Remarks of Commissioner Maureen K. Ohlhausen[1]
Forum Global
2014 Cloud Computing Conference
Washington, DC
June 11, 2014

Introduction

Thank you to Forum Global for inviting me here today, and thank you to all of you for attending. I am honored to be here with Ambassador de Almeida and am looking forward to his comments and our discussion afterwards.

As a Commissioner at the Federal Trade Commission – the U.S.'s primary privacy and data security agency – my comments today will focus on protecting consumers as commercial computation goes international by moving into the cloud. I will also emphasize the importance of international cooperation in our increasingly interconnected world. Cooperation and interoperability are critical, as the global economy depends on open international trade in information and cross-border information flows. I will highlight two important examples of interoperability efforts – the U.S. / EU Safe Harbor, and the Asia-Pacific Economic Cooperation privacy framework – describing the FTC's role thus far and detailing how we are working to improve these frameworks.

Importance of International Trade in Information

But first, why does cooperation matter? It matters because the Internet has transformed how data moves around us, making international communications a routine matter. Cross-border data flows are ubiquitous and happen transparently to the sender and receiver. Data may be routed over borders even if the end points of the communication are in the same country. Given the distributed and location-agnostic nature of the Internet, it is difficult to determine where data

[1] The views expressed in this speech are solely those of Commissioner Ohlhausen and are not intended to reflect the views of the Commission or any other Commissioner.

flows start and end. Dr. Michael Mandel has preliminarily estimated however that cross-border data flows comprise 16-25% of all U.S. data traffic, while approximately 13-16% of data traffic in Europe crosses into other regions.[2] What is crystal clear is that communication between the U.S. and Europe has been growing rapidly, with telecom providers adding transatlantic cable capacity at an average annual rate of 19% between 2008 and 2012.[3]

These cross-border data flows have been a key driver of economic growth. A McKinsey Global Institute study estimates that, in the world's top ten economies, the Internet contributed more than 10% to GDP growth in the last five years alone.[4] And trade between the U.S. and the EU has clearly benefited from our increased interconnectedness. A recent U.S. Chamber of Commerce report calls "the transatlantic exchange between the EU and the United States … the most important economic link in the world" with "[t]he transatlantic marketplace consisting of the EU and the United States together accounts for half of world GDP and 3 trillion USD (2.4 trillion euro) in bilateral investments."[5] According to a March 2013 comScore report, eight of the top ten websites visited by UK consumers are based in the U.S., and the two most popular retail sites for European consumers are Amazon and Apple.[6] Dr. Mandel calls cross-border flows "the

---

[2] Dr. Michael Mandel, Progressive Policy Institute Working Paper: *Data, Trade, and Growth*, 5 (Aug. 15, 2013) ("*Mandel PPI*"), *available at* http://southmountaineconomics.files.wordpress.com/2013/09/datatradegrowth-8-15-13.pdf.

[3] *Id.* at 3-4.

[4] McKinsey Global Institute, *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*, 2 (May 2011), *available at* http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Internet%20matters%20-%20Nets%20sweeping%20impact/MGI_internet_matters_exec_summary.ashx.

[5] European Centre for International Political Economy, *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*, 6 (Mar. 2013) *available at* https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

[6] *See* comScore, Inc., *Europe Digital Future in Focus 2013* (Mar. 2013), *available at* http://www.comscore.com/Insights/Blog/2013_Digital_Future_in_Focus_Series. (cited in Protecting Consumers and Competition in a New Era of Transatlantic Trade, Keynote Address by FTC Chairwoman Edith Ramirez, 2 (Oct. 29, 2013)).

purest form of a broadband bonus, since countries that exchange data win without anyone losing."[7]

Cloud computing is a special case of cross-border data flows and is about more than just sending content. Cloud computing enables parties in different geographical locations to contribute in real time to the same work product, resulting in what Paul Schwartz has called a "distributed computing" environment that gives firms "greater flexibility that ever before in deciding on shape of work" and "play[s] an important role today in allowing novel business approaches."[8] Cloud computing is the core technology that is enabling a wide range of location-agnostic business models and consumer services.

Cloud computing is big, and it is still growing fast. According to Cisco estimates, global cloud Internet traffic is predicted to increase nearly 4.5-fold between 2012 and 2017. Overall, cloud IP traffic is forecast to grow at a compound annual growth rate of 35% from 2012 to 2017. And by 2017, nearly two-thirds of all data server workloads will be processed in cloud data centers.[9]

FTC Authority. Cross-border information flows are clearly beneficial, but they also raise issues for consumer protection agencies such as the FTC. As a consumer protection agency, one key issue raised by cross-border information flows is jurisdiction – how can our policies reach actions that take place outside of the physical borders of the U.S.? In some ways, this isn't a new problem. The FTC has long dealt with international companies in both our consumer protection and antitrust oversight roles. And we have successfully applied our data security and privacy laws to companies whose violations have international components. For

---

[7] *Mandel PPI* at 27.
[8] Paul M. Schwartz, A Report from the Privacy Projects.org, *Managing Global Data Privacy in the Cloud,* 12 *available at* http://www.law.berkeley.edu/files/Schwartz.pdf.
[9] Cisco Global Cloud Index: Forecast and Methodology, 2012-2017, 1 (2013) *available at* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html.

example, just this past January, the FTC settled a case with GMR Transcriptions Services.[10] GMR was a medical transcription service operating in the U.S. that used a subcontractor in India to transcribe medical records. GMR claimed that it kept the medical data securely. However, GMR's subcontractor used unsecured FTP servers to transmit the medical records, resulting in the indexing of these files by a major search engine. The FTC alleged that GMR's claims to store records securely and to oversee its subcontractors, combined with a lack of reasonable measures to do so, was both deceptive and unfair to consumers. In short, this case demonstrated that outsourcing data doesn't outsource the responsibility for protecting that data.

Additionally, as the 2006 U.S. SAFE Web Act explicitly confirmed, the FTC has jurisdiction to redress harm in the United States caused by foreign wrongdoers. The Act also confirmed the FTC's jurisdiction to redress harm abroad caused by U.S. wrongdoers.

Importance of Cooperation and Interoperability

These domestic tools are useful, and the FTC has actively applied them when necessary. However, because privacy protections in various jurisdictions around the world differ, unilateral action alone is insufficient to protect consumers while supporting the growing and beneficial international trade based on information. In particular, the location-agnostic nature of cloud computing means that today a consumer can access and use services that extend far beyond the geographic, legal, and social boundaries of the consumer's home country. A single service might have physical components in several jurisdictions. Thus countries must work together to achieve their consumer protection policy goals. As the FTC noted in its 2012 Privacy Report, "[M]eaningful protection for [cross-border] data requires convergence on core principles, an

[10] Press Release, Fed. Trade Comm'n, *Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information* (Jan. 31, 2014) available at http://www ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

ability of legal regimes to work together, and enhanced cross-border enforcement cooperation. Such interoperability is better for consumers, whose data will be subject to more consistent protection wherever it travels, and more efficient for businesses by reducing the burdens of compliance with differing, and sometimes conflicting, rules."[11] Finding ways to work together to promote international trade in information and data services while protecting the privacy of consumers – a concept that differs by jurisdiction – is critical to unlocking the full economic benefits of cloud computing and other cross-border data flows.

Of course, there are several ongoing efforts to increase international privacy interoperability. In the remainder of my remarks, I'd like to highlight two important efforts: the U.S. EU Safe Harbor framework, and the APEC Privacy Framework.

U.S. / EU Safe Harbor. As you know, the U.S. / EU Safe Harbor framework provides a way for businesses to transfer personal data from the EU to the U.S. in a manner consistent with EU law. Because cloud computing is location-agnostic, the Safe Harbor is an important part of protecting EU consumer privacy while also enabling EU consumers to access the benefits of cloud computing services outside of the EU.

Since the establishment of the Safe Harbor in 2000, the FTC has been committed to the effective operation of the program. The companies that participate in the Safe Harbor self-certify that they adhere to principles of notice and choice, access, security, data integrity, and enforcement. More than 3,000 companies currently participate in the program, including all the major U.S. cloud service providers.

[11] FTC Report, Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, 10 (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf,

There are three important Safe Harbor-related issues the FTC is working to improve: enforcement cooperation, awareness of the program, and program administration.

First, **enforcement cooperation**. The FTC is an active enforcer of the Safe Harbor framework, but cross-border cooperation is critical to the effectiveness of the framework. The FTC is strongly committed to vigilant enforcement of Safe Harbor certifications. As the Safe Harbor program has grown over the past decade, so has the FTC's enforcement activity. To date, we have brought Safe Harbor enforcement actions against 24 companies -- including Google, Facebook and MySpace -- resulting in orders protecting consumers worldwide, millions of them in Europe. Most recently we brought 14 cases against companies that claimed to be participating in Safe Harbor who had allowed their registrations to lapse. These cases show we are committed to the integrity of the Safe Harbor Framework and send the signal to companies that they cannot falsely claim participation in the program. Such enforcement is a key part of preserving the cross-border trade in information that is so important to the global economy, and we will continue to do our duty to enforce the program.

However, we cannot do it alone. We look forward to working with our European colleagues on future Safe Harbor enforcement. Given the international scope of cloud computing, cross-border cooperation on Safe Harbor and other privacy cases is essential to combat global challenges. In particular, we believe that authorities in EU Member States have a critical role to play in monitoring and reporting possible Safe Harbor violations. We have committed to review, on a priority basis, referrals received from EU Member States regarding noncompliance with the Safe Harbor framework. We have received only a few Safe Harbor referrals from Member States since the establishment of the framework, but we stand ready to act

on referrals as they come in. Importantly, we also routinely explore whether a Safe Harbor violation exists as a standard part of our privacy and data security investigations.

The FTC is also focused on raising awareness of the Safe Harbor Framework among U.S. businesses and E.U. consumers. We launched a section of our business center website devoted to the Safe Harbor framework. These materials explain the FTC's role enforcing Safe Harbor.[12] The site also provides legal resources, reports and blog posts about the Safe Harbor, and links to the Department of Commerce's export.gov website which explains in detail the steps to participate.[13] The FTC's site is updated as new cases and reports related to the Safe Harbor become public.

And we are looking for ways to partner with the European Commission and the member states to raise awareness among EU consumers about the Safe Harbor. We want EU consumers to understand how U.S. businesses comply with the Safe Harbor framework, what enforcement actions the FTC has taken to ensure compliance, and perhaps most importantly, how EU consumers can access redress mechanisms and assistance from European authorities. I welcome your ideas on how we can better raise awareness for EU consumers.

Our third area of focus is managing and improving the administration of the Safe Harbor framework. The FTC works closes with Department of Commerce and the Director-General for Justice to monitor and address Safe Harbor implementation issues. We have supported Commerce's ongoing efforts to improve the administration of the program and lower the costs of the dispute resolution system. In particular, we have reviewed the European Commission's recommendations for improving Safe Harbor administration and are working with

[12] Fed. Trade Comm'n., Bureau of Consumer Protection Bussiness Center, *U.S. – EU Safe Harbor Framework*, *available at* http://www.business ftc.gov/us-eu-safe-harbor-framework (last visited June 10, 2014).
[13]Export.gov, U.S. Companies Export, *Welcome to the U.S. – EU Safe Harbor*, http://export.gov/safeharbor/eu/eg_main_018365.asp (last visited June 10, 2014).

EC officials to consider appropriate improvements. In fact, FTC staff is meeting with EC representatives this week to further discuss these issues.

The Safe Harbor is a major component of the FTC's ongoing efforts to strengthen the interoperability of privacy regimes in different countries. But it is not the only such effort. Indeed, the Commission is working around the world to build frameworks and agreements that enable data to move between countries with different privacy and consumer protection regimes.

APEC. Our work on the Asian-Pacific Economic Cooperation framework is another good example of our interoperability efforts. As you know, the APEC framework facilitates interoperability of different privacy regimes. FTC Chairwoman Edith Ramirez recently described APEC as "allow[ing] information to flow freely among the 21 APEC economies …. yet still maintain[ing] strong privacy protections for consumer data."[14] The FTC has participated in APEC from the beginning, helping to develop the privacy framework, the Cross-Border Privacy Rules, and the Cross-order Privacy Enforcement Arrangement. The U.S. was the first APEC economy accepted to join the Cross Border Privacy Rules system in 2012, and the FTC became the first approved privacy enforcement authority in the Cross-Border Privacy Rules system. And the APEC Framework continues to gather momentum. In 2011, China and other APEC members committed to promote the interoperability of data privacy regimes in the region, and, to that end, it is our understanding that China is actively considering next steps toward determining whether to participate in the CBPR system. Mexico was accepted into the APEC CBPR system last year. And in May of this year, Japan became the third APEC economy to be accepted.

[14] Protecting Consumers and Competition in a New Era of Transatlantic Trade, Keynote Address by FTC Chairwoman Edith Ramirez, 2 (Oct. 29, 2013) *available at* *http://www.ftc.gov/public-statements/2013/10/protecting-consumers-competition-new-era-transatlantic-trade* .

I want to highlight one other recent effort that will promote interoperability. Recently the FTC announced the results of a project mapping the APEC Cross Border Privacy Rules to the EU Binding Corporate Rules.[15] The resulting document was jointly designed by APEC officials and the EU's Article 29 Data Protection Working Party to be a practical reference tool for companies that seek "double certification" under these APEC and EU systems.[16] The document shows the substantial overlap between the EU and APEC frameworks, while noting the areas in which the regimes differ. Understanding the contours of these two systems should help companies design their systems and practices to comply with both regimes. Practical efforts like these will help build the interoperability necessary to support our increasingly connected economies.

Conclusion. The benefits of cross-border data flows generally, and cloud computing specifically, are substantial and growing. These advances are bringing countries, businesses, and citizens together in a way the world has never before seen. Fittingly, it is also bringing international policy makers together, as we seek to protect the interests of the citizens we serve. To best serve those citizens and consumers, we must continue to cooperate by finding ways to increase the interoperability of our privacy and consumer protection regimes. I trust that today's conference will explore many of these issues. The FTC stands ready to continue this work, and I look forward to discussing these issues further with you today.

---

[15] Press Release, Fed. Trade Comm'n., *FTC Signs Memorandum of Understanding with UK Privacy Enforcement Agency* (Mar. 6, 2014) *available at* http://www.ftc.gov/news-events/press-releases/2014/03/ftc-signs-memorandum-understanding-uk-privacy-enforcement-agency.

[16] Article 29 Data Protection Working Party, Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC/CBPR Accountability Agents, 1 (Feb. 27, 2014).