Remarks to the Mentor Group
Forum for EU-US Legal-Economic Affairs
Brussels, April 16, 2013

Good afternoon, and thanks to Tom Kosmo and the Mentor Group for inviting me to address you today. I am delighted to be here in the company of Dr. Martin Selmayr, Advocate General Juliane Kokutt, and Judge Marc van der Woude, all of whom are thought leaders in the European Union privacy sphere.

Tom has asked me to speak to you today about the privacy regime in the United States. In so doing, I hope also to convey to you what I believe to be a central reality that lies at the interface between EU and U.S. privacy law: while many commenters dwell on the significant differences between the EU and US privacy regimes I believe it is important to recognize that we also have much in common.[1] On both sides of the Atlantic, we are grappling with how best to revise our privacy laws in light of the revolution 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 Federal Trade Commission 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",[2] Louis Brandeis was a "trustbuster" of the Progressive Era, leading a crusade against the large steel trusts and other monopolies that were engulfing the US 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."[3] After Woodrow Wilson won that election with Brandeis's help, Wilson asked Brandeis to recommend specifically how to solve the problem of the trusts. Brandeis conceived of the Federal Trade Commission, which, at Brandeis' urging, Congress empowered 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." [4]

Today, the FTC is the only federal agency in the United States with both consumer protection and competition jurisdiction. Our dual mission is to prevent business practices that are anticompetitive, and to stop deceptive or unfair practices that harm consumers. We seek to

---

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

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

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

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

accomplish our twin goals without unduly burdening legitimate business activity, and we do so through a variety tools given to us by Congress.

The Federal Trade Commission's focus on consumer privacy stems directly from our authority to prohibit unfair or deceptive acts or practices in commerce. We take action against companies that fail to comply with their own privacy policies or otherwise misrepresent their information management practices. But just as importantly, we also address unfair 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.[5]

As specific privacy and data use issues have arisen over the past 40 years, Congress has supplemented the Federal Trade Commission's broad remedial authority by charging us and other agencies with enforcing specific data protection and privacy laws, including laws designed to protect financial[6] and health information ,[7] children,[8] information used for credit, insurance, employment and housing decisions,[9] and commitments made by companies that handle data about EU citizens.[10] We even enforce the Do Not Call law[11] – allowing US consumers to avoid telemarketing phone calls – creating what Dave Barry, one of our leading humorists, has called the most popular US government program since the Elvis stamp.

At the Federal Trade Commission, privacy protection is "mission critical." 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 have resulted in orders that, for the next 20 years will govern data collection and use activities of Google,[12] Facebook,[13] MySpace[14] and Twitter.[15] We have also brought myriad cases

---

[5] 15 U.S.C. § 45(n).

[6] 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), 15 U.S.C. §§ 1681-1681t.

[7] 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. 300jj et seq. §§17901 et seq.

[8] Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501-6505.

[9] FRCA, 15 U.S.C. §§ 1681-1681t.

[10] EU Directive 95/46/EC.

[11] Do-Not-Call Implementation Act of 2003, 15 U.S.C. § 61010 et. seq.

[12] Fed. Trade Comm'n, Statement of the FTC Regarding Google's Search Practices, *In the Matter of Google Inc.* (Jan. 3, 2013) *available at* http://www.ftc.gov/os/2013/01/130103googlesearchstmtofcomm.pdf.

[13] In the Matter of Facebook, Inc., FTC File No. 0923184 (2011) *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf (agreement containing consent order).

[14] In the Matter of Myspace, LLC, FTC File no. 1023058 (2012) *available at* http://ftc.gov/os/caselist/1023058/120508myspaceorder.pdf (agreement containing consent order).

against companies that are not household names, but whose practices were troubling. We've sued companies spamming consumers and installing spyware on their computers.[16] We've challenged companies that failed to properly secure personal consumer information. We have sued ad networks,[17] analytics companies,[18] data brokers,[19] and software developers.[20] We have vigorously enforced the Children's Online Privacy Protection Act.[21] 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.[22]

Together, these enforcement efforts have established what some scholars call "the common law of privacy" in the United States.[23] The 100-year-old legislative history of the Federal Trade Commission Act shows that – in contrast to what might transpire in a civil law jurisdiction – Congress intentionally left to my agency the job of defining – through our enforcement actions – the conduct prohibited under the law. As Congress said at the time the FTC Act was being debated, there simply are "too many unfair practices to define."[24] So it is

---

[15] In the Matter of Twitter, Inc., FTC Docket No. C-4316 (2011) *available at* http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf (decision and order).

[16] *See, e.g.*, Press Release, FTC Halts Computer Spying (Sept. 25, 2012), *available at* http://www.ftc.gov/opa/2012/09/designware.shtm.

[17] *See, e.g.*, In the Matter of Epic Marketplace, Inc. et al., FTC File No. 1123182 (Dec. 5, 2012), *available at* http://ftc.gov/os/caselist/1123182/121205epicorder.pdf (agreement containing consent order).

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

[19] United States v. Spokeo, Inc., FTC. File No. 1023163 (Jun. 12, 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. 1123195 (Jan. 10, 2013), *available at* http://www.ftc.gov/os/caselist/1123195/130110filquarianagree.pdf (agreement containing consent order).

[20] *See, e.g.*, In the Matter of DesignerWare LLC, FTC File No. 1123151 (Sept. 25, 2012), *available at* http://www.ftc.gov/os/caselist/1123151/designerware/120925designerwareagree.pdf (agreement containing consent order).

[21] *See, e.g.*, Press Release, Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books (Feb. 1, 2013), http://www.ftc.gov/opa/2013/02/path.shtm.

[22] *See, e.g.*, Press Release, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), *available at* http://ftc.gov/opa/2012/12/databrokers.shtm.

[23] 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, as well as 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* (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").

[24] S. REP. NO. 597, 63d Cong., 2d Sess., at 13 (1914).

through our enforcement actions that the FTC has taken up Congress's mandate to flesh out, in an incremental but powerful way, privacy practices that are deceptive or unfair.

In addition to our privacy enforcement work, the FTC is actively engaged in ongoing policy development to improve our approach to privacy protection in light of rapid technological change. And we use the tools Brandeis intended for this purpose: we hold hearings, public workshops, and conferences to discuss cutting edge issues with stakeholders; and we issue reports that summarize our findings and make recommendations both to businesses and to Congress.

Our privacy policy work is both extensive and ongoing. In March last year, we issued a landmark privacy report in which we developed a new framework for thinking about privacy in the US, including best practices for firms to follow based on three core principles of privacy by design, simplified choice, and greater transparency regarding the collection and use of personal data. We called on firms to operationalize the report's recommendations by developing better privacy notices and robust choice mechanisms, particularly for health and other sensitive information.[25]

In addition to our big privacy rethink, the FTC has recently focused its policy efforts in more targeted ways. In the past year, we have addressed privacy issues raised by mobile disclosures[26] as well as facial recognition technology.[27]

The cumulative learning from this careful and incremental policy work led our agency last year to support President Obama's call on Congress to consider enacting general privacy legislation to provide every U.S. citizen with the baseline privacy protections articulated in the President's Consumer Privacy Bill of Rights. We also supported the President's call to "companies to begin immediately working with privacy advocates, consumer protection enforcement agencies, and others to implement these principles in enforceable codes of conduct."[28]

The baseline principles enumerated in the Consumer Privacy Bill of Rights will sound familiar to a Brussels-based audience.

---

[25] *See* Press Release, FTC Issues Final Commission Report on Protecting Consumer Privacy (Mar. 26, 2012), *available at* http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

[26] *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.

[27] *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.

[28] *See* 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.; *and* Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, An FTC Report (Mar. 26, 2012) *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf. at 27 and C-8.

Through these baseline principles, we are calling on industry to:

- Provide more transparency so that consumers can better understand companies' collection, use and retention practices with respect to consumer information.

- Give consumers more effective tools to assert greater control over their information and how it is used.

- Provide appropriate access to the data companies hold about them.

- Take appropriate steps to ensure that the data they hold about consumers is accurate.

- Take reasonable steps to secure the data about consumers that they have.

- And create a climate of accountability.[29]

A comparison of the US regime to protect consumer privacy with the draft EU privacy regulation highlights both our convergence on many of the goals around modernizing our privacy regimes, and our divergence on some of the mechanisms we choose to get there. The EU draft regulation reflects our common ground on many key issues — promoting privacy by design, protecting children's privacy, enhancing data security, and providing consumers with appropriate access, correction and deletion rights.

In some instances, we differ on how to achieve these common goals. We both believe that consumer consent is important, but we have different approaches as to when and how that consent should be obtained. We both recognize the importance of encouraging notification of data breaches, but our views may differ with respect to the timing and scope of those notifications. In short, the particular solutions we develop may differ, but the challenges we face and our desire to solve them are the same.

One important area where the difference in implementation between the U.S. and EU is most significant is in the area of cross-border data transfers. In the U.S. and elsewhere, we have relied on holding those who transfer data accountable for its safe- keeping, and self-regulatory codes of conduct to protect the privacy of personal information that flows across borders. The two most notable mechanisms are the U.S-EU Safe Harbor Framework, which applies to data transfers from the EU to the U.S., and the APEC Cross-Border Privacy Rules System, which enables entities in APEC member economies to share data while adhering to stringent privacy standards. Both systems have an important and effective government enforcement backstop.

The EU's current law applies a more restrictive approach to cross-border transfers, often focusing on whether the foreign country provides an "adequate" level of privacy protection rather than the data protection practices of the recipient. Given the complexity of international data flows and different legal regimes around the globe, I think that providing more flexibility

[29] *Id*. at 9-23.

for cross-border data transfers could enhance privacy protection, spur innovation and trade, and help us achieve interoperability between our two systems.

Winston Churchill has 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. I know there are many who believe that the gap between the EU and US privacy regimes is growing. From where I sit, however, I see an opportunity for achieving real interoperability between our systems. Granted, in the US we largely employ a different mechanism – a flexible statutory mandate with broad enforcement authority. Yet we use our robust tools to achieve many of the same goals: protecting consumers' privacy in the growing data-driven marketplace – online and off, mobile and stationary. The FTC's common law of privacy is well respected by our international counterparts. Perhaps this is why many of my international colleagues confess – also under Chatham House rules – that for them, an ideal privacy regulatory regime would be one with "U.S. style enforcement, and EU style regulation."

Of course, in making this observation, I am not arguing that one legal system is somehow inherently better equipped to deal with privacy issues over the other. To the contrary, there is always room for improvement. This is why I support comprehensive privacy legislation in the U.S. What I am saying, however, is that although the U.S. may for historic reasons approach privacy through our different legal tradition – one that uses a framework approach, backed up by strong enforcement – I believe this approach achieves many of the same goals as those embraced by EU data protection authorities.

So let the Churchillian optimists in all of us recognize that, as we strive for interoperability, we need not achieve uniformity.

As another one of my heroes, John F. Kennedy, said at a 1963 commencement address: "[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."[30]

We will not erase the differences in our privacy regimes. And, as Kennedy noted 50 years ago, we need not erase them, because we have plenty of common ground for mutual recognition of our different, but equally effective, privacy frameworks.

It is only proper that I return to Louis Brandeis to wrap up my talk. In 1890, Brandeis co-authored an article for the Harvard Law Review entitled "The Right to Privacy",[31] which is still considered a seminal piece in the continuing discussion about privacy and the role it plays in our lives. In "The Right to Privacy", Brandeis grappled with his concerns about modernizing the law to address "shapshot photography" – a technology that was new in his day, and one which he feared allowed the press to "overstep[] in every direction the obvious bounds of propriety and of

[30] John F. Kennedy, Commencement Address at American University (June 10, 1963).

[31] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. R. 193 (1890).

decency."[32] In advocating for the creation of a tort for breach of privacy to solve his concerns, Brandeis argued that an individual citizen's greatest tool in guarding his privacy was the common law, since "[t]he common law has always recognized a man's house as his castle, impregnable, often, even to his own officers engaged in the execution of its command."[33]

As we grapple with the new technologies of our day – on the internet, in mobile, and in the cloud – and our increasingly globalized and interdependent world, I would submit that it is worthwhile to reflect on the ultimate trust that Brandeis placed in the common law tradition to solve some of the thorniest privacy concerns. We should recognize the value not only of legislative solutions, but also the strength of a broad and flexible framework, coupled with strong enforcement, to ensure that consumer privacy is appropriately protected in our modern technological era.

[32] *Id*. at 196.

[33] *Id*. at 220.