Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014) Intersentia-January 2014

Bridging the Divide: A Perspective on U.S.-EU Commercial Privacy Issues and Transatlantic Enforcement Cooperation

By Commissioner Julie Brill

Lately, we hear a great deal about the contentious relationship between the U.S. and EU on privacy issues, fraught with both philosophical differences and practical challenges that have been exacerbated by recent revelations of government surveillance for national security purposes.[1] This narrative overlooks what I believe is at the core of the relationship between the U.S. and EU frameworks for protecting consumer privacy: an overwhelming degree of commonality on our bedrock privacy principles and the goals we aim to achieve.[2] In my view, the real story is the similarities, not the differences. I think we should focus less on the divide and more on bridging that divide. At times, the water between us may seem tumultuous, but if we take a closer look at what is happening on the ground, we will find cooperative activities that are building bridges to connect us, increase our mutual understanding, and strengthen our longstanding bilateral relationship. While it may not make the headlines, our cross-border privacy enforcement cooperation plays an integral role in fortifying our evolving and vitally important transatlantic relationship.

In this paper,[3] I examine the relationship between the U.S. and EU on commercial privacy issues and explore how transatlantic enforcement cooperation helps sustain that relationship.

- Section I explains the historical origins of the U.S. Federal Trade Commission's role in privacy enforcement.

---

[1] *See* Glen Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: the Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (JUN. 9, 2013), *available at* http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. These national security issues are outside the scope of this paper, as well as the jurisdiction of the U.S. Federal Trade Commission. Moreover, I believe that commercial privacy and concerns about citizens' privacy from governmental surveillance are both important, but separate and distinct issues. *See* Julie Brill, Commissioner, Fed. Trade Comm'n, European Institute Opening Panel Remarks, *available at* http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf.

[2] James Q. Whitman, *The two Western cultures of privacy: dignity versus liberty*, 113 YALE L. J. 1151 (2004).

[3] Commissioner Brill thanks her Attorney Advisor, Shaundra Watson, for her invaluable assistance in preparing this paper.

- Section II describes the FTC's current privacy and data security enforcement activities.
- Section III outlines current policy developments to enhance the U.S. privacy framework.
- Section IV identifies the commonalities between the U.S. and EU privacy norms and discusses the need to strive for interoperability to accommodate some of the inevitable differences between our privacy frameworks.
- Section V describes efforts to pursue cross-border privacy enforcement cooperation.
- Finally, Section VI highlights multilateral policy development, bilateral agreements, and other tools to enhance cooperation.

I. The U.S. Federal Trade Commission's Role in Privacy Enforcement

On both sides of the Atlantic, policy makers are grappling with how best to reframe our privacy norms in light of the rapid change in Internet and mobile technologies. In the United States, my agency – the Federal Trade Commission – is uniquely situated to play a critical role in answering this important policy question. After all, the FTC was the creation of the father of modern privacy law, Louis Brandeis.

Before he became a justice on the United States Supreme Court, before he wrote his famous dissent in *Olmstead v. United States* where he argued that "against the government", Americans have "the right to be let alone",[4] Louis Brandeis was one of the Progressive Era's preeminent "trustbusters", leading a crusade against the large steel trusts and other monopolies that were engulfing the U.S. economic system. His call to cut back on the trusts' economic power focused the 1912 presidential election on the "larger debate over the future of the economic system and the role of the national government in American life."[5] After President Woodrow Wilson won that election with Brandeis's help, President Wilson asked Brandeis to present specific recommendations aimed at solving the problem of the trusts. Brandeis conceived of the Federal Trade Commission, an independent, bi-partisan Commission led by five Commissioners. At Brandeis' urging, Congress empowered the FTC to investigate and prohibit unfair methods of competition with a "broad and flexible mandate, wide-ranging powers, and the ability, at its best, to respond to the needs of changing times."[6]

Today, the FTC is the only federal agency in the United States that addresses consumer protection and competition issues in broad sectors of the economy. Our dual mission is to prevent business practices that are anticompetitive, and to stop deceptive or unfair practices that harm consumers. We seek to accomplish our twin goals without unduly burdening legitimate business activity, and we do so through a variety tools given to us by Congress.

---

[4] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[5] ARTHUR S. LINK., WOODROW WILSON AND THE PROGRESSIVE ERA, 1910-1917 (Harper & Brothers, 1954).

[6] Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 ANTITRUST L. J. 1, 5-6 (2003).

The FTC has a long tradition of using its authority against unfair or deceptive practices to protect consumer privacy. We take action against companies that fail to comply with their own privacy and data security policies or otherwise misrepresent their information management practices. And, just as importantly, we also address unfair collection and use of personal information and unfair data security practices that inflict harm on consumers that they cannot reasonably avoid, and that does not offer offsetting benefits to consumers or competition.[7]

As specific privacy and data security issues have arisen over the past 40 years, Congress has supplemented the FTC's broad remedial authority by charging us and other agencies with enforcing other privacy laws, including laws designed to protect financial[8] and health information,[9] children's information,[10] and information used for credit, insurance, employment and housing decisions.[11]

II. Current U.S. Enforcement Efforts to Protect Privacy and Data Security

At the FTC, protecting consumer privacy is one of our most important missions. We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of companies that operate throughout the Internet and mobile ecosystem. Our most well-known cases – against Google,[12] Facebook,[13] and Myspace[14] – have led to orders that, for the next 20 years, govern the data collection and use activities of these companies. And in each of these cases we have addressed the companies' failure to comply with the U.S.-EU Safe Harbor Framework.

In addition, we have brought myriad cases against companies that are not household names, but whose practices infringe on consumer privacy. We've sued companies spamming

---

[7] 15 U.S.C. § 45(n).

[8] Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12 and 15 U.S.C.).

[9] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 & 42 U.S.C.); Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. §§ 201 note, 300jj *et seq*., 17901.

[10] Children's Online Privacy Protection Act of 1998, Pub. L. 105-277, 112 Stat. 2581-728 (codified as amended at 15 U.S.C. §§ 6501-6505).

[11] Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681-1681x).

[12] In the Matter of Google, Inc., FTC File No. 102 3136 (Oct. 13, 2011), *available at* http://ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf (decision and order).

[13] In the Matter of Facebook, Inc., FTC File No. 092 3184 (July 27, 2012), *available at* http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf (decision and order).

[14] In the Matter of Myspace, LLC, FTC File No. 102 3058 (Aug. 30, 2012) *available at* http://ftc.gov/os/caselist/1023058/120911myspacedo.pdf (decision and order).

consumers and installing spyware on their computers.[15] We've challenged companies that failed to properly secure consumer information.[16] We have sued ad networks,[17] analytics companies,[18] data brokers,[19] and software developers.[20] We have brought actions against traditional credit reporting agencies and other entities that failed to comply with the Fair Credit Reporting Act.[21] We have vigorously enforced the Children's Online Privacy Protection Act.[22] We have also targeted app developers as well as handheld device manufacturers engaged in inappropriate data collection and use practices.[23]

As part of our ongoing effort to address privacy issues in the changing technological landscape, we recently brought our first action involving the Internet of Things.[24] In that case,

---

[15] *See, e.g.*, *FTC v. Flora*, 2011 U.S. Dist. LEXIS 121712 (C.D. Cal. Aug. 12, 2011), *available at* http://www.ftc.gov/os/caselist/1023005/110929loanmodorder.pdf; *FTC v. CyberSpy Software*, LLC, *et al*., No. 08-CV-01872 (M.D. Fla. Apr. 22, 2010), *available at* http://www.ftc.gov/os/caselist/0823160/100602cyberspystip.pdf (stipulated final order).

[16] *See, e.g.,* In the Matter of Twitter, Inc., FTC File No. 092 3093 (March 3, 2011) *available at* http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf (decision and order).

[17] *See*, *e.g.*, In the Matter of Epic Marketplace, Inc. et al., FTC File No. 112 3182 (Mar. 13, 2013), *available at* http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf (decision and order).

[18] *See, e.g.*, In the Matter of Upromise, Inc., FTC File No. 102 3116 (Apr. 3, 2012), *available at* http://www.ftc.gov/os/caselist/1023116/120403upromisedo.pdf (decision and order).

[19] *See, e.g., U.S. v. Spokeo, Inc*., No. 12-CV-05001 (C.D. Cal. June 19, 2012), *available at* http://ftc.gov/os/caselist/1023163/120612spokeoorder.pdf (consent decree and order); In the Matter of Filiquarian Pub. LLC et al., FTC File No. 112 3195 (Apr. 30, 2013), *available at* http://www.ftc.gov/os/caselist/1123195/130501filquariando.pdf (decision and order).

[20] *See, e.g.*, In the Matter of DesignerWare LLC, FTC File No. 112 3151 (Apr. 11, 2013), *available at* http://www.ftc.gov/os/caselist/1123151/designerware/130415designerwaredo.pdf (decision and order).

[21] *See, e.g., U.S. v. Certegy Check Servs., Inc.,* No. 1:13-cv-01247 (D.D.C. 2013) available at http://www.ftc.gov/os/caselist/1123184/130815certegyorder.pdf) (final judgment and order)*;* In re Filiquarian Publ'g, LLC, *FTC File No. 112 3195 (Apr. 30, 2013), available at* http://www.ftc.gov/os/caselist/1123195/130501filquariando.pdf (decision and order).

[22] *See, e.g., U.S. v. Artist Arena, LLC*, No. 12-CV-7386 (S.D.N.Y. Oct. 3, 2012), *available at* http://www.ftc.gov/os/caselist/1123167/121003artistarenadecree.pdf (stipulated final order).

[23] *See, e.g., U.S. v. Path*, *Inc.*, No. 13-CV-0448 (N.D. Cal. Feb. 8, 2013) (Consent decree and order), *available at* http://www.ftc.gov/os/caselist/1223158/130201pathincdo.pdf; In the Matter of HTC, Inc., FTC File No. 122 3049 (June 25, 2013), *available at* http://www.ftc.gov/os/caselist/1223049/130702htcdo.pdf (decision and order).

[24] In the Matter of TRENDnet, Inc., FTC File No. 122 3090 (Sept. 4, 2013), *available at* http://www.ftc.gov/os/caselist/1223090/130903trendnetorder.pdf (agreement containing consent order); *see also* Julie Brill, Op-Ed., *From Regulators, Guidance and Enforcement*, N.Y. TIMES, Sept. 8, 2013, *available at* http://www.nytimes.com/roomfordebate/2013/09/08/privacy-and-the-internet-of-things/regulators-must-guide-the-internet-of-things.

the company failed to secure the software for its Internet-accessible video cameras, which put hundreds of private lives on public display.[25]

All told, we have brought hundreds of privacy enforcement actions over the last several years:

- 44 cases involving inappropriate collection and use of consumer data (since 1999);
- 21 cases involving violations of children's privacy (since 2000);
- 47 cases against entities that had poor data security practices (since 2000);
- over 100 cases involving spammers and spyware (since 2001);
- over 100 violations of our Do Not Call laws (since 2003); and
- over 30 cases involving violations of the Fair Credit Reporting Act (since 2003).

This impressive body of enforcement work also has secured hundreds of millions of dollars in penalties and restitution for consumers.

Together, these enforcement efforts have established what some scholars call "the common law of privacy" in the United States, in which the FTC articulates – to industry, defense counsel, consumer groups and other stakeholders – in an incremental, but no less effective way, the privacy practices that are deceptive or unfair.[26]

III. Current Policy Developments to Enhance Privacy Norms in the U.S.

As a complement to our privacy enforcement work, the FTC is actively engaged in ongoing research and policy development to improve privacy protection in light of rapid technological change. Last year, the FTC issued its landmark privacy report in which the agency developed a new framework for addressing privacy in the U.S., including best practices for companies to follow based on three core principles: privacy by design, simplified choice, and greater transparency around data collection and use.[27] We called on companies to operationalize the report's recommendations by developing better just-in-time notices and robust choice

---

[25] *See id.*

[26] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (forthcoming 2014), *available at* http://ssrn.com/abstract=2312913. *See also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011), (discussing how chief privacy officers reported that "state-of-the-art privacy practices" need to reflect both established black letter law and FTC cases and best practices, including FTC enforcement actions and FTC guidance); Christopher Wolf, *Targeted Enforcement and Shared Lawmaking Authority As Catalysts for Data Protection in the United States,* BNA Privacy and Security Law Report, Oct. 25, 2010), *available at* http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf (FTC consent decrees have "created a 'common law of consent decrees,' producing a set of data protection rules for businesses to follow").

[27] *See* FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 26, 2012) *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf [hereinafter FTC Privacy Report].

mechanisms, particularly for health and other sensitive information.[28] We have held workshops and issued reports on cutting-edge issues, including facial recognition technology,[29] kids apps,[30] mobile privacy disclosures,[31] and mobile payments.[32] The FTC is actively studying the data broker industry to learn more about the ways that companies collect, buy, and sell consumer data. We hope to issue a report later this year on how data brokers could improve their privacy practices.[33]

Various policymakers are working on improving U.S. data security and privacy laws to better address current challenges. In last year's privacy report, the FTC indicated its support for baseline privacy legislation[34] and called on Congress to enact data broker legislation that would increase the transparency of the practices of data brokers.[35] In addition, U.S. lawmakers have recommended legislation that would protect children from online tracking.[36] And of course the Obama Administration has been actively working on privacy legislation that would implement its Consumer Privacy Bill of Rights.[37]

IV. Recognizing Commonalities and Striving for Interoperability

As the FTC's privacy report, the Obama Administration's Consumer Privacy Bill of Rights, and the FTC's other policy and enforcement initiatives illustrate, the U.S. aims to achieve many of the same objectives that are outlined in the draft EU data protection legislation.[38] For

---

[28] *See id.*

[29] *See* Press Release, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), *available at* http://ftc.gov/opa/2012/10/facialrecognition.shtm.

[30] *See* FED. TRADE COMM'N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* (December 2012), *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.

[31] *See* Press Release, FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures (Feb. 1, 2013), *available at* http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm.

[32] *See* FED. TRADE COMM'N, *Plastic, Paper, or Mobile? An FTC Workshop on Mobile Payments* (March 2013), *available at* http://www.ftc.gov/os/2013/03/130306mobilereport.pdf.

[33] *See* Press Release, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 12, 2012), *available at* http://www.ftc.gov/opa/2012/12/databrokers.shtm.

[34] *See* FTC Privacy Report, *supra* note 27, at 13.

[35] *See* FTC Privacy Report, *supra* note 27, at 14.

[36] *See* Do Not Track Kids Act, H.R. 1895, 112th Cong. (2011), *available at* https://www.govtrack.us/congress/bills/112/hr1895/text.

[37] *See* WHITE HOUSE, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. [hereinafter "White House Privacy Report"]; *See also* Alex Byers, *White House Pursues Online Privacy Bill Amid NSA Efforts*, Politico (Oct. 7, 2013, 5:03 AM), http://www.politico.com/story/2013/10/white-house-online-privacy-bill-nsa-efforts-97897.html.

instance, on both sides of the Atlantic, we are striving to protect children's privacy, spur companies to implement privacy by design, increase transparency, strengthen data security, and encourage companies to adopt accountability measures.[39] As the technological challenges facing the EU and the U.S. have grown, so has our common effort to protect consumers. In some instances, we differ on how to achieve these common goals. For example, we both believe that consumer consent is important, but we have different approaches as to when and how that consent should be obtained. The particular solutions we develop may differ, but the challenges we face and our focus on solving them are the same.

Of course, our privacy frameworks — which are based on different legal and cultural traditions — influence how we address these common challenges. In a world with diverse privacy frameworks, interoperability is critical. We should work together to preserve existing mechanisms and develop new ways that allow our different privacy frameworks to co-exist while facilitating the flow of data across borders. The U.S.-EU Safe Harbor Framework, which enables the lawful transfer of personal data from the EU to the U.S., is vital to preserving interoperability.[40]

Most importantly from my perspective, the Safe Harbor provides the FTC with an effective tool to protect the privacy of EU citizens. Our cases against Google,[41] Facebook,[42] and Myspace[43] — which each protect EU consumers as well as American consumers, and together protect 1 billion consumers worldwide — have demonstrated the effectiveness of this Framework, as well as the FTC's determination to enforce it.

V. Cross-Border Enforcement Cooperation Enhances Our Ability to Address Global Challenges

One key component of interoperability is the ability to cooperate on enforcement matters, including those that involve potential violations of Safe Harbor. In light of our increasingly interconnected world, the FTC has devoted significant resources toward enhancing international

---

[38] *See* FTC privacy report, *supra* note 27; White House Privacy Report, *supra* note 37; *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 and on the Free Movement of such Data (General Data Protection Regulation)*, COM (2012) 11 amended (Oct. 21, 2013), *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf (listing the European Parliament Committee on Civil Liberties, Justice, and Home Affairs's latest amendments to Articles 1-91).

[39] *See id.*

[40] *See* U.S. DEP'T OF COMMERCE, *Safe Harbor Privacy Principles* (Jul. 21, 2000), *available at* http://export.gov/safeharbor/eu/eg_main_018475.asp.

[41] *See* In the Matter of Google, Inc., *supra* note 12.

[42] *See* In the Matter of Facebook, Inc., *supra* note 13.

[43] *See* In the Matter of Myspace, LLC., *supra* note 14. As of the date this paper was submitted for publication, MySpace is no longer in the U.S.-EU Safe Harbor Framework. However, the safeguards contained within the MySpace order continue to protect U.S. and EU consumers alike.

enforcement cooperation so that we are better able to address global challenges. The U.S. SAFE WEB Act of 2006, which the U.S. Congress recently renewed, gives the FTC necessary tools to address cross-border privacy and consumer protection issues.[44] We can act to protect consumers in Europe and other areas of the globe from bad actors in the U.S.,[45] and we can share confidential or other sensitive information that we obtain in our investigations with agencies in other countries if they are investigating violations "substantially similar" to practices prohibited by laws that the FTC enforces.[46] Among other things, one of the factors that the law requires us to consider when deciding whether to assist an agency in another country is whether the agency is willing to assist us if we need help in a future case.[47]

It is this indispensible, yet much overlooked, work of on-the-ground enforcement cooperation – sharing experiences and information, identifying targets, locating and sharing evidence, and returning money to aggrieved consumers – that strengthens our relationships with our foreign counterparts. As of mid-2012, the FTC has used its authority under the U.S. SAFE WEB Act to provide evidence in response to 63 information-sharing requests from 17 foreign agencies in nine countries,[48] and issued 52 administrative subpoenas in 21 investigations on behalf of nine agencies in five countries,[49] including enforcement authorities in the EU.[50] As we strive to expand our international enforcement cooperation, we should be cognizant of the lingering challenges to day-to-day cooperation and the importance of flexible legal frameworks that facilitate data flows across borders, particularly in the context of privacy and consumer protection enforcement. We have used our authority under the U.S. SAFE WEB Act to further this goal and have also promoted similar approaches in privacy frameworks around the world.

VI. Multilateral Policy Development, Bilateral Agreements, and Other Tools to Enhance Cooperation

In addition to the key, yet unsung, efforts in specific cross-border enforcement cases, we

---

[44] Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 ("U.S. SAFE WEB Act"), Pub. L. No. 109-455, 120 Stat. 3372 (2006) (codified in scattered sections of 15 U.S.C. and 12 U.S.C. § 3412(e)).

[45] 15 U.S.C. § 45(a)(4).

[46] 15 U.S.C. § 46(f)(2), 57b-2(b)(6).

[47] 15 U.S.C. § 46(j)(3)(A).

[48] *Hearing on Reauthorizing the U.S. SAFE WEB Act of 2006*, 112th Cong. (2012) (Prepared Statement of the Federal Trade Commission), at 5, a*vailable at* http://www.ftc.gov/os/testimony/120712safeweb.pdf.

[49] *See id.*

[50] *See, e.g.,* FTC, *The U.S. SAFE WEB Act, The First Three Years: A Report to Congress* (Dec. 2009), *available at* http://www.ftc.gov/os/2009/12/P035303safewebact2009.pdf, at 8. The U.S. SAFE WEB Act also provides the FTC with the ability to arrange staff exchanges with foreign agencies to further enhance cooperation. 15 U.S.C. § 57c-1. Since the law was passed, the FTC has hosted 62 international colleagues who have worked with FTC staff on a wide range of issues handled by the agency.

have embarked on numerous initiatives to deepen our ties to the data protection and privacy authorities around the globe, and in the EU in particular. In April 2013, I met with EU data protection authorities at the 90th Article 29 Data Protection Working Party meeting in Brussels, where we explored ways to leverage our common ground.[51] We have continued this dialogue with our EU counterparts on an ongoing basis. We have also taken concrete steps to pursue more effective bilateral cooperation with EU data protection authorities. We recently entered into a Memorandum of Understanding with the Irish Office of the Data Protection Commissioner to enhance our enforcement cooperation on a bilateral basis.[52] This MOU creates a framework for increased and more streamlined privacy enforcement cooperation that could be useful in other bilateral relationships.

The FTC, like its EU counterparts, also participates in multilateral organizations to enhance privacy enforcement cooperation. As a member of the U.S. delegation to the OECD's Working Party on Information Security and Privacy (WPISP), FTC staff has worked closely with its counterparts in the EU and other OECD member countries to develop the OECD Council's Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy.[53] The OECD's influential recommendation encouraged OECD member countries to improve their domestic legal frameworks to facilitate cross-border cooperation and to provide mutual assistance to other countries on privacy enforcement matters.[54] FTC staff, along with colleagues from the EU, also actively participated in the OECD WPISP's Privacy Expert Working Group, which recently conducted a review of the OECD's seminal 1980 Privacy Guidelines.[55] The OECD's revised guidelines, released in September 2013, build on its previous work and further emphasizes the need for OECD member countries to establish privacy authorities, provide them with sufficient resources, and facilitate their ability to cooperate in privacy enforcement matters.[56]

As part of its broader effort to increase international privacy enforcement cooperation, the FTC has worked extensively with its EU colleagues in the OECD and elsewhere to enhance our efforts to protect consumers from unwanted emails and texts, or spam. Notably, FTC staff,

---

[51] *See* Press Release, Article 29 Data Protection Working Party Meeting with FTC Commissioner Julie Brill (Apr. 29, 2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130429_pr_april_plenary_en.pdf.

[52] Memorandum of Understanding Regarding Mutual Assistance in the Enforcement of Laws Protecting Personal Information in the Private Sector, U.S. FED. TRADE COMM'N-DATA PROTECTION COMMISSIONER OF IRELAND, June 2013, *available at* http://www.ftc.gov/os/2013/06/130627usirelandmouprivacyprotection.pdf.

[53] OECD, Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy (2007), *available at* http://www.oecd.org/internet/ieconomy/38770483.pdf.

[54] *See id.*

[55] *See* OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[56] *See* OECD, OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Pesonal Data (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

representatives from the EU, and our counterparts from elsewhere around the globe have collaborated on a number of initiatives relating to spam enforcement cooperation, including:

- The OECD Council's Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam, which encouraged member countries to ensure that their domestic frameworks made cooperation with other authorities and the private sector possible. [57]
- The London Action Plan, a public-private enforcement network that addresses spam and other cybersecurity issues.[58] The FTC has worked with participating authorities on their respective enforcement of anti-spam laws, such as laws in EU member states implemented pursuant to the e-Privacy Directive.[59]
- Memoranda of Understanding with EU and other authorities, including the Spanish and UK data protection authorities, to improve spam enforcement cooperation.[60]

Through the Global Privacy Enforcement Network (GPEN),[61] the FTC has sought to develop practical cooperative tools that will enhance cooperation on a wide range of privacy and data security issues with EU data protection authorities and privacy authorities around the world. We have joined our EU counterparts in participating in coordinated GPEN enforcement sweeps, sending warning letters earlier this year to 10 data brokers who may have been violating the Fair Credit Reporting Act.[62] In addition, we have actively participated in an effort led by our United Kingdom and Canadian counterparts to launch the International Conference of Data Protection and Privacy Commissioners' initiative to address challenges in global privacy enforcement

---

[57] *See* OECD, Council Recommendation on Cross-Border Co-operation in the Enforcement of Laws Against Spam, (Apr. 13, 2006), http://www.oecd.org/fr/sti/ieconomie/oecdrecommendationoncross-borderco-operationintheenforcementoflawsagainstspam.htm.

[58] *See* The London Action Plan: International Spam Enforcement Cooperation, *available at* http://londonactionplan.org/the-london-action-plan/ (last visited Nov. 5, 2013).

[59] *See Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37*. The FTC has also cooperated with non-EU countries to combat international spamming enterprises. *See, e.g., FTC v. Atkinson*, No. 1:08-cv-05666 (N.D. Ill. Nov. 4, 2009). In conjunction with other relevant members of the London Action Plan, the FTC has also worked to improve international cooperation with foreign agencies—including authorities in Europe—that enforce privacy and consumer protection laws prohibiting unsolicited telephone communications.

[60] *See* Memorandum of Understanding on Mutual Enforcement Assistance in Commercial Email Matters, U.S. FED. TRADE COMM'N-AGENCIA ESPANOLA DE PROTECCION DE DATOS, F.T.C., Feb. 24, 2005, *available at* http://www.ftc.gov/os/2005/02/050224memounderstanding.pdf; Memorandum of Understanding on Mutual Enforcement Assistance in Commercial Email Matters, U.S. FED. TRADE COMM'N-U.K. OFFICE OF FAIR TRADING-U.K. INFORMATION COMMISSIONER, H.M. SECRETARY OF STATE FOR TRADE AND INDUSTRY IN THE U.K.-AUSTRALIAN COMPETITION AND CONSUMER COMMISSION-AUSTRALIAN COMMUNICATIONS AUTHORITY, F.T.C., Oct. 16, 2003, *available at* http://www.ftc.gov/os/2004/07/040630spammoutext.pdf.

[61] *See* GLOBAL PRIVACY ENFORCEMENT NETWORK, https://www.privacyenforcement.net/ (last visited Oct. 28, 2013).

[62] *See* Press Release, FTC Warns Data Broker Operations of Possible Privacy Violations; Letters Issued As Part of Global Privacy Protection Effort, http://www.ftc.gov/opa/2013/05/databroker.shtm.

cooperation.[63] Notably, the European Data Protection Supervisor has been a valuable partner in both the GPEN and International Conference initiatives. As part of its work in implementing the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules, the FTC has not only worked with APEC member economies to develop a Cross-Border Privacy Enforcement Arrangement,[64] it has also collaborated with data protection officials from the EU and APEC region to explore how to facilitate interoperability between the APEC Cross-Border Privacy Rules and EU member states' binding corporate rules.[65]

Conclusion

All of these initiatives – cooperating on individual investigations, participating in multilateral policy development, entering into bilateral agreements, and developing practical tools for cross-border enforcement – enhance our collective ability to protect consumers from inappropriate data collection and use practices, and from violations of other laws designed to ensure privacy and data security. The global community of privacy and data protection authorities should be proud of these collective accomplishments, and yet we should not rest on our laurels, as we have only scratched the surface of what is truly possible in terms of effective international enforcement cooperation.

There are certainly hundreds of privacy officials all over the world who have labored tirelessly to move the ball of enhancing consumer privacy and strengthening international cooperation forward. Among those officials, Peter Hustinx's contributions in the field of privacy — and public service generally — are unparalleled. As we forge ahead to solidify existing relationships and build new ones, it will be difficult if not impossible to replace the invaluable insight, strategic vision, and leadership that Peter selflessly provided during his more than forty years in public service. And while we will miss Peter, both professionally and personally, his legacy will continue to inspire us to put "more effective protection in practice."[66]

Another great leader, Winston Churchill, also knew a thing or two about the importance of international cooperation. He said that "[a] pessimist sees the difficulty in every opportunity; an optimist sees the opportunity in every difficulty." I, like Churchill, am an inveterate optimist.

---

[63] *See* Resolution on International Enforcement and Cooperation, 35th International Conference of Data Protection and Privacy Commissioners, September 23-26, 2013, *available at* https://privacyconference2013.org/web/pageFiles/kcfinder/files/4.%20Enforcement%20coordination%20resolution%20EN%20.pdf.

[64] *See* ASIA-PACIFIC ECONOMIC COOPERATION, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx (last visited Oct. 31, 2013).

[65] *See* Press Release, Article 29 Data Protection Working Party Promoting Cooperation on Data Transfer Systems Between Europe and the Asia-Pacific, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130326_pr_apec_en.pdf.

[66] *See* Peter Hustinx, Closing Remarks, 35th International Conference of Data Protection and Privacy Commissioners (Sept. 26, 2013), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-09-26_Speech-Warsaw_EN.pdf.

I know there are many who believe that the gap between the EU and U.S. privacy regimes is growing, and that practical solutions to stem the tide of increased distrust and divergent views are slipping from our grasp. However, I continue to see an opportunity for recognizing how much we have in common, and attaining a mutual respect for our differences. Transatlantic enforcement cooperation plays a critical role in building trust and achieving real victories on behalf of consumers, efforts which will continue to bridge the divide between us.