IAPP Europe Data Protection Congress
Commissioner Julie Brill's Keynote Speech
"At the Crossroads"
December 11, 2013
Brussels, Belgium

Thank you Florian Thoma for that kind introduction, and thanks to Trevor Hughes, Brendan Lynch, Rita Di Antonio and IAPP for inviting me to speak this morning. It is a pleasure to be here today. I always enjoy the opportunity to engage with my European colleagues, and I see many familiar faces in the audience today.

Oliver Wendell Holmes, Sr., an American poet, Paris-trained physician, and father of the famous Supreme Court Justice, once said, "The great thing in this world is not so much where we are, but in what direction we are moving." These words should have particular significance to you in this room, you who care deeply about privacy issues. In our world – the world of privacy – we find ourselves at a crossroads, contemplating the direction in which we will move. The path that we choose next will have significant consequences. It will define the scope of protections for important privacy rights, and help determine, in some small part, the future of the transatlantic relationship.

As we contemplate our future course, we need to ask whether we – industry and regulators, as well as governments – will be able to work together to develop ways to both protect consumer privacy and spur innovation? At this pivotal fork in the road, I believe that the answer to this question is "yes". And although there may be obstacles along the way to obtaining the twin goals of protecting consumer privacy and spurring innovation, we should be mindful of the words of Eleanor Roosevelt: "A stumbling block to the pessimist is a stepping-stone to the optimist."

I am an inveterate optimist. I believe the work that all of you do within your companies – your collaboration with your engineers, computer programmers, marketing teams and others to address privacy issues raised by your companies' products and services – does an enormous amount of good, both for your companies and for consumers. For those of you who work at companies – either US-based or based here in Europe – that intersect with the US regulatory regime, you know that one of the ways you can offer your company some of the best advice about appropriate privacy practices is to study closely the work of the US Federal Trade Commission.

The Federal Trade Commission has a very broad mandate. We engage in competition and consumer protection enforcement, covering a wide swath of the economy. We have become the leading privacy regulator in the United States by building a robust data protection and privacy enforcement program that focuses on both traditional offline products and services, as well as on the evolving digital and mobile marketplace. The FTC uses its authority to stop unfair or deceptive practices that violate consumers' privacy or place consumers' data at risk.[1] We also

[1] 15 U.S.C. §45(a).

vigorously enforce laws that protect consumers' financial[2] and health[3] information, information about children,[4] and information used to make decisions about credit, insurance, employment, and housing.[5]

We have used our broad enforcement authority to challenge inappropriate privacy and data security practices of well-known companies, such as Google,[6] Facebook,[7] Twitter,[8] and MySpace.[9] We also have brought myriad cases against companies that are not household names, but whose practices violated the law. We've sued companies that spammed consumers,[10] installed spyware on computers,[11] failed to secure consumers' personal information,[12] deceptively tracked consumers online,[13] violated children's privacy laws,[14] and inappropriately

---

[2] 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.).

[3] 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.

[4] 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).

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

[6] 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).

[7] 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).

[8] 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).

[9] 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).

[10] *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.

[11] *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).

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

[13] *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).

[14] *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).

collected information on consumers' mobile devices.[15] We have obtained millions of dollars in penalties and restitution, and placed dozens of companies under 20-year orders requiring better privacy and data security practices, as well as mandatory audits. And perhaps most importantly for you in this audience today, many of the FTC's privacy and data security enforcement actions have a global impact, protecting consumers in the U.S., EU, and around the world.

As a complement to our privacy enforcement work, the FTC is actively engaged in policy development to improve privacy protection in this era of rapid technological change. We issued a landmark privacy report last year,[16] and we have addressed cutting-edge privacy questions involving facial recognition technology,[17] kids apps,[18] mobile privacy disclosures,[19] and mobile payments.[20]

Two new emerging technologies — big data analytics and the Internet of Things — have the potential to accelerate data collection and use in ways that are not transparent to consumers, and that could potentially harm them. As a result, the FTC has sought to learn more about the privacy implications of these technologies through our in-depth study of the data broker industry[21] and our workshop last month on the Internet of Things.[22] I have personally urged industry to provide consumers with innovative and immersive tools to increase transparency of practices using these new technologies, to provide consumers with more effective choice

---

[15] *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).

[16] *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*].

[17] *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.

[18] *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.

[19] *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.

[20] *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.

[21] *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.

[22] *See* Press Release, FTC Announces Agenda, Panelists for Upcoming Internet of Things Workshop (Nov. 8, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/11/ftc-announces-agenda-panelists-upcoming-internet-things-workshop.

mechanisms, and to better protect sensitive information – such as information about health and sexual orientation – that is used or created through these new technologies.[23]

And I have made specific recommendations in these two areas. First, with respect to data brokers, I've launched an initiative I call "Reclaim Your Name". "Reclaim Your Name" urges data brokers to take four steps to increase transparency and choice in the invisible world of data profiling and data analytics, by: (1) helping consumers find out how data brokers are collecting and using data; (2) giving them access to information that data brokers have compiled about them; (3) allowing them to opt out if they learn a data broker is selling their information for marketing purposes; and (4) providing them the opportunity to correct errors in information used for substantive decisions.[24] With respect to the world of connected devices – refrigerators, cars, fitness bands – what we at the FTC call the "Internet of Things" – the question is not whether our privacy laws and best practices apply – they clearly do. Rather the question is how they should be applied to products where the consumer may not even realize she has a device that is connected and collecting personal information, and the device itself may have no consumer interface.[25] In this context, I have encouraged companies to return to some fundamental principles: embrace privacy by design and build in protections from the start; ensure that connected devices collect only the data necessary for functioning and that it is held securely for the minimum time necessary; and, importantly, even if the device has no user interface, create a consumer-friendly dashboard that explains through icons, graphics or other simple terms the data the device collects about consumers, the uses of the data, and who else might see the data.[26]

In short, with respect to cutting-edge technologies that may provide enormous benefits to consumers but also carry with them some real risks to privacy and data security, I have urged industry to choose a path that values privacy as well as innovation by adopting practices that will engender consumer trust so critical to consumer acceptance and enjoyment.

And what about different governments – in particular the United States and the European Union? Will they be able to work together to meet these 21st Century challenges by developing ways to both protect consumer privacy and spur innovation? Once again, I believe the answer is "yes".

---

[23] *See* Julie Brill, Op-Ed., *Demanding Transparency from Data Brokers*, WASH. POST, Aug. 15, 2013, *available at* http://articles.washingtonpost.com/2013-08-15/opinions/41412540_1_data-brokers-fair-credit-reporting-act-data-fuel; Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at 23rd Computers Freedom and Privacy Conference: Reclaim Your Name (June 26, 2013), *available at* http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf.

[24] *See id.*

[25] *See* 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

[26] Julie Brill, Commissioner, Fed. Trade Comm'n, Lecture at the New York University-Poly Sloan Lecture Series: A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data (Oct. 23, 2013), *available at* http://www.poly.edu/sloanseries/reclaim-your-name.php.

I believe that there are important similarities between the U.S. and EU evolving privacy frameworks. As technological challenges facing the U.S. and EU have grown, so has our common effort to protect consumer privacy. The U.S. and EU are both taking steps to:

- Protect children's privacy;
- Spur the adoption of privacy by design;
- Enhance consumer control;
- Increase transparency;
- Improve data accuracy and consumers' access to their data;
- Strengthen data security; and
- Encourage accountability.[27]

The challenges we face and our yearning to address them are largely the same. Yet the specific mechanisms we develop to implement these goals may differ. For example, we both believe that consent is important, but we have different approaches as to when and how that consent should be obtained.

In light of the differences between our privacy frameworks, interoperability is critical. We need to develop and preserve existing mechanisms that help facilitate the flow of information across borders while at the same time protecting consumer privacy. The U.S.-EU Safe Harbor Framework is one important method for achieving this goal.[28] Safe Harbor provides the FTC with a very effective tool for protecting the privacy of EU consumers.

The FTC has vigorously enforced the Safe Harbor. Since 2009, the FTC has brought ten Safe Harbor cases. Although we have received very few referrals from EU member state authorities 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. This is how we discovered the Safe Harbor violations of Google, [29] Facebook, [30] and Myspace. [31] The orders in

---

[27] *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); *FTC Privacy Report*, *supra* note 16.

[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] 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).

[30] 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).

[31] 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). Although Myspace does not

these three cases require the companies to implement comprehensive privacy programs and subject the companies to ongoing privacy audits for 20 years.[32] Our actions against Google, Facebook, and Myspace protect a billion consumers worldwide, including millions of EU citizens.

In addition to our previous enforcement actions, we have opened numerous investigations into Safe Harbor compliance in recent months. We welcome leads and take complaints seriously, such as the recent complaints about a large number of companies submitted by a European-based consumer advocate. If we discover in our investigations that companies have committed Safe Harbor-related law violations, we will take appropriate enforcement actions. The FTC's vigilance in enforcing Safe Harbor violations will continue to be a vital part of the Safe Harbor program in the months and years ahead.

But let me acknowledge the elephant in the room: Safe Harbor has received its share of criticism recently, in large part due to the recent revelations about government surveillance.[33] There is no doubt that these revelations have created tensions in the transatlantic relationship. They have sparked a robust debate in Washington, here and around the globe about government surveillance and its impact on individual privacy. This is a debate I personally welcome, as my own view is that it is a conversation that is overdue. 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.

But I also think it is important that we recognize 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. The EU itself has recognized the distinction between national security and commercial privacy. Indeed, the 1995 EU Data Protection Directive and approved transfer mechanisms, such as model contracts, also have national security exceptions.[34] Simply put, none of these data transfer mechanisms, including Safe Harbor, was designed to address national security issues. As I've said before, Safe Harbor may be an easy target, but I do not believe that it is the right target.[35]

---

currently self-certify to Safe Harbor, the Myspace order still provides privacy protections for both U.S. and EU consumers.

[32] *See* 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); 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); 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).

[33] *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.

[34] *See* 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] Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at Fourth Annual EU Data Protection and Privacy Conference (Sept. 17, 2013), *available at*

In the commercial context, Safe Harbor is an effective mechanism for creating interoperability between the U.S. and EU privacy frameworks, and provides the FTC with an effective enforcement mechanism. In its recent report on Safe Harbor, the European Commission also recognized the value of Safe Harbor and the benefits that cross-border data flows provide to both the U.S. and EU economies.[36] And while I believe that the national security issues will necessarily have to be addressed outside the Safe Harbor context, I think the European Commission's decision to continue the Safe Harbor is a big step in the right direction.

And yet, as with most good things in life – especially those with which we've had almost fifteen years of experience – there is room for improvement. Let me be clear, I strongly support Safe Harbor, and I do not believe that it should be suspended, or renegotiated. Yet there are some concrete steps that could be taken to improve Safe Harbor's usefulness to businesses and consumers. Let me highlight three areas that I believe could enhance the Safe Harbor program: more accessible and affordable Alternate Dispute Resolution mechanisms; increased transparency; and strengthened accountability mechanisms. Others who have closely and carefully analyzed Safe Harbor —such as the Future of Privacy Forum — also recognize its value and successful operation, and at the same time have recommended improvements along these lines.[37] Indeed, the European Commission's report on Safe Harbor indicates its support for further efforts in each of these areas.[38]

First, I strongly support efforts to reduce or eliminate fees for Alternative Dispute Resolution, or ADR, providers. Consumers should not have to pay substantial fees simply to have their complaints heard. Currently, five of the seven major ADR providers offer their services to EU consumers for free, and an estimated 80% of Safe Harbor companies have selected the ADR providers that are free to consumers. The Department of Commerce has successfully reduced the fees for one provider from thousands of dollars to $200. This is certainly a positive development. I think further efforts to reduce or eliminate the remaining ADR fees would be helpful, and I know that my colleagues at the Department of Commerce are committed to continuing to work toward this goal.

Second, I think there should be additional measures to increase transparency in the administration of the Safe Harbor program. These transparency measures could include, as the European Commission noted, requiring more companies to provide links to the Department of Commerce's Safe Harbor website and their chosen ADR provider, in order to make information

---

http://www.ftc.gov/sites/default/files/documents/public_statements/keynote-address-forum-europe-fourth-annual-eu-data-protection-and-privacy-conference/130917eudataprivacy.pdf.

[36] *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM (2013) 847 final (Nov. 27, 2013), *available at* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf [hereinafter *Safe Harbor Report*].

[37] *See* FUTURE OF PRIVACY FORUM, *The US-EU Safe Harbor An Analysis of the Framework's Effectiveness in Protecting Personal Privacy* (December 2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf.

[38] *See Safe Harbor Report*, *supra* note 36.

more easily accessible to consumers.[39] In addition, more could be done to educate European consumers about the Safe Harbor program. The FTC has a section dedicated to Safe Harbor on its Business Center website.[40] I encourage EU DPAs and other relevant stakeholders, particularly those here in the EU, to provide similar educational materials, so that businesses and consumers can better understand the Safe Harbor program and how to exercise their rights.

Third, I believe that stakeholders should consider ways to increase the accountability of companies engaged in cross- border data transfers. Many stakeholders in the US, including the FTC, have recognized the need to enhance accountability in privacy compliance, before issues hit the radar of enforcers like the FTC. Accountability mechanisms can play an important role in ensuring that companies protect the privacy and security of consumers' data regardless of how their data are transferred.[41] We should collectively look closely at these and other measures that might enhance accountability.

I am hopeful that we can work together to address each of the three issues that I have highlighted to implement practical improvements that would meaningfully enhance privacy protections and trust on both sides of the Atlantic.

So as we stand at the crossroads now, let's take the path where new technologies thrive, and longstanding privacy principles are embraced. The path where national governments celebrate their shared values and respect their differences. Rather than building barriers, I for one am interested in building bridges. I call on all stakeholders – including my European colleagues – to join me in this endeavor.

---

[39] *See id.*

[40] *U.S.-EU Safe Harbor Framework*, FED. TRADE COMM'N (Dec. 9, 2013, 4:32 PM), http://business.ftc.gov/us-eu-safe-harbor-framework.

[41] *See, e.g.*, ASIA-PACIFIC ECONOMIC COOPERATION, *The Cross Border Privacy Rules System: Promoting Consumer Privacy and Economic Growth Across the APEC Region* (Sep. 5, 2013), http://www.apec.org/Press/Features/2013/0903_cbpr.aspx (last visited Dec. 11, 2013).