would replace national laws passed in each EU Member State to implement the 1995 Directive on Data Protection and proposing strict new privacy rules (and penalties for violating those rules).[25] Upon final passage of the Regulation, the current 1995 Data Protection Directive would be repealed. The proposed rules are intended to take into account the pervasive new technologies capable of collecting and sharing information about people, and to give individuals more control over their personal information.

- Under the new Regulation, individuals and organizations would only need to deal with one supervisory authority, located in the country of their main establishment or residence, rather than the fragmentary jurisdiction currently provided by the Directive. The Regulation would make organizations outside the EU subject to its provisions if they process personal data to offer goods or services to EU residents, or monitor their behavior. And, if they are subject to its rules, with certain exceptions, they must appoint a representative to whom data protection concerns may be addressed.

  A new principle of accountability would require data controllers to demonstrate their compliance with the law by maintaining extensive documentation on their processing, implementing appropriate security requirements, and performing impact assessments when required. This replaces the current requirement of administrative filings.
- There are new rights to have data deleted (the "right to be forgotten") and to move data from one service to another ("data portability"), which would have a particular effect in relation to social media.
- Borrowing from the U.S.-developed concept of data security breach notification laws, data breaches would have to be reported to supervisory authorities without undue delay and, where feasible, within twenty-four hours—a time period most people experienced with data breach notification view as impractical. "Serious breaches" must also be reported to affected individuals.
- Binding Corporate Rules are expressly recognized in the Regulation as an appropriate form of compliance for international cross-border transfers of data. They will be subject to approval by only *one* supervisory authority, thus shortening the current and very long approval process.
- Where consent is to be a ground for data processing, it must be explicit. Implied consent will no longer be possible and, once given, consent can be withdrawn at any time.
- Fines may be imposed by supervisory authorities for violations of the proposed Regulation, reaching up to 2 percent of an organization's annual turnover in the most serious cases. This potential fining authority for failing to abide by the Regulation's many still-to-be-clarified provisions is viewed by many as potentially draconian.

The draft Regulation has entered the political process of the EU co-decision procedure, under which agreement will need to be reached between the European Parliament and the Council of the European Union. There is no way to predict exactly how long that process may take, but debate has begun.

The Obama Administration's Proposals for Better Privacy

One month after the announcement in Brussels of the proposed Regulation to replace the Data Protection Directive, the Obama Administration announced its "Privacy Blueprint" for the United States, calling for legislation containing a Privacy Bill of Rights and proposing enforceable codes of conduct developed through a so-called "Multistakeholder Process."[26]

The cornerstone of the Administration's privacy blueprint is the Consumer Privacy Bill of Rights, which adapts the decades-old Fair Information Practice Principles to the interconnected and interactive world. The Privacy Bill of Rights applies to commercial uses of personal data and seeks to provide greater privacy protection for consumers and greater certainty for businesses.

There are seven core rights that comprise the Privacy Bill of Rights:[27]

- **Individual Control:** Consumers have a right to exercise control over what personal data organizations collect from them and how they use it.
- **Transparency:** Consumers have a right to easily understandable information about privacy and security practices.
- **Respect for Context:** Consumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.
- **Security:** Consumers have a right to secure and responsible handling of personal data.
- **Access and Accuracy:** Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate.
- **Focused Collection:** Consumers have a right to reasonable limits on the personal data that companies collect and retain.
- **Accountability:** Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

The Administration's blueprint contemplates a multistakeholder approach spearheaded by the Department of Commerce that will produce enforceable codes of conduct that implement the Privacy Bill of Rights. The multistakeholder approach is championed by the Administration due to the "flexibility, speed, and decentralization necessary to address Internet policy challenges."[28] This process is designed to avoid a one-size-fits-all approach and instead opts for flexibility and a tailored standard. In addition to flexibility, the speed with which the multistakeholder process is expected to be able to produce solutions—as compared to the regulatory or law making process—is also appealing due to the constantly evolving nature of privacy issues.

Referring to the differences in national privacy laws that create challenges for businesses that wish to transfer data across national borders, the Administration states that it is "critical to the continued growth of the digital economy that they strive to create interoperability between privacy regimes."[29] The Administration states that it is committed to increasing international interoperability by pursing mutual recognition of commercial privacy frameworks, international codes of conduct based on the multistakeholder process, and bilateral or multilateral enforcement cooperation.

Finally, the Administration calls on Congress to adopt the Consumer Privacy Bill of Rights—noting that Congress should provide the FTC and State Attorneys General with the power to enforce those rights—as well as a national standard for security breach notification, which would replace the patchwork of state breach notification laws that are currently in effect in forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands.

The Federal Trade Commission's Privacy Viewpoint

Shortly after the White House announcement of its privacy proposals, the independent U.S. Federal Trade Commission followed with a report on privacy containing that agency's expectations and hopes for the collection of personal information. Entitled "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," the Report is intended to articulate "best practices" for companies that collect and use consumer data, and to assist Congress as it considers new privacy legislation.[30]

The Report calls for companies to implement (1) privacy by design, (2) simplified consumer choice, and (3) greater transparency; and it recommends that Congress pass baseline privacy legislation. The Report also encourages companies to incorporate substantive privacy protections (e.g., data security, collection limits, retention and disposal practices, and data accuracy) and maintain comprehensive data management procedures throughout product and service life-cycles. In addition, companies are called upon to give consumers a choice about their data at a time and in a context in which the consumer is making the decision, and to obtain affirmative express consent before collecting sensitive data or making material retroactive changes to privacy representations. The Report proposes that privacy notices should be clearer, shorter, and more standardized.

FTC Chairman Jon Leibowitz, commenting on the Report, stated: "If companies adopt our final recommendations for best practices—and many of them already have—they will be able to innovate and deliver creative new services that consumers can enjoy without sacrificing their privacy."[31]

In the Report, the FTC recommends new targeted legislation to address the practices of data brokers, and recognizes that the more sensitive the data, the greater the protections needed. The new framework applies to both online and

offline contexts and to data that is "reasonably linkable" to specific consumers, computers, or devices.

The Report also highlights five "action items" that the FTC will focus on over the next year to promote the new privacy framework:[32]

- **Do Not Track:** The FTC will work with industry to implement an "easy-to-use, persistent, and effective Do Not Track system" which will allow users to opt out of being tracked by online advertising networks and other data collectors.
- **Mobile:** The FTC recommends that companies providing mobile services improve their privacy practices, including through the use of shorter, more meaningful disclosures.
- **Data Brokers:** As mentioned above, the FTC is supporting targeted legislation to provide consumers with greater access to the personal information held by data brokers. It also recommends that data brokers develop a centralized website to identify themselves to consumers, describe their information practices, and detail the access rights and other choices they provide with respect to consumer data.
- **Large Platform Providers:** The FTC is planning to host a public workshop in the second half of 2012 to explore privacy issues associated with "comprehensive" online tracking that can be conducted by ISPs, operating systems, browsers, and other large platforms.
- **Self-Regulatory Codes:** The FTC will participate in the Department of Commerce's upcoming multistakeholder process to develop voluntary, enforceable industry codes of conduct.

Impact of the Recent Proposals

As is evident from these descriptions of the EU, White House, and FTC 2012 proposals, there indeed are common aspects to the EU and U.S. proposals. Both call for implementation of the "Privacy by Design" concept intended to build privacy sensitivity and consideration into every stage of the development of products and services. Both recognize the importance of accountability by those who collect and use personal data. Both reflect the principle that people should not be surprised by the use of their personal data collected for one purpose but used for another purpose. There is no disagreement about the need for informed consent about the collection and use of personal information (although the *kind* of consent envisioned in each jurisdiction differs as to various categories of data). Finally, the U.S. view of what constitutes "personal data" seems to be moving toward the EU's: the FTC refers to data that can be "reasonably linked to a specific consumer, computer or other device,"[33] a standard very close to—and arguably even broader than—the EU definition of personal data.[34]

Big differences in approach emerge from the fact that the United States, while proposing a first-ever federal privacy law with a "Privacy Bill of Rights," still intends to rely on a variety of self-regulation (more precisely, co-regulation, since self-regulatory rules could be enforced by law enforcement). And the U.S. proposed rules do not contemplate a "right to be forgotten," a major feature of the EU proposal and one that First Amendment scholar Professor Jeffrey Rosen has labeled "the biggest threat to free speech on the Internet in the coming decade."[35]

Similarly, there is no right to "data portability" in the U.S. proposals as there is in the EU plan. The EU proposal contemplates broad jurisdiction to enforce its law, even extending to U.S. businesses without a physical presence in the EU, under certain circumstances. And even though the EU has borrowed the data breach notification idea from the United States, it proposes a presumptive obligation to provide notice within twenty-four hours of a breach, a time frame widely regarded as wholly unworkable by those who have worked under the U.S. data breach laws. Finally, the EU proposes a schedule of monetary fines of up to 2 percent of an entity's global worldwide turnover for violations of the proposed Regulation—an amount that many stakeholders view as unreasonable due to the discretion given to enforcers in assessing such a fine.

. . . the U.S. proposed rules do not contemplate a "right to be forgotten," a major feature of the EU proposal . . .

Until the EU Regulation is finalized, businesses need to consider the impact of the proposed new rules on their operations and on their bottom lines. Importantly, they also need to consider whether the proposed rules even are achievable under their particular business models. The period ahead will be one of adjustments to the proposed EU Regulation to make it acceptable to the European Parliament and to the Council of the European Union, the bodies responsible for the co-decision procedure required to adopt the Regulation. Input can be expected from businesses in Europe concerned about the practicality and the effect on trade of the proposed more-restrictive privacy rules. Likewise, in the United States, the exact shape of the new privacy framework is still to be determined, on Capitol Hill and through the work of the Executive Branch.

As things now stand there is a big gap to bridge between the two trans-Atlantic approaches. Both are, in many ways so close, yet very far apart in fundamental respects. ■

[1] What They Know—Wsj.com, http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Apr. 19, 2012) (updated periodically).

[2] Viviane Reding, European Commission Vice President and Commissioner for Justice, Fundamental Rights and Citizenship, and John Bryson, U.S. Secretary of Commerce, EU-US Joint Statement on Data Protection (Mar. 19, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/192&format=HTML&aged=0&language=EN&guiLanguage=en.

[3] Fed. Trade Comm'n, Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (the five FIPPs, as set forth by the FTC, are: (1) Notice/Awareness, (2) Choice/Consent, (3) Access/Participation, (4) Integrity/Security and (5) Enforcement/Redress) (last visited Apr. 19, 2012).

[4] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html (last visited April 19, 2012).

[5] Financial Services Modernization Act (Gramm-Leach-Bliley), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15. U.S.C. §§ 6801–6809).

[6] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C. and 29 U.S.C.).

[7] Children's Online Privacy Protection Act (COPPA), Pub. L. No. 105-277, 112 Stat. 2681-728 (1998) (codified at 15 U.S.C. §§ 6501–6506).

[8] Eli Lilly and Co., FTC File No. 012-3214 (2002), *available at* http://www.ftc.gov/os/caselist/0123214/0123214.shtm (Eli Lilly provided a service to consumers that used the anti-depressant medication Prozac, which enabled the consumers to receive email reminders when it was time to take or refill their medication. In an email communicating the termination of the reminder program, an Eli Lilly employee accidentally disclosed to each participant in the program the email addresses of all other participants, which, the FTC claimed, was contrary to the claims of privacy and confidentiality that Eli Lilly made in its privacy policies.).

[9] Microsoft Corp. FTC File No. 012-3240 (2002), *available at* http://www.ftc.gov/os/caselist/0123240/0123240.shtm (Microsoft made a series of misrepresentations about its data privacy and security practices with regard to data collected through its Passport Web services. Notably, Microsoft claimed that it did not collect any personally identifiable information other than as described in its privacy policy and that it employed a high level of online security with respect to the data collected, claims which the FTC alleged were false and misleading.).

[10] Gateway Learning Corp., FTC File No. 042-3047 (2004), *available at* http://www.ftc.gov/os/caselist/0423047/0423047.htm (Gateway rented consumers' personal information to third parties contrary to statements in its online privacy policy that it would not do so absent the consumer's explicit consent.).

[11] Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted laws that require notification of security breaches that involve protected personal information. These laws require notification in a reasonable amount of time to the individuals whose data was compromised, and in some instances, to state government entities, such as the State Attorney General's office and consumer reporting agencies. *See, e.g.*, Cal. Civ. Code § 1798.82.

[12] BJ's Wholesale Club, Inc., FTC File No. 042-3160 (2005), *available at* http://www.ftc.gov/os/caselist/0423160/0423160.shtm (The FTC alleged that BJ's failed to provide reasonable security for sensitive consumer information. Specifically, the FTC noted that BJ's failed to encrypt the information, stored it for longer than necessary, stored it in an unsecure manner, and failed to take measures to prevent and detect unauthorized access to its networks and systems.).

[13] DSW, Inc., FTC File No. 052-3096 (2005), *available at* http://www.ftc.gov/os/caselist/0523096/0523096.shtm.

[14] Facebook, Inc., FTC File No. 092-3184 (2011), *available at* http://ftc.gov/os/caselist/0923184/index.shtm.

[15] Google, Inc., FTC File No. 102-3136 (2011), *available at* http://www.ftc.gov/os/caselist/1023136/index.shtm.

[16] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247 (2011).

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[18] *See* Nick Leiber, *Why the Google-Italy Privacy Case Matters to Your Business*, Bloomberg Businessweek (Mar. 3, 2010), http://www.businessweek.com/smallbiz/running_small_business/archives/2010/03/why_the_google-.html; *see also* Kit Eaton, *Italy Convicts Google Execs on Privacy Invasion Charges, Revisits Dark Ages*, Fast Co. (Feb. 24, 2010, 7:19 AM), http://www.fastcompany.com/1560995/google-youtube-italy-law-legal-court-bullying-video-students-privacy.

[19] *Serious Threat to the Web in Italy*, Google Official Blog (Feb. 24, 2010, 4:57 AM), http://googleblog.blogspot.com/2010/02/serious-threat-to-web-in-italy.html#!/2010/02/serious-threat-to-web-in-italy.html.

[20] *See* Claire Davenport, *Spain Refers Google Privacy Complaints to EU's Top Court*, Reuters (Mar. 2, 2012, 1:31 PM), http://www.reuters.com/article/2012/03/02/us-eu-google-idUSTRE8211DP20120302 (The individual requests to remove data from Google's search results include a plastic surgeon who wants to have all references to a "botched operation" removed, and a man who wishes that references to the repossession of his home due to non-payment of social security be removed).

[21] Viviane Reding, European Commission Vice President and Commissioner for Justice, Fundamental Rights and Citizenship, Speech at the 2nd Annual European Data Protection and Privacy Conference: The Future of Data Protection and Transatlantic Cooperation (Dec. 6, 2011) ("I am worried that US 'self-regulation' will not be sufficient to achieve full interoperability between the EU and US."), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/851&type=HTML.

[22] *See Welcome to the U.S.-E.U. Safe Harbor*, Export.Gov, http://export.gov/safeharbor/eu/eg_main_018365.asp (last visited Apr. 19, 2012).

[23] *See Model Contracts for the Transfer of Personal Data to Third Countries*, European Comm'n—Justice, http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm (last visited Apr. 19, 2012).

[24] *See Overview—BCR*, European Comm'n—Justice, http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm (last visited Apr. 19, 2012).

[25] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Jan. 25, 2012, *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[26] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), *available at* www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[27] *Id.* at 1.

[28] *Id.* at 23.

[29] *Id.* at 31.

[30] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012) [hereinafter FTC Privacy Report], *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[31] Fed. Trade Comm'n, FTC Issues Final Commission Report on Protecting Consumer Privacy (Mar. 26, 2012), http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

[32] FTC Privacy Report, *supra* note 30, at 72–73.

[33] *Id.* at 22.

[34] The EU definition refers to data that can permit, directly or indirectly, the identification of a natural person (art. 2, Directive 95/46/EC, *supra* note 17). Although the EU definition does not refer to machine addresses, most European data protection authorities believe that IP addresses and other machine identifiers are "personal data" because a machine can in many cases be linked to an individual.

[35] Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88 (2012), *available at* http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.