The Second Wave of Global Privacy Protection: Symposium Introduction

PETER SWIRE*

This Introduction to the Symposium provides a concise history of how privacy has developed as a global and technological policy issue since the rise of the commercial Internet in the 1990s. In brief, the 1990s brought a flurry of activity in privacy protection across the world. The 1995 European Union Data Protection Directive and U.S. laws, such as the Health Insurance Portability and Accountability Act ("HIPAA") and the Children's Online Privacy Protection Act ("COPPA"), are but a few examples of legislation passed to address privacy in the digital age. The first wave of privacy protection was accompanied by significant legal discussion and scholarship in law review articles, symposia, and policy settings. However, during the years following the terrorist attacks of September 11, 2001, legislation and attention to privacy issues cooled as security issues took center stage.

We are now in the midst of a second wave of global privacy initiatives. We have experienced explosive growth in international data flows, online behavioral advertising, social networks, and mobile computing. The European Union has proposed a major overhaul of the 1995 Directive, and comprehensive privacy laws have spread to numerous countries around the world. In the United States, the Obama Administration has proposed a privacy bill of rights for online commerce, and the Federal Trade Commission has pushed numerous privacy initiatives.

To address these developments, the Ohio State Law Journal hosted the Symposium on "The Second Wave of Global Privacy Protection" on November 16, 2012. The Symposium brought together a unique set of panelists to match the nature of the emerging debates. To discuss these global issues, half of the panelists came from outside of the United States. An FTC Commissioner and recent White House official offered their views on policy developments. The academics included both lawyers and technologists. The conference also featured prominent experts from the private sector, where many of the day-to-day decisions affecting privacy are made. Indeed, the Symposium includes the first detailed history of privacy as a profession, co-authored by the President of the International Association of Privacy Professionals, which has grown in a little over a decade to over 13,000 members.[1]

---

*Nancy P. & Lawrence J. Huang Professor of Law and Ethics, Georgia Institute of Technology. The author was faculty advisor for the 2012 Symposium, and at that time was the C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University. For financial support for the Symposium, thanks to the Moritz College of Law, Microsoft, Google, the Center for Interdisciplinary Law and Policy Studies, and the Moritz Intellectual Property Law Society and International Law Society.

[1] Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897, 897 (2013).

This Introduction seeks to provide a readable summary of how information privacy issues have developed since the rise of the Internet in the 1990s. The history here is thematic rather than exhaustive. It explains the perspective of one person who has lived through these events, both as a participant and as an academic observer. An enormous number of persons have worked on an enormous number of privacy and data protection issues that could have been discussed within this history. The history here focuses especially on the United States, with significant attention to Europe, although much of the rest of the world has now adopted privacy laws. The author's apologies in advance for the omissions and simplifications that are part of any attempt to discuss broad themes.

I. THE FIRST WAVE OF GLOBAL PRIVACY PROTECTION

The first wave of global privacy protection crested in the late 1990s, but had numerous sources in earlier developments. For instance, the Fair Credit Reporting Act of 1970 established a U.S. regime for the handling of sensitive financial information. The first set of Fair Information Practices Principles ("FIPPs") was announced by a group chaired by Willis Ware in the U.S. Department of Health, Education, and Welfare in 1973.[2] In Europe, Sweden passed the first national data protection law in 1970, and such laws spread over time.[3] Globally, the Council of the Organization for Economic Co-operation and Development adopted privacy guidelines in 1980, providing a widely recognized set of definitions for FIPPs.[4]

The rise of the Internet greatly increased public attention to information privacy issues. Hard as it may be to believe for students today, commercial activity on the Internet was not permitted until 1992.[5] The Internet then grew explosively during the 1990s, accompanied both by great excitement about what it could foster and great concern about possible privacy and other downsides. One common theme was that, "with the click of a mouse," private personal information could be transferred to many and distant recipients.[6]

The rise of the Internet occurred as the European Union was finalizing work on its Data Protection Directive, which was issued in 1995 and went into effect

---

[2] *See generally* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973).

[3] PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 22 (1998).

[4] *See* Michael Kirby, The History, Achievement and Future of the 1980 OECD Guidelines on Privacy 1, 3 (Mar. 10, 2010), *available at* www.oecd.org/sti/ieconomy/44945835.doc.

[5] Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847, 860 (2003).

[6] Peter P. Swire, The Administration Response to the Challenges of Protecting Privacy 7 (Jan. 8, 2000) (unpublished manuscript), *available at* http://www.peterswire.net/pspublications-unpub.htm (quoting President Clinton statement about "click of a mouse").

in 1998.[7] The rationale for the Directive was based on two key concepts. First, the European Union was designed to be a common market, and it was thus vital to have rules that allowed for the free flow of goods and information within that market area. Along with this reason to encourage greater information flows, the EU based its data protection rules on the view that individuals have fundamental rights in the personal data about themselves.

To implement these ideas of free flow of data and protection of fundamental rights, the 1995 Data Protection Directive required member states to write national legislation that provided for a detailed set of FIPPs, including notice, user consent, access, and security. Each member state created an independent data protection authority, and enforcement by these authorities has increased over time. Importantly to EU-U.S. relations, the Directive had detailed provisions in Articles 25 and 26 that set limits on sending personal data out of the EU unless there was "adequate" protection of privacy by the recipient of the data.[8] The rationale was that it would violate the fundamental rights of Europeans if their data was processed overseas without adequate protections. Based on my discussions with EU data protection experts, I believe that many of them hoped that the United States and other countries would respond by passing comprehensive privacy laws similar to the Directive. Roughly speaking, other major economies have now done so, but the United States has not.

By the late 1990s, privacy policy in the United States was thus being driven by two key factors—the rise of the Internet and the possibility of a trade war with Europe. The Federal Trade Commission played a key role in structuring public debate about privacy and the Internet. Leaders in that effort included FTC Commissioner Christine Varney, as well as FTC Chairman Robert Pitofsky and Director of the Bureau of Consumer Protection Jodie Bernstein. The biggest policy innovation was that commercial activities on the Internet were governed by Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive" trade practices.[9] The FTC during this period prodded industry to post privacy policies; violations of those policies then became enforceable as a deceptive practice. During this period, the FTC pushed industry groups to create codes of conduct, building on the long-standing FTC practice of encouraging self-regulation in advertising and other areas. In addition, FTC leadership used a combination of carrot and stick to prompt industry efforts—if industry acted in good faith on privacy then the stick of comprehensive legislation would not be deployed.[10]

---

[7] *See* Council Directive 95/46, art. 12, 1995 O.J. (L 281) 42 (EC). For discussion of the history and intent of the Directive, see generally SWIRE & LITAN, *supra* note 3; Bartosz M. Marcinkowski, *Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard*, 74 OHIO ST. L.J. 1167 (2013).

[8] Council Directive 95/46, arts. 25–26, 1995 O.J. (L 281) 45–46 (EC).

[9] 15 U.S.C. § 45(a)(1) (2006).

[10] The FTC issued a series of privacy reports in this period, including a 2000 report where a majority of the Commissioners recommended enacting online privacy legislation. FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC

The Clinton Administration coordinated closely with the FTC on privacy during this period. The Administration had multiple considerations in forming its privacy policy. In addition to responding to Internet privacy concerns and the EU Directive, the Administration was trying to find a middle way between updating privacy protections while also favoring as light a regulatory touch as possible for the Internet. At the time that I was serving as Chief Counselor for Privacy in 1999 and 2000, the Administration had settled into the following position. We supported legislation for sensitive data in particular sectors, but were not prepared to support legislative mandates for the Internet and the economy as a whole. During this period, the Administration made major efforts to implement laws and regulations for the health care and financial services sectors, under the HIPAA and the Gramm–Leach–Bliley Act of 1999 ("GLBA"). We also supported the Children's Online Privacy Protection Act of 1998, implemented by the FTC. But, as of 2000, we were not quite ready to say that we favored comprehensive privacy legislation.

The politics of what seemed possible certainly influenced this position, but so did awareness that the legal system was facing a complex and unprecedented set of issues in seeking to regulate online privacy. My view is that, as a society, we were moving steeply up the learning curve on the issue of privacy protection. As the Clearwater and Hughes history of the privacy profession shows, the first prominent use of the term "chief privacy officer" was not until 1999.[11] There simply were very few privacy professionals to draft, interpret, and comply with new privacy laws. In writing the HIPAA and GLBA rules, we encountered numerous issues with no close precedent. To give one example, HIPAA applied to health information about a particular individual, but not to "de-identified" data. For this key definition of what was covered by the law, where was the line between "identified" and "de-identified"? After much work and public comment, we issued a definition of "de-identified" that has governed ever since.[12] But similar challenges existed throughout the drafting process, and we were concerned that comprehensive online privacy legislation could have many and significant unintended consequences for the rapidly evolving Internet.

The peak of the first wave of global protection came at the turn of the millennium. The importance of privacy was illustrated by a Wall Street Journal/NBC poll from September 1999, which asked Americans what concerned them most in the coming century. "Loss of personal privacy" topped the list, as the first or second concern of 29% of respondents. None of the other issues, including terrorism, world war, and global warming had a score higher than 23%.[13] During this period, public-interest privacy groups gained in staff

---

MARKETPLACE 36 (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf.

[11] Clearwater & Hughes, *supra* note 1.

[12] 45 C.F.R. § 164.514(b) (2012).

[13] *Our Expectations: Medical Advances—and the Loss of Privacy*, WALL ST. J., Sept. 16, 1999, at A10.

and visibility.[14] Academics and policy makers contributed to a growing literature on privacy issues, such as a high-profile symposium in the Stanford Law Review in 2000.[15]

A large set of policy initiatives went into effect as well. In 2000, the United States and EU completed negotiations of the Safe Harbor agreement, which continues in force as of this writing in 2013.[16] The Safe Harbor created a legal framework for a company to export data from the EU to the United States with many but not all of the legal protections in the EU Directive, if the company promises to submit to an enforcement regime. During this short period, other staples of U.S. privacy protection also moved forward. In addition to the HIPAA, GLBA, and COPPA rules, covering a large portion of the U.S. economy, the FTC began regular enforcement under Section 5, federal agencies posted privacy policies, and privacy impact assessments became a best practice for federal agencies. In the fall of 2000, the Clinton Administration supported legislation to raise the legal standards before law enforcement could access e-mails, and the bill was criticized by leading Republicans for not being protective enough on privacy.[17] President Bush entered office in 2001, but surprised many observers by deciding to let the HIPAA medical privacy rules go into effect.[18] Many Internet privacy bills were being considered by the Congress, and enactment seemed a distinct possibility.

II. THE EFFECT OF THE 9/11 ATTACKS

With the attacks of September 11, 2001, everything changed.[19] The new focus was overwhelmingly on security rather than privacy. The Congress quickly passed the USA-PATRIOT Act of 2001, which was unrecognizably less protective of privacy than the provisions being debated in Congress for e-mail and other access the year before. The reaction in Europe was similar, with numerous statutory and practical changes that expanded surveillance activities.[20] As we now know, the U.S. government created the Terrorist

---

[14] COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 31–32 (2008) (discussing EPIC, "a public interest research center").

[15] *See* Symposium, *Cyberspace and Privacy: A New Legal Paradigm?*, 52 STAN. L. REV. 987 (2000).

[16] For current information on the Safe Harbor, see *Safe Harbor*, EXPORT.GOV, http://export.gov/safeharbor/ (last updated July 1, 2013).

[17] For discussion of the proposed legislation, see Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1308–09 n.10 (2004).

[18] Clearwater & Hughes, *supra* note 1.

[19] For a critical discussion of the idea that "everything changed," see Swire, *supra* note 17, at 1342–48. For one example of changes, see generally Yofi Tirosh & Michael Birnhack, *Naked in Front of the Machine: Does Airport Scanning Violate Privacy?*, 74 OHIO ST. L.J. 1263 (2013).

[20] "A significant development in Germany since 9/11, and, indeed, since the end of the Cold War, has been a steady stream of legislation that expands the powers of the [intelligence and law enforcement agencies] . . . and an increase in their ability to work

Screening Program and other measures to increase drastically the acquisition of communications information without a warrant.

Two oft-repeated phrases exemplified the change. In the wake of the bombings, many stressed the need to "connect the dots"—to use personal information intensively to detect and prevent the next group of terrorists from pulling off an attack. Vendors of information systems claimed that their databases could have connected the dots and spotted the 9/11 bombers in advance, if only those pesky privacy laws had not stood in the way. The second idea was that agencies and companies had to abandon the old principle of "need to know." Need to know was essentially a data minimization principle—only the individuals who needed to see data should see it, to protect privacy but also to reduce the risk of national security leaks. The new idea, championed by the 9/11 Commission and others, was that we should shift from "need to know" to "need to share." The walls between databases should be torn down, on this view, so that vital information would be available to the full range of analysts who might spot and prevent the next attack.[21]

With so much emphasis on information sharing, Congress lost interest in regulating information usage in the private sector. Although Internet privacy bills were introduced and considered in hearings, nothing came close to passage. Without the threat of legislation, the energy went out of many of the self-regulatory efforts that industry had created during the first wave.[22] Meanwhile, at the FTC, the agency focused its privacy efforts on areas where concrete harms could be proved, such as identity theft or weak security measures. The broader set of concerns covered by privacy as a fundamental right received less attention.

Negotiations between the United States and the EU also demonstrated the shift. The Safe Harbor of 2000 in effect created requirements on U.S. companies that wished to export personal data from Europe. By contrast, the most prominent privacy negotiations after 9/11 concerned U.S. government access to passenger name records.[23] The United States sought these records in hopes of detecting possible terrorists before they entered the country. Rather

---

together and share information." Paul M. Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, 2 INT'L DATA PRIVACY L. 289, 296 (2012); *see also* Ian Brown, *Government Access to Private-Sector Data in the United Kingdom*, 2 INT'L DATA PRIVACY L. 230, 235 (2012) (describing broad access to communications by UK authorities after 9/11).

[21] I have discussed the history and theory of information sharing during this period in Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951 (2006).

[22] *The Need for Privacy Protections: Is Industry Self-regulation Adequate?: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 112th Cong. 4–5 (2012) (statement of Peter Swire).

[23] Marjorie J. Yano, *Come Fly the (Unfriendly?) Skies: Negotiating Passenger Name Record Agreements Between the United States and European Union*, 5 ISJLP 479, 479–81 (2010).

than negotiating new privacy limits on data flows, the PNR accord focused on large-scale new information sharing.

In the period after 9/11, new privacy developments did continue, often with modest public attention. Privacy protection became more institutionalized. The first wave had created new legal regimes that now caused companies to hire privacy professionals to address HIPAA, GLBA, COPPA, Safe Harbor, and organizations' privacy policies. With the appointment of Nuala O'Connor Kelly in 2003, the Department of Homeland Security appointed the first chief privacy officer required by U.S. statute.[24] In the trans-Atlantic setting, a slow start for Safe Harbor evolved over time into the governance structure for thousands of companies' transfer of data from the EU to the United States. Within the EU, compliance with the 1995 Data Protection Directive became more institutionalized, with an increasing body of non-binding but influential guidance from a group of regulators known as the Article 29 Working Party.[25] Around the globe, a steady stream of countries adopted privacy legislation for the first time, in large part in order to qualify for what the EU considered "adequate" privacy protection.

One other type of privacy requirement also snuck up on the private sector during this period, with considerable effects. California was the first state to have a data breach law go into effect, in 2003, requiring notice to individuals whose sensitive personal information had been accessed by hackers or other unauthorized persons.[26] The idea spread quickly. Today, almost all states have a data breach law, and the idea has spread to other countries and is included in the draft Regulation being considered in the European Union. The spread of data breach laws gave a large boost to the practice of privacy; in the event of a breach, lawyers and forensic information experts get hired to craft the response, and computer security departments have an important justification for greater spending in order to reduce the risks and costs of data breaches.

III. THE SECOND WAVE OF GLOBAL PRIVACY PROTECTION

Compared to the period after the 9/11 attacks, we are now in a second wave of global privacy protection. A number of technological and market developments together rival the effect in the first wave created by the beginning

---

[24] *Privacy in the Hands of the Government: The Privacy Officer for the Department of Homeland Security and the Privacy Officer for the Department of Justice: Hearing Before the Subcomm. on Commercial and Admin. Law of the H. Comm. on the Judiciary*, 109th Cong. 39 (2006), *available at* http://commdocs.house.gov/committees/judiciary/hju27606.000/hju27606_0.HTM (testimony of Sally Katzen, Professor, George Mason University Law School).

[25] *Article 29 Working Party*, EUR. COMMISSION, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last visited Oct. 14, 2013) (homepage of the Article 29 Working Party).

[26] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915 (2007).

of the commercial Internet. Consider four examples. First, social networks such as Facebook enormously increase the quantity and variety of information online about many individuals. Second, the pervasiveness of smartphones and other mobile computing devices increases the usefulness of computing in our daily lives, while also leaving detailed records of our location and other activities. Third, online behavioral advertising has rebounded from a low level a decade ago to become a large industry that gathers and acts on detailed records of individuals' activities across multiple sites. Fourth, the emergence of cloud computing means that far more of our personal information is stored in remote data centers, often in other countries. Taken together, these trends of social networks, mobile computing, online advertising, and cloud computing raise numerous issues that go beyond the core privacy topic of the 1990s, the rules for a website gathering data about a user who visits that site.

These developments became more important as the memories of 9/11 began to fade. By the 2006 election in the United States, opposition to the Iraq War and concerns about warrantless wiretapping were two issues that contributed to the Democratic Party taking control of both the Senate and the House of Representatives.[27] In contrast to the "security trumps privacy" atmosphere of 2001, there were major debates in Congress about whether the USA-PATRIOT Act and Foreign Intelligence Surveillance Act had gone too far toward intruding on personal privacy. Most of the surveillance authorities survived this congressional scrutiny, but privacy had clearly re-emerged as a salient political issue.

The fading of 9/11 and the new technological developments sparked intense press coverage of commercial privacy topics, such as front-page stories about Facebook's privacy policies and the "What They Know" series by the *Wall Street Journal*,[28] documenting the surprising technical ways that users are often tracked across the Internet. The financial crisis that peaked in 2008 and 2009 temporarily pulled political attention away from privacy, but privacy policy initiatives were building at the FTC, in the Obama Administration, in global standards bodies, and in the European Union.

With the 2009 appointment by President Obama of Chairman Jon Leibowitz, the FTC expanded its privacy enforcement and policy activities. The FTC brought enforcement proceedings against many of the largest Internet companies, including Facebook, Google, and Twitter, resulting in consent decrees under which the companies agreed to institute comprehensive privacy programs for a decade or longer. The FTC, which as an independent agency develops its own policy views distinct from the administration's, also intensified its privacy workshops and reports. In early 2012, the FTC issued the

---

[27] For one contemporaneous account of the importance of Iraq and warrantless wiretapping to the election, see John Amato, *The Faulty List of Glenn Reynolds*, CROOKS & LIARS (Oct. 17, 2006, 7:19 PM), http://crooksandliars.com/2006/10/18/the-faulty-list-of-glenn-reynolds.

[28] *What They Know*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Oct. 14, 2013).

wide-ranging *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*.[29] This report highlighted three themes: a broader view of privacy harms than the FTC had held after 9/11, the importance of global interoperability for data flows and privacy protections, and the desirability of legislation to augment self-regulatory efforts.[30] Overall, the report reflected what was likely the most ambitious view by any U.S. agency to date about what should be done to protect privacy.

Also in early 2012, the Obama Administration itself released a white paper entitled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*.[31] This white paper announced support for what it called a "Consumer Privacy Bill of Rights," embodying the principles of individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.[32] The white paper also announced support for U.S. legislation to adopt the Consumer Privacy Bill of Rights, marking the first time that any U.S. administration had explicitly called for such legislation.[33]

These FTC and Obama Administration reports supported what they call "multistakeholder processes" to develop enforceable privacy codes of conduct.[34] One of these, convened by the U.S. Department of Commerce, has resulted in a draft standard for privacy notices for mobile applications.[35] Another such process was convened in the World Wide Web Consortium, the international standards body that developed HTML and other major web standards.[36] This "Do Not Track" process has sought to build a consensus standard among over 100 stakeholders groups including privacy advocates, online advertisers, browsers, and regulators. The basic idea of this effort has been to develop a mechanism in users' browsers to indicate individuals' choices

---

[29] *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012) [hereinafter FTC PROTECTING CONSUMER PRIVACY], *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[30] *Id.* at 7–13.

[31] *See generally* 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.

[32] *Id.* at 1–2.

[33] *Id.* at 35.

[34] *Id.* at 2; FTC PROTECTING CONSUMER PRIVACY, *supra* note 29, at 3.

[35] For information about the Mobile Application Transparency process, see *Privacy Multistakeholder Process: Mobile Application Transparency*, NAT'L TELECOMM. & INFO. ADMIN., http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency (last visited Oct. 14, 2013).

[36] For the activities of the Tracking Protection Working Group, where the Do Not Track standard has been considered, see *Tracking Protection Working Group*, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/2011/tracking-protection/ (last visited Oct. 14, 2013). From November 2012 until August 2013, the author was co-chair of this Working Group.

about whether they wish to have their browsing activity tracked across multiple websites. Despite intense efforts to craft consensus, deep-seated disagreements among participants have thus far prevented any consensus standard emerging for Do Not Track.

As these U.S. and global standards efforts have unfolded, the European Union has moved forward with the first comprehensive overhaul of the 1995 Data Protection Directive. In 2012, the European Commission, led by European Commissioner for Justice, Fundamental Rights, and Citizenship Viviane Reading, proposed a draft Regulation that would, if enacted, become enforceable law throughout the European Union.[37] The draft Regulation would re-write numerous aspects of the Directive.[38] For instance, it would provide a new "right to be forgotten," empowering individuals to demand that online services not display categories of documents about the individual.[39] It would provide a new "right to data portability," ensuring that individuals could easily shift all of their data from one online service to another.[40] It would broaden the jurisdictional reach of EU data protection requirements, more clearly than before applying even to websites based only in other countries. In addition, it would greatly increase the possible fines for violations, authorizing penalties of up to two percent of global revenues.

The Call for Papers for the Ohio State Symposium on the Second Wave of Global Privacy Protection went out in 2012 as these initiatives were becoming prominent in the FTC, the Obama Administration, global standards groups, and the European Union. The Symposium featured a keynote discussion with FTC Commissioner Julie Brill and Danny Weitzner, who spearheaded the Obama Administration's privacy white paper. Four panels addressed the major dimensions of current privacy debate: Private Sector and Technology; Private Sector and Globalization; Public Sector and Technology; and Public Sector and Globalization. The diverse and important papers on these topics are included in this volume, and will be available online through the Ohio State Law Journal.

IV. CONCLUSION

The first wave of global privacy protection coincided with the amazing growth of the Internet during the 1990's. By 2001, the European Union had implemented its Data Protection Directive, the United States had created privacy laws for health care, financial services, and other sectors, and the Safe

---

[37] *See generally Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012).

[38] *See id.* at 1–2.

[39] Jeffrey Rosen, *The Right To Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf.

[40] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335, 336–37 (2013).

Harbor was in place to create a legal structure for flows of personal information across the Atlantic. Privacy policy became much less visible in the wake of the attacks of September 11, 2001, as security concerns and information sharing became the dominant policy themes. A new set of technological and market changes emerged by the time that President Obama was elected in 2008, notably including social networks, mobile computing, online behavioral advertising, and cloud computing. We are seeing the second wave of global privacy protection debates in response to these changes.

Simultaneous with this story of policy ebbs and flows, there has been a steady increase in the professionalization and institutionalization of privacy protection. Companies and government agencies have employed a steadily increasing number of privacy professionals. A much larger number of experts is participating in the policy, technological, and legal debates of the second wave of global privacy protection.

Writing in the fall of 2013, it is difficult to predict what lasting legal changes will emerge from the second wave. At the time of this writing, the U.S. Congress has been gridlocked on most issues, and the obstacles to U.S. privacy legislation continue to appear considerable. In Europe, the fate of the draft Regulation is unclear. It would be risky, however, to assume that most or all new privacy protections will be blocked. The level of privacy debate is intense. The first wave culminated in multiple laws and new practices that have had enduring effect, and so might the second wave. Meanwhile, as Australian privacy expert Graham Greenleaf discussed in a panel at the Symposium, the number of countries with data privacy laws has continued to rise, and climbed past 100 in 2013.[41] More of those laws over time have real enforcement effect, so we see more legal and national sources for privacy protection than previously.

The 2013 Snowden leaks about U.S. surveillance, encryption, and other practices also create an unknown but potentially large effect on global privacy protections. The European Parliament showed renewed interest in the draft Regulation in the wake of the first group of Snowden leaks.[42] President Obama has announced a Review Group on Intelligence and Communications Technology, with recommendations due by early 2014.[43] The Congress is considering a variety of new bills. In 2012, this Symposium already contemplated a second wave of global privacy protection. Time will tell

---

[41] Graham Greenleaf, *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*, J.L. INFO. & SCI. (forthcoming 2013), *available at* http://ssrn.com/abstract=2280877 (manuscript at 3).

[42] In September 2013, the European Parliament nominated Edward Snowden for the Sakharov Prize for Freedom of Thoughts, considered Europe's top human rights awards. Dan Bilefsky, *Snowden Among Nominees for a European Human Rights Prize*, N.Y. TIMES, Sept. 17, 2013, http://www.nytimes.com/2013/09/18/world/europe/snowden-nominated-for-human-rights-award.html.

[43] The author was appointed as one of five members of this Review Group.

whether we are living through a mere ripple, an actual tidal wave, or something in between.