**Forum Europe Fourth Annual EU Data Protection and Privacy Conference**
**Commissioner Julie Brill's Keynote Address**
**September 17, 2013**
**Brussels, Belgium**

Good morning. I would like to thank Forum Europe for the invitation to participate in this important conference today. I am always delighted to have the opportunity to engage with my EU counterparts on issues that are important to all of us, and I see many of my friends in the audience today.

A lot has changed since this past April when I was last in Brussels. The revelations about the U.S. National Security Agency's programs[1] have sparked a global debate about government surveillance and its effect on individual privacy. As many of you know, I have spent a lifetime working on consumer protection and privacy issues, so it should be no surprise that this is a debate I welcome. It is a conversation that is long 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, my personal view is that there are some important facts that we should keep in mind as we collectively attempt to answer some very tough questions:

- First, whether we call privacy a "fundamental right" or a Constitutional right, the U.S., EU, and many other countries around the world place tremendous value on privacy. Our legislative and regulatory frameworks may differ, but the acknowledgment of the need for privacy protections and the principles underlying how we define those protections are, at their core, the same.[2]

- Second, national security exceptions in laws, including privacy laws, are the norm, not the exception, for countries around the globe, including EU Member States and third countries that have received European Commission adequacy determinations.[3] As we revisit the proper scope of government surveillance, the

---

[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.

[2] *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.

[3] *See, e.g.*, 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 [hereinafter "EU Data Protection Directive"]; Personal Information Protection and Electronic Documents Act, R.S.C. 2000, c. 5, 6-8, 11, *available at* http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf (Can.). *See generally* Christopher Wolf, *An Analysis of Service Provider Transparency Reports on Government Requests for Data*, HOGAN LOVELLS (Aug. 27, 2013), http://www.hldataprotection.com/files/2013/08/Hogan-Lovells-White-Paper-Analysis-of-Transparency-Reports.pdf.

sufficiency of procedural safeguards, and how to "balance the ends with the means",[4] we should examine these issues with a global lens, as these challenges are not unique to a single sovereign.

- Third, the recent events provide a teachable moment that should encourage us to redouble our efforts on improving transparency and privacy protections for consumers in the commercial sphere. We have a renewed opportunity to be proactive rather than reactive, and to move the separate but equally important conversation about enhancing consumer privacy forward, not backward. It is important to acknowledge that commercial privacy and national security issues are two distinctly separate issues. Indeed, the EU has recognized this distinction, as the data protection laws do not apply to national security issues.[5] And this is the right approach, helping to ensure the solutions we develop will be tailored to each set of problems we seek to address.

At the Federal Trade Commission, we address commercial privacy. We do not have criminal jurisdiction, or jurisdiction over national security issues. Of course, there are other U.S. officials who are charged with addressing those issues, and they are eager to do so.

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 policies or otherwise misrepresent their information management practices. And, just as importantly, we also address unfair collection and use of personal information that inflicts harm on consumers that they cannot reasonably avoid, and that does not offer offsetting benefits to consumers or competition.[6]

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[7] and health information,[8] children,[9] and information used for credit, insurance, employment and housing decisions.[10]

---

[4] *Full Transcript: President Obama's Press Conference with Swedish Prime Minister Fredrik Reinfeldt in Stockholm*, WASH. POST, Sept. 4, 2013, *available at* http://www.washingtonpost.com/politics/full-transcript-president-obamas-press-conference-with-swedish-prime-minister-fredrik-reinfeldt-in-stockholm/2013/09/04/35e3e08e-1569-11e3-804b-d3a1a3a18f2c_story.html.

[5] *See* EU Data Protection Directive, *supra* note 3, at 42.

[6] 15 U.S.C. § 45(n).

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

[8] Health Insurance Portability and Accountability Act of 1996 (HIPAA), 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 (HITECH) Act of 2009, 42 U.S.C. §§ 201 note, 300jj *et seq*., 17901.

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,[11] Facebook,[12] and MySpace[13] – 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.

We have also brought myriad cases against companies that are not household names, but whose practices crossed the line. We've sued companies spamming consumers and installing spyware on their computers.[14] We've challenged companies that failed to properly secure consumer information.[15] We have sued ad networks,[16] analytics companies,[17] data brokers,[18] and software developers.[19] We have vigorously

---

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

[10] 15 U.S.C. §§ 1681-1681t.

[11] 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).

[12] 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).

[13] 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).

[14] *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).

[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 (Mar. 13, 2013), *available at* http://www.ftc.gov/os/caselist/1123182/130315epicmarketplacedo.pdf (decision and order).

[17] *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).

[18] *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).

[19] *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).

enforced the Children's Online Privacy Protection Act.[20] And with the world moving to mobile, we have targeted app developers as well as handheld device manufacturers engaged in inappropriate data collection and use practices.[21]

As part of our ongoing effort to address privacy issues in the changing technological landscape, just two weeks ago we brought our first action involving the Internet of Things.[22] In that case, the company failed to secure the software for its Internet-accessible video cameras, which put hundreds of private lives on public display.[23]

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.[24]

In addition to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve privacy protection in light of rapid technological change. We have held hearings and issued reports on cutting edge issues, including facial recognition technology[25], kids apps,[26] mobile privacy disclosures,[27] and mobile

---

[20] *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.

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

[22] 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.

[23] *See id.*

[24] 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").

[25] *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.

[26] *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.

payments.[28] 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.[29] We called on companies to operationalize the report's recommendations by developing better just-in-time notices and robust choice mechanisms, particularly for health and other sensitive information.[30]

The FTC is also 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.[31] In last year's privacy report, the FTC called on Congress to enact data broker legislation that would increase the transparency of the practices of data brokers.[32]

But we don't have to wait for legislation. I recently launched "Reclaim Your Name", a comprehensive initiative to give consumers the means they need to reassert control over their personal data.[33] I call on industry to develop a user-friendly, one-stop online shop to provide consumers with some tools to find out about data broker practices and to exercise reasonable choices about them.[34] Acxiom, the largest data broker in the U.S., has taken the first step toward greater transparency by launching aboutthedata.com, a web portal that allows consumers to access, correct, and suppress the data that the company maintains about them.[35] And while there is certainly room for Acxiom to

---

[27] *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.

[28] *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.

[29] *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"].

[30] *See id.*

[31] *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.

[32] *See* FTC Privacy Report, *supra* note 29, at 14.

[33] *See* 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.

[34] *See id. See also* 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.

[35] *See generally* Natasha Singer, Acxiom Lets Consumers See Data It Collects, N.Y. TIMES, Sept. 4, 2013, *available at* http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html?pagewanted=all.

improve its portal, I encourage other industry players to join Acxiom and step up to the plate to provide consumers with greater transparency about their data collection and use practices.

The FTC has also supported baseline privacy legislation.[36] The Obama Administration has been actively working on privacy legislation that would implement its Consumer Privacy Bill of Rights.[37]

Through the FTC Act and other US privacy and data protection laws, the FTC's privacy report and other policy initiatives, and the Obama Administration's Consumer Privacy Bill of Rights, the US aims to achieve many of the same objectives that are outlined in the draft EU data protection regulation. For instance, on both sides of the Atlantic, we are striving to protect children's privacy; spur companies to implement privacy by design, increase transparency, and adopt accountability measures; and require companies to provide notice about data breaches. As the technological challenges facing the EU and the US have grown, so has our common ground in protecting 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 desire to solve them are the same.

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.[38]

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, Facebook, and MySpace — 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.

In recent months, the NSA revelations have led some to ask whether the Safe Harbor can adequately protect EU citizens' data in the commercial context. My unequivocal answer to this question is "yes." As I said before, the issue of the proper scope of government surveillance is a conversation that should happen – and will happen – on both sides of the Atlantic. But it is a conversation that should proceed outside out of the

---

[36] *See* FTC Privacy Report, *supra* note 29, at 13.

[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.

[38] *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.

commercial privacy context. In the commercial space, the Safe Harbor Framework facilitates the FTC's ability to protect the privacy of EU consumers. 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.

I understand that Safe Harbor, in part because of its notoriety, is an easy target, but I ask you to consider whether it is the right target. Neither the Safe Harbor nor the EU data protection directive was designed to address national security issues.[39] Data transferred to "adequate" countries, or through binding corporate rules, approved contractual clauses, or the Safe Harbor, are all subject to the same national security exceptions. The most salient difference is that, for transfers made pursuant to Safe Harbor, the FTC is the cop on the beat for commercial privacy issues. The same is not true of the other transfer mechanisms. So, from my consumer protection enforcer's perspective, the Safe Harbor provides more, not less, privacy protection. And, for that reason, I support its continuation.

While some things have changed since my last trip to Brussels in April, many things have remained the same. Our enforcement is still robust, including our enforcement of the Safe Harbor. Our policy development continues. And I believe that the common ground between the U.S. and the EU is still quite fertile.

Last April when I was here I quoted one of my heroes, John F. Kennedy, and I believe it is worth quoting him again. Fifty years ago, in 1963, he said: "[L]et us not be blind to our differences—but let us also direct attention to our common interests and to the means by which those differences can be resolved. And if we cannot end now our differences, at least we can help make the world safe for diversity."[40]

These words continue to ring true – especially now, when we each have so much work to do to foster better consumer privacy protections for all of our citizens.

---

[39] *See id. See also* EU Data Protection Directive, *supra* note 3.

[40] *See* John F. Kennedy, Commencement Address at American University: Towards a Strategy of Peace (June 10, 1963), *available at* http://www.jfklibrary.org/Asset-Viewer/BWC7I4C9QUmLG9J6I8oy8w.aspx.