Commissioner Julie Brill's Opening Panel Remarks
European Institute
Data Protection, Privacy and Security:
Re-Establishing Trust Between Europe and the United States
October 29, 2013

Good morning. I would like to thank Joëlle Attinger and the European Institute for inviting me to speak to you today. I am honored to be here with Jan Philipp Albrecht, Jim Halpert, and our esteemed colleagues from the European Parliament's LIBE committee. Welcome to Washington. I am very happy to say that we are once again open for business.

Your visit comes on the heels of a significant milestone in Brussels. Just last week, the LIBE committee reconciled thousands of amendments to the proposed EU data protection legislation, passed an initial draft, and authorized negotiations with the Council.[1]

In the U.S., we have followed the EU's revision of its privacy framework closely. Although we often hear about the differences between the U.S. and EU privacy frameworks, I think it's important to highlight that we share many of the same goals. The draft EU data protection legislation that the LIBE committee approved last week adopts measures that echo many of the FTC's efforts here in the U.S., including calling on firms to:

- Adopt privacy by design;
- Increase transparency;
- Enhance consumer control;
- Improve data accuracy and consumers' access to their data;
- Strengthen data security;
- Provide parental control over information companies collect about children; and
- Encourage accountability.[2]

As the technological challenges facing the EU and the U.S. have grown, so has our common effort to protect consumers. In some cases, we differ on how to achieve these common goals.[3] For example, we both believe that consent is important, but we have different approaches

[1] *See* Press Release, European Parliament Committee on Civil Liberties, Justice, and Home Affairs, Civil Liberties MEPs pave the way for stronger data protection in the EU (Oct. 21, 2013), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20131021IPR22706%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN.

[2] *See 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); 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.

as to when and how that consent should be obtained. The particular means we choose may differ, but the challenges we face and our focus on solving them are the same.

Despite our commonalities, recent events make the title of today's discussion – "Re-Establishing Trust Between Europe and the United States" – particularly relevant. There is no doubt that the revelations about the National Security Agency's surveillance programs have severely tested the close friendship between the US and many of our European colleagues. Let me take a moment to address this issue.

Edward Snowden's disclosures about the NSA have sparked a global debate about government surveillance and its impact on individual privacy.[4] There is great interest in the United States and in Europe in having the revelations about the NSA serve as a catalyst for change in the way governments engage in surveillance to enhance national security. As some of you know, I have spent a lifetime working on privacy issues, so it should be no surprise that this is a debate I personally welcome, as my own view is that it is a conversation that is overdue.

But I also think it is important that we have the right conversation — one that is open and honest, practical and productive. As we move forward with this conversation, we should keep in mind that consumer privacy in the commercial sphere, and citizens' privacy in the face of government surveillance to protect national security, are two distinctly separate issues. I and my colleagues at the FTC focus on the appropriate balance between consumer privacy interests and commercial firms' use of consumer data, not on national security issues. And I believe the recent revelations should spur a separate and equally long overdue conversation about how we can further enhance consumer privacy and increase transparency in the commercial sphere.

The FTC is the premier U.S. consumer protection agency focused on commercial privacy. The FTC has a great track record of using its authority to go after unfair or deceptive practices that violate consumer privacy, and vigorously enforcing other laws designed to protect financial[5] and health[6] information, information about children[7], and credit information used to make decisions about credit, insurance, employment, and housing.[8]

---

[3] *See* Julie Brill, Commissioner, Fed. Trade Comm'n, Address at the Mentor Group Forum for EU-US Legal Economic Affairs: Remarks to the Mentor Group (Apr. 16, 2013), *available at* http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf.

[4] *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.

[5] 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.).

[6] 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. 300jj et seq. §§17901 et seq.

[7] 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).

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. We have brought enforcement actions against well-known companies, such as Google,[9] Facebook,[10] Twitter,[11] and Myspace.[12]

We have also brought myriad cases against companies that are not household names, but whose practices violated the law. We've sued companies that spammed consumers,[13] installed spyware on computers,[14] failed to secure consumers' personal information,[15] deceptively tracked consumers online,[16] violated children's privacy laws,[17] inappropriately collected information on consumers' mobile devices,[18] and failed to secure Internet-connected devices.[19] We have obtained millions of dollars in penalties and restitution in our privacy and data security cases, and placed numerous companies under 20-year orders with robust injunctive provisions.

---

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

[9] 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).

[10] 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).

[11] 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).

[12] 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).

[13] *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.

[14] *See, e.g., 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).

[15] *See, e.g.*, In the Matter of LabMD, FTC File No. 102 3099 (Aug. 28, 2013), *available at* http://www.ftc.gov/os/adjpro/d9357/130829labmdpart3.pdf (administrative complaint).

[16] *See, e.g.,* In the Matter of Epic Marketplace, Inc., *et al.*, FTC File No. 112 3182 (Dec. 5, 2012), *available at* http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf (decision and order).

[17] *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).

[18] *See 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).

[19] *See* 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.

As a complement to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. In addition to our landmark privacy report issued last year, we have addressed cutting-edge privacy issues involving facial recognition technology,[20] kids apps,[21] mobile privacy disclosures,[22] and mobile payments.[23]

In light of our increasingly interconnected world, the FTC has devoted significant time to enhancing international privacy enforcement cooperation so that we are better able to address global challenges. We continue to foster a strong relationship and engage in ongoing dialogue with European data protection authorities. We meet regularly with EU DPAs, and in April I met with the entire Article 29 Working Party. The Article 29 Working Party has been kind enough to recognize the FTC as a crucial partner in privacy and data protection enforcement.[24] And the Working Party, like the FTC, has welcomed the ongoing dialogue and constructive cooperation between us, and stressed the need for further transatlantic cooperation, especially in enforcement matters, in order to achieve our common goals.[25] Indeed, the FTC's recent Memorandum of Understanding with the Irish DPA establishes a good framework for increased, more streamlined, and more effective privacy enforcement cooperation.[26] And just last month, we worked very closely with our EU and Canadian counterparts to launch the International Conference of Data Protection and Privacy Commissioners' initiative to address challenges in global privacy enforcement cooperation.[27]

---

[20] *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.

[21] *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.

[22] *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.

[23] *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.

[24] 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.

[25] *See Id.*

[26] 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.

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

Another critical role played by the FTC is to enforce the U.S.-EU Safe Harbor framework.[28] We know that Safe Harbor has received its share of criticism, particularly in the past few months. We've read the news reports and heard about the recent Parliamentary hearings about Safe Harbor.[29] Given the active debate over Safe Harbor right now, I'd like to address head-on the contention in some quarters that Safe Harbor isn't up to the job of protecting EU citizens' data in the commercial sphere.

First, the FTC vigorously enforces the Safe Harbor. As the Safe Harbor program has grown over the past decade, so has the FTC's enforcement activity. Since 2009, we have brought ten Safe Harbor cases.[30] When Safe Harbor was established, the FTC committed to review on a priority basis all referrals from EU member state authorities.[31] With few referrals over the past decade, we have taken the initiative to proactively look for Safe Harbor violations in every privacy and data security investigation we conduct. That is how we discovered the Safe Harbor violations of Google, Facebook, and Myspace in the last few years. These cases demonstrate the enforceability of Safe Harbor certifications and the high cost that companies can pay for non-compliance. The orders in Google, Facebook, and Myspace require the companies to implement comprehensive privacy programs and subject the companies to ongoing privacy audits for 20 years.[32] Violations of these orders can result in hefty fines, as Google discovered when we assessed a $22.5 million civil penalty against the company last year for violating its consent decree.[33] The FTC orders against Google, Facebook, and Myspace help protect over a billion consumers worldwide, hundreds of millions of whom reside in Europe. These cases demonstrate that Safe Harbor gives the FTC an effective and functioning tool to protect the privacy of EU citizen data transferred to America. Without the Safe Harbor, my job to protect EU consumers' privacy, where appropriate, would be much harder. In an era where we face many threats to privacy, Safe Harbor has been an effective solution, not the problem.

Second, going forward, the FTC will continue to make the Safe Harbor a top enforcement priority. Indeed, we have opened numerous investigations into Safe Harbor compliance in recent months. We will continue to welcome any substantive leads, such as the complaint we received in the past month from a European-based consumer advocate alleging a large number of Safe Harbor-related violations. And, let me be clear, we take this recent complaint very seriously. Of

---

[28] *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.

[29] *See LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, Sixth Hearing* (Oct. 7, 2013), *available at* http://www.europarl.europa.eu/ep-live/en/committees/video?event=20131014-1500-COMMITTEE-LIBE.

[30] *See* Legal Resources, Bureau of Consumer Protection Business Center, U.S. FED. TRADE COMM'N, *available at* http://business.ftc.gov/legal-resources/2840/3.

[31] *See* Letter from Robert Pitofsky, Chairman, Fed. Trade Comm'n to John Mogg, Director, Directorate-General XV, European Commission (Jul. 14, 2000), *available at* http://export.gov/static/sh_en_FTCLETTERFINAL_Latest_eg_main_018455.pdf.

[32] *See* Google, *supra* note 9; Facebook, *supra* note 10; Myspace, *supra* note 12.

[33] *See* Press Release, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), *available at* http://ftc.gov/opa/2012/08/google.shtm.

course, as we do in every instance, we take the necessary time to separate fact from fiction. And, as I am sure many in this audience would appreciate, we also proceed carefully to provide proper notice and appropriate levels of due process. If we discover in our investigations that companies have committed Safe Harbor-related law violations, we will take appropriate enforcement actions.

As I mentioned earlier, I think it is healthy to have a vigorous debate over how to appropriately balance national security and privacy, but that ongoing debate should not be allowed to distort discussions in the commercial sphere about role of the Safe Harbor in protection consumer privacy. The EU itself has created national security exemptions in its existing data protection laws,[34] and the European Commission proposed such exemptions for government surveillance in its draft data protection regulation.[35] In other words, the EU has justifiably recognized the need to tackle their member states' national security issues separately. Safe Harbor is no different and warrants a similar approach. Just as the EU Data Protection Directive was not designed to address national security issues, neither was the Safe Harbor. Whatever the means to transfer data about European consumers for commercial purposes – whether to countries whose laws are deemed "adequate", through approved contractual clauses, or by way of the Safe Harbor – all these transfer mechanisms are subject to national security exceptions. The difference is that, for Safe Harbor violations, the FTC is the cop on the beat. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection.

I know that some of you in this room may have taken a different view of the Safe Harbor framework. I hope my thoughts give you cause to reexamine the virtues of the Safe Harbor system. As the draft regulation continues its journey through the process of review and adoption, I am hopeful that we can continue to work together to promote both the free flow of data and strong consumer privacy protections.

And while it may not make the headlines or the nightly news, in the midst of all of the recent developments at home and across the pond, our efforts to enhance privacy enforcement cooperation continue to build trust day by day. We want to continue to develop these ties of cross border law enforcement cooperation – including Safe Harbor enforcement – that enhance privacy and data security – as these are the ties that build rather than erode trust, the ties that bind rather than divide us. We have worked extensively with our friends in the EU on these and other issues, and we look forward to continuing that collaboration to enhance privacy protection for consumers on both sides of the Atlantic.

Thank you.

---

[34] Directive 1995/46/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, 2005 O.J. (L 281) 31, 42, *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[35] *See 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 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.