United State International Trade Commission

Digital Trade in the U.S. and Global Economies

March 7, 2013

Testimony of

Martin Abrams

President the Centre for Information Policy Leadership
At Hunton Williams LLP

Mr. Chairman, honorable commission members, distinguished participants, my name is Martin Abrams and thank you for the honor of testifying.

I am President of the Centre for Information Policy Leadership at Hunton & Williams LLP. The Centre is a global information policy center and think tank that does work in the area of privacy and information security. The Centre is funded by forty companies, mostly American headquartered. However our programs involve governments, privacy protection agencies, academics and privacy advocates. While based in the United States, we think of ourselves as having a global perspective. My views today are mine, and do not necessarily reflect those of our funders, Hunton & Williams LLP, or the firm's clients.

My topic is the impact of privacy and data protection law on data movement that is the foundation for trade. During its twelve year history the Centre has facilitated global debates, discussion and consensus on thoughtful data governance that protects individuals while facilitating global data flows. The Global Accountability Project, begun by the Centre in 2008 was originally focused on data transfer governance based on organizational accountability. The

Centre has led APEC discussions on cross border privacy rules for processors. My colleague at the Centre, Paula Bruening is part of the working group advising the OECD on changes to the OECD Privacy Guidelines. Lastly, the Centre has led workshops in Asia, Australia, Europe, and North, Central and South America, in part to assure privacy law is not an impediment to the free flow of data that facilitates commerce.

Prior to joining the Centre I was involved in discussions between the United States department of Commerce and the European Commission on movement of data from the European Community to the U.S. Those talks eventually resulted in the safe harbor arrangement that has facilitated the movement of data from Europe to the United States.

Key Topics to be Covered

Data protection law creates three impediments to digital trade and the free movement of data:

1. Data protection law creates barriers to data transfer;
2. Cultural differences between observation in the United States and states with data protection laws;
3. Legal obstacles to big data and analytics.

Introduction: Data and Trade are One in the Same

There is not an industry today that is not both data driven and dependent on global data flows. The Centre's funders include financial services, pharmaceuticals, entertainment, consumer goods, retail, and education, and all are data driven. Furthermore, data must move agilely everywhere from China, to Zambia, to Finland, to the United States. Five years ago we could have segmented our member companies into those that collected and kept data within borders, and those that needed global privacy solutions. Now every company needs global solutions. For example, a large bank with retail customers only in the United States still needs to move data to its risk center located in Singapore. That bank is confronted with the question of whether the data collected in Chicago and processed in Singapore will be able to return to the United States under Singapore law? That bank, even though it's retail customers are in the U.S. now needs a global policy. Globalization of data flows is even important for the smallest of organizations. The one-man taxi service I use in Dallas, Texas now has a smart phone app that allows me to reserve his taxi while sitting in a hotel in Warsaw. When I used that service in Poland a data transfer was initiated across borders.

Data Protection Law and Barriers to Transfer

When data protection and privacy laws began to emerge in the 1970's there was a concern that the laws would block the flow of data from a country with tight laws to another where the laws

were either non-existent or different. The OECD was concerned that impediments to the flow of data would negatively impact commerce, and formed a task force to develop privacy guidelines. In 1980 the OECD approved the OECD Privacy Guidelines to set a common standard for privacy that facilitates the free movement of data. The OECD guidelines have become the basis for most of the overarching national privacy laws that have been enacted.

The United States adopted the OECD Guidelines but never enacted an overarching privacy law. Instead the United States has developed a privacy framework that is a mosaic of sector specific laws, state laws, court decisions, and broad use of the Federal Trade Commission's Section 5 authority to prohibit unfair and deceptive trade practices. This mosaic has done a comparatively effective job of preventing privacy harms. However the data protection laws that exist in many of our trading partners go beyond the targeted prevention of privacy harms. Instead they create mechanism for assuring data is processed in a controlled manner. Many of the laws are dependent on individuals providing consent based on a specific set of described purposes. Others require a legal basis for processing with consent often the preferred legal basis. In either case, every time that data is touched it is a processing that requires a legal permission. In the United State it is the use of data, not the processing that is covered by our privacy mosaic.

In practical terms, while the prevention of harm is directly targeted in the United States and indirectly in data protection regimes, one tends to have the same issues and outcomes most of the time. The U.S. Federal Trade Commission and the community of data protection commissioners spend a great deal of time enforcing against organizations with less than adequate security or use information in a deceptive fashion. However, the operational differences are significant, and those differences cause friction.

The 1995 European Data Protection Directive[i1] was enacted by the European Union to assure the free movement among the now 27 states. The Directive requires all 27 states to have data protection laws that are very similar. The Directive, however, prohibits data from being transferred from any of those 27 states to a jurisdiction that does not have adequate data protection laws. The determination of adequacy is based on how well a nation's laws to protect data (a) match the controls contained in the Directive and (b) establish an independent data protection agency. Only a handful of countries have been found adequate, and the United States is not one of them.[2] However, the Safe Harbor framework negotiated between the United States Department of Commerce and the European Commission is deemed adequate and is used by many companies to move data to the United States from Europe.

[1] EU Data Protection Directive 95/46

[2] A number of countries in Latin America and Asia have followed Europe and adopted an adequacy requirement for data transfers.

There are other legal means for transferring data to the United States from Europe. They include model contracts approved by a data protection authority and binding corporate rules also approved by a data protection authority.

Between Safe Harbor, model contracts and binding corporate rules most companies that need to transfer data to the United States have been able to do so.

The Emergence of Accountability Mechanisms and Interoperability

A means of moving beyond the limitations of location specific governance are concepts of accountability which, in turn create a mechanism for interoperability between data protection and privacy regimes.

Data transfers once meant copying a file to a magnetic medium, placing the medium on an airplane and flying it to a destination for processing. Twenty years ago governing data based on physical location made sense. Today a data transfer means an individual in one location sees and manipulates data that was initially collected in another location, even if that data is stored in the original location. Before the individual can see the data it moves over open networks using routes that change second by second. Furthermore, the resting place for that data may be different today than it will be tomorrow. Therefore governance by location is problematic.

An example may be helpful. A research project might require investigators in a score of locations coming together for a virtual meeting where the data from each is shared with all. The data set used for the meeting exists only for the duration of the meeting. From a governance perspective, which country's laws govern that data during the duration of the meeting? Legacy data protection regimes were not designed to deal with that question. Yet applications such as the one described happen every day.

The alternative to linking controls to geographies is to link controls to organizations. This public policy approach that targets organizations rather than geography is known as accountability. Accountability requires the organization to have policies and mechanisms to put those policies into effect, and be answerable to regulators for the effectiveness of those policies and mechanisms. This concept of responsible and answerable organizations rests on the foundation of the accountability principles that are part of the OECD Privacy Guidelines and APEC Privacy Framework. European Binding Corporate Rules and APEC Cross Border Privacy Rules are certified accountability. There is a growing awareness that privacy governess for emerging technologies and business processes will increasingly have to depend on accountability. The

essential elements of accountability are described in the "Galway Paper" released by the Global Accountability Project in 2009.[3]

Canada already uses accountability to govern transfers, and the new Singapore data protection law uses organizational accountability to assure adequacy. I believe, over time, judging organizations rather than geographies will facilitate the global movement of data.

The creation of certified accountability in both Asia Pacifica and Europe has led to discussion on interoperability between legal seems that approach privacy from different perspectives. APEC and the EU both have mechanisms for certified accountability, Cross Border Privacy Rules in APEC and Binding Corporate Rules in Europe. There are currently discussions ongoing between the EU and APEC on how those regimes might work together. Interoperability holds promise for narrowing issues between privacy enforcement based on harm and data protection.

Cultural Differences in Observation

The freedom for an individual or organization to observe another in the United States tracks to free expression and the First Amendment to the Constitution. I am free to observe you in a public place, including your front yard. I am free to observe you in your back yard as I fly overhead. However the freedom to observe is not unlimited. I am prohibited from observing you by sticking my head in your window.

This freedom to observe extends to the digital world. The Internet has made observation both easier and easier to create a record of that observation. The targeted advertising that makes free content available on the internet is an example of the fruits of this freedom to observe.

This freedom to observe is uniquely American. Data protection regimes, on the other hand, require permission every time data is touched. In data protection countries digital observation is a processing of data. Therefore there is a conflict between business processes developed in the United States that include observation, and the application of data protection law outside the United States. This limits the ability to take innovations developed in the United States based on observation and apply them in data protection countries.

This is not new. Justice Michael Kirby, former Chief Justice of the Australia High Court led the group of experts that developed the OECD Privacy Guidelines. Justice Kirby observed, in a speech in delivered at the OECD in 2010, that the hardest issue to resolve in the 1980 negotiations was the difference in the way Americans look at free expression, and the more limited application of free expression in the balance of the OECD member states.

[3] The Centre for Information Policy Leadership is the secretariat for the Global Accountability Project

I believe the toughest trade impediments to resolve will be those based on cultural and legal differences on how countries view observation.

Legal Obstacles to Big Data and Advanced Analytics

Innovation in a modern economy is increasingly driven by the application of mathematics to large data sets. Over time those data sets have become larger and more diverse, with the aggregation of data from many sources. Today data scientists conduct analysis to see the insights they can gather by overlaying data sets over other data sets. We often refer to this new methodology as big data. There are limited restrictions to big data processing in the United States, and the restrictions are typically based on specific identified harms. For example lenders may not discriminate based on gender, race or age, and therefore lenders may not use predictive models that use those criteria.

Data protection laws typically require that individuals be made aware of the purposes for which data is collected. Big data processes are about discovering the predictive value of data, therefore one often does not understand the purposes for which data will be used until after the discovery phase of big data.[4] As U.S. increasingly applies big data processes one will find friction between business processes originating in the United States and applied in countries with legacy data protection regimes.

Businesses and economic leaders are increasingly recognizing the innovative value that comes from big data processes and advanced analytics. The Centre for Information Policy among others is working on ways to use accountability to create governance structures for big data that will be acceptable in European countries with data protection law. European law allows for the use of legitimate business interest combined with risk abatement to create a legal basis to process. The Centre issued a paper February 28, 2013 that covers this issue directly.

Finding a legal basis to conduct big data processes in data protection countries where processing permissions are consent based might be more difficult. However I am confident those issues will be resolved.

Conclusion

The differences between the privacy mosaic that exists in the United States and the more control oriented data protection laws in much of the rest of the world does act as an impediment to the free flow of digital goods between the United States and those countries. There is no question that those differences create costs for American business and impede the exploitation of innovations that are developed in the United States.

[4] "Big Data and Analytics: Seeking Foundations for Effective Privacy Guidance," Centre for Information Policy Leadership, February 28, 2013 describes a two phase approach to big data with the first phase discovery.

Those differences may be classified as impediments to transfer, and limits on the export of observation and big data based business processes. I believe the differences on transfers and big data will be narrowed over time. The economic necessity of moving data freely, and using predictive sciences to create new value are becoming so crystal clear that these issues will be resolved. It will take work and negotiations but the global community will find better governance structures. Legislating the new governance structures will be hard, but will happen.

I also believe that the differences in view on observation based business processes are deep seeded and will be more difficult to resolve. Some of the narrowing may occur when the United States begins to define the limits of observation on the Internet, like we have in physical space.

Thank you for your time and interest. I will be pleased to answer your questions.