Remarks to the European Parliament

Interparliamentary Committee Meeting on
The Reform of the EU Data Protection Framework:
Building Trust in a Digital and Global World

Session VII: Data Protection in the global context -
The transatlantic dimension

Cameron F. Kerry
General Counsel
United States Department of Commerce

October 10, 2012

I. Introduction

In a joint statement issued in March of this year, EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson said "[t]he United States and the European Union clearly share a commitment to promoting the rights of individuals to have their personal data protected and to facilitating interoperability of our commercial data privacy regimes."[1] In this spirit, the United States has invited the EU to participate in its multistakeholder processes to create enforceable codes of conduct in areas not currently subject to data privacy laws in the U.S., and today the EU listens to the United States' perspective on legislative proposals to reform and strengthen data protection laws and enforcement rules in the EU.

This collaboration would not be possible if we did not share values. In the EU, privacy is articulated as a fundamental right. This committee is focused on the best way to update privacy principles implemented in its comprehensive privacy law and recognized in the Lisbon Treaty. In the United States, respect for privacy is broadly enshrined in the Bill of Rights to our Constitution. Our desire to preserve individual autonomy led the United States to establish

[1] U.S.-EU Joint Statement on Privacy from EU Commission Vice-President Viviane Reding and U.S. Commerce Secretary John Bryson (19 March 2012).

privacy protections for a broad array of sensitive sectors such as health, finance, and education. Concern for how the government manages personal data in its possession led to enactment of the federal Privacy Act and development of the Fair Information Practice Principles (FIPPs) in the 1970s. These same principles informed the 1995 EU Privacy Directive. The Federal Trade Commission and State Attorneys General vigilantly enforce general consumer protection laws to provide consumer privacy protections in sectors that are not covered by a specific Federal data privacy law.

The U.S. and the EU also share commitment to fostering economic growth, innovation, and job creation.[2] Both the U.S. and EU understand that privacy protections are critical to maintaining consumer trust online, and that this trust is critical to the growth of the digital economy. These factors can help companies grow. While developing rules of the road to protect privacy, we must also recognize that the changing digital landscape is constantly evolving and innovating. Privacy protections must be flexible enough to encourage trust and allow for innovation.

These purposes are especially important in fragile economic times. The United States and Europe are linked not only by common values but also by inextricable economic ties. Trade between the EU and U.S. accounts for nearly one-third of world trade flows and is responsible for approximately 15 million jobs.[3] As we each work on the project of improving our respective privacy protections for individuals, we also must maintain and grow this economic partnership and allow our companies to develop and market products and services that support the economic

[2] *See* **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, COM(2012)9 (25 January 2012).**
[3] http://ec.europa.eu/trade/creating-opportunities/bilateral-relations/countries/united-states/

jobs and growth agenda each of our governments seeks to advance. In this context, we should be careful to do no harm.

II. Overview of President Obama's Privacy Blueprint

In February 2012, President Obama released his privacy blueprint, reaffirming our nation's commitment to privacy. As the President wrote, "Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones. … So, it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our time."[4]

The privacy blueprint proposes a framework consisting of four key elements: A Consumer Privacy Bill of Rights; a multistakeholder process to specify how the principles in the Consumer Privacy Bill of Rights apply to particular business contexts; baseline legislation enabling strong and effective enforcement of the Bill of Rights by the FTC; and a commitment to increase interoperability between the United States' privacy framework and those of our international partners. The privacy blueprint in full is attached to this submission.

The first element of the privacy blueprint, the Consumer Privacy Bill of Rights, adapts the Fair Information Practice Principles to provide affirmative statements of rights designed to give consumers understandable guidance as to what they can expect from companies and how they can take responsibility for their information. The principles call on companies to examine their relationship with consumers as well as their own needs and practices, to limit the collection and retention of data appropriately, and to secure this data. The principles as set forth by the Administration are individual control; transparency; respect for context; security; access and accuracy; focused collection; and accountability.

[4] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (23 February 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

The Administration has proposed that the principles be enacted into legislation as a Consumer Privacy Bill of Rights to provide a foundation for consumer privacy in areas not currently covered by specific Federal data privacy laws.

The second element of the privacy blueprint is to foster multistakeholder processes to develop codes of conduct specifying how the principles in the Consumer Privacy Bill of Rights apply to particular business contexts. In the United States, we use the multistakeholder process to engage the private sector, civil society, and other interested viewpoints to develop codes of conduct. Our privacy blueprint includes international partners as stakeholders, and we have extended an invitation to DG Justice to participate in our multistakeholder processes. The first multistakeholder process is underway to develop a code of conduct addressing mobile application transparency − how companies that provide applications and interactive services for mobile devices provide information to end users about how personal data is used. A second multistakeholder process on another issue will be announced shortly. For the United States, such multistakeholder processes are the key to development of nimble and adaptive protections that reconcile the interests and concerns of consumers and businesses alike.

The third element of the Obama Administration's privacy blueprint is effective enforcement. The strongest policy in the world means little if it is not implemented or is honored more in the breach than in the observance. In the United States, we have strong enforcement by the Federal Trade Commission and by the state attorneys general. Although we do not currently have privacy legislation that applies generally to every business – and we are trying to change that – we can still hold companies accountable to the public promises they have made for handling personal data, be it via their privacy policy, by subscribing to the Safe Harbor Framework, or through other public commitments. This is very different from pure self-

regulation in which companies set their own rules and face no consequences for breaching them. In the United States, these commitments are actively enforced by state and federal authorities, and have led to remedies that require specific, ongoing commitments for privacy protections. Companies are being held to the commitments they make.

The final element of the Administration's privacy blueprint is to promote international interoperability. The United States seeks international cooperation to create frameworks that permit secure and efficient cross-border data flows that protect individuals' privacy so that differing approaches to commercial data privacy do not become barriers to trade and commerce, harming both consumers and companies. Interoperability does not mean that approaches to privacy must be identical; rather it means that they are able to work together seamlessly despite differences. The vital element is mutual recognition – an agreement whereby two governments recognize the legal effect of each other's system based on common principles and comparable protection. Such interoperability is critical to maintaining our extraordinary economic relationship, fostering trade and preventing non-tariff barriers, and unlocking the full potential for our economic innovation and growth.

III. Comments on the Proposed Data Protection Regulation

We have carefully reviewed the proposed Data Protection Directive and Regulation. The draft Regulation is a comprehensive document that demonstrates thorough consideration of an extraordinarily wide range of data protection questions we all share. We recognize many points in common with our own effort to update U.S. privacy laws. Nevertheless, I would like to focus on a few aspects of the proposed regulation in light of our shared interest in protecting commercial data, enhancing consumer trust, and promoting continued data flows and economic growth of the global digital economy.

The first is how adequacy is treated.

The EU and the U.S. have different legal systems, but these differences in legal systems do not hamper our ability to export goods and services to each other. Our laws on patents, copyright, anti-bribery, competition, computer fraud, and many other laws relevant to businesses and consumers may differ, but we have developed mechanisms and frameworks of mutual recognition and assistance that allow our enforcement officials and interested parties to seek redress in matters that cross national borders.

So it should be with privacy.

The Obama Administration's privacy blueprint calls for mutual recognition of privacy frameworks based on common principles. Mutual recognition is a two-way street – it requires global partners to consider and understand each other's systems, and to build upon their shared values. It also leads to global partners being able to enforce companies' privacy obligations. Enforcement cooperation and effective enforcement therefore are essential for successful implementation of mutual recognition and true interoperability.

The US-EU Safe Harbor Framework is a concrete example of a flexible mechanism to enable mutual recognition. The Framework has provided thousands of small and medium sized enterprises based in the United States, as well as large multinational companies, with the opportunity to certify their willingness to adhere not only to U.S. law but also to specified practices required to do business in the EU. An independent recourse mechanism ensures that there is a readily available and affordable way to resolve disputes. FTC enforcement has been critical to ensuring that companies meet their Safe Harbor commitments.

While the proposed Regulation ensures Safe Harbor will continue to enable trade and privacy protection by grandfathering existing determinations, and also endorses the use of

Binding Corporate Rules, it could do more to enable similar mechanisms for mutual recognition and allow development of new mechanisms. The proposed Data Protection Regulation, like the current Directive, defines adequacy as a one-way recognition. Instead of allowing differing legal systems to coexist and encouraging enforcement cooperation to achieve interoperability, it would insist that non-EU legal systems harmonize with the EU as a prerequisite to the free flow of information across its borders. This focuses on differences rather than points in common, and on the process of privacy protection rather than the outcomes.

The provisions on data transfers to non-EU countries also do not take into account that the global marketplace runs on continuous, instantaneous transfers of data streams around the world, and is responding by creating innovative methods that permit interoperability of regimes with differing legal systems. For example APEC, the Asia-Pacific Economic Cooperation Group, has created a voluntary system of Cross Border Privacy Rules based on agreed privacy principles coupled with accountability. The United States was the first to apply to be part of this transnational mutual recognition system followed by Mexico, and several other of the world's largest economies expect to apply soon. The applicant countries are currently seeking suitable accountability agents to certify that participants meet stringent, globally-recognized standards; when the system is fully operational it has the potential to streamline the data privacy policies and practices of companies that operate throughout the APEC region, facilitating the transfer of personal data in a privacy-protective manner.

The global marketplace will demand mutual recognition and innovative solutions that permit businesses to streamline their operations across countries with differing legal regimes, as the Cross Border Privacy Rules do. Streamlined and clarified Binding Corporate Rules ("BCRs") also could be a useful tool for holding multinational actors accountable on a global

basis. The Regulation could be enhanced to provide more details about how to assess the adequacy of proposed BCRs and their verification and monitoring mechanisms. A mechanism for efficiently converting codes of conduct into BCRs also could serve as a useful tool.

In the Obama Administration's Consumer Privacy Bill of Rights, one of the principles articulated is accountability. Accountability would provide consumers with the right to have their personal data handled by companies that have appropriate measures in place to ensure they adhere to all of the privacy principles discussed. This principle seeks to make companies accountable to both consumers and enforcement authorities to adhere to the Consumer Privacy Bill of Rights, and to make companies hold their employees responsible for adhering to these principles. Accountability would also require that when a company discloses personal data to a third party, the company should make the third party contractually obligated to adhere to the Consumer Privacy Bill of Rights, unless required by law to do otherwise.

The United States recommends that when reforming the EU Data Protection framework, Parliament recognize the value of mutual recognition and allow for the development and adoption of trans-border accountability mechanisms as a means of facilitating effective privacy protections while still promoting innovation and enhancing trade. For example, Canada's federal privacy law allows for trans-border data flow so long as the recipient of the data is bound to a comparable level of protection.

A second issue we wish to address is the setting of technical standards. In our review of our own privacy framework, we concluded that technical standards were best set by multistakeholder processes, and not by federal regulation. We believe that government policymakers and regulators must approach technical standards with a measure of humility that recognizes the limits of their ability to keep pace with technological change.

This is consistent with longstanding U.S. statutory and administrative policy promoting the use of standards development organizations (such as ISO, the International Standards Organization) leading the development of voluntary consensus standards. It is also consistent with the OECD Council Recommendations on Principles for Internet Policymaking. The Obama Administration has stepped up reliance on standards as an important tool for innovation; a White House memorandum released in January on *Principles for Federal Engagement in Standards Activities to Address National Priorities* notes that "The vibrancy and effectiveness of the U.S. standards system in enabling innovation depend on continued private sector leadership and engagement. Most standards developed and used in U.S markets are created with little or no government involvement."

The proposed Regulation vests broad authority in the European Commission to prescribe uniform technical standards for achieving data protections. Technical measures have an essential role to play in protecting data privacy, but specifying by government prescription what such mechanisms should be would be unwise. The Internet runs on standards that were developed in consensus-based multistakeholder processes, allowing for all stakeholders to voice their concerns and opinions, and resulting in a product that considered as many possibilities and contingencies as conceivable to provide an adaptable platform in a fast-changing technological environment. The change in this environment moves at a faster pace than government regulation, and prescriptive standards can freeze or retard technological development.

Think back five years: the first iPhone had just been introduced. Today, over half of mobile users in the United States own smartphones, and over 45% of mobile device users use smartphones in the EU countries tracked by comScore.[5] Before the iPhone, one standard

[5] Number of European Smartphone Users Accessing News Surges 74 Percent Over Past Year, comScore Press Release (22 March 2012), *available at* http://www.comscore.com/Press_Events/Press_Releases/2012/3/

considered for adoption was to require that the middle key of cell phone dial pads have a raised dot to facilitate use by the visually impaired. Had that standard been adopted, it could have blocked the glass panel screen and virtual keyboard that is ubiquitous on smartphones and tablets today.

The United States recommends that as the EU reforms its data protection framework, Parliament should recognize that overregulation of technical standards may fragment global markets and pose major obstacles to interoperability and innovation. Even if the Regulation provides stakeholders with opportunities to review and comment on proposed rules, the sheer number of possible delegated acts could put a serious strain on stakeholders' resources, which in turn would degrade the quality of input that the Commission receives. The United States supports a bottom-up, consensus based, multistakeholder approach to standards development.

Another issue where we would urge you to consider modifying the draft is in the description of consent. One of the most significant principles that distinguishes the Consumer Privacy Bill of Rights from some articulations of the FIPPs is Respect for Context. This principle expresses that consumers have a right to have personal data collected and used in ways consistent with their relationship with the company.

Respect for Context draws on the more traditional principles of "purpose specification," that the use of the data intended by the company should be indicated in advance of its collection, as well as on the principle of "use limitation," which would prevent companies from using personal data outside of the specified purposes previously articulated. Respect for context builds on these traditional principles, but further refines them to benefit both consumers and businesses,

---

Number_of_European_Smartphone_Users_Accessing_News_Surges_74_Percent_Over_Past_Year?piCId=66039; Alex Cocotas, U.S. Smartphone Penetration Hits 50%, Business Insider (03 October 2012), *available at* http://articles.businessinsider.com/2012-03-30/news/31258792_1_smartphone-click-range; Dan Graziano, More Than 50% of U.S. Mobile Users Own Smartphones, BGR (07 May 2012), *available at* http://www.bgr.com/2012/05/07/us-smartphone-penetration-50-percent/.

by recognizing that consumers generally understand that companies use personal data for purposes consistent with the context in which the consumer discloses the data. The principle also recognizes that a one-size-fits-all consent requirement could cause frustration to individual users because of a proliferation of consent requests and ultimately could devalue the significance of consent as consumers simply click through rather than stop to make informed choices. Recognizing that relationships between a consumer and a company can change over time in an unforeseen manner, this principle limits the use of personal data to uses that are consistent with the consumers' original purposes in disclosing data.

Respect for context allows adaptive uses of personal data in innovative ways that may benefit consumers, so long as the company affords appropriate transparency and individual control to the process. This provides companies with flexibility, but also requires them to understand and act consistently with consumers' expectations about their practices and to give consumers meaningful choices about the collection, use, and disclosure of personal data. This principle also holds that privacy controls should be adapted to the age and sophistication of the typical users of a company's products or services, creating a framework that may require greater protection for personal data obtained from children and/or teenagers than for adults.

Another principle in our Consumer Privacy Bill of Rights is individual control, which would provide consumers with the right to exercise appropriate control over what personal data companies collect from them and how they use and disclose it. Notice and choice is one way to enable individual control, but it can be more effective and meaningful if reserved to situations where the contemplated uses of data are not readily apparent from the context. As technology evolves, we envision the capability to offer consumers options that go beyond a binary choice. An important and complementary aspect of individual control is the right to withdraw consent to

use personal data that a company controls. The means of withdrawing consent should be on a comparable footing with the means used initially to grant consent.

Empowering individuals with control over the collection, use, and disclosure of data about them is crucial for effective privacy protections. However, we recognize that users may expect, and indeed prefer or even demand, different rules to govern different types of personal data collection depending on the context of the interaction. The privacy blueprint therefore allows for consent to be inferred in certain contexts, such as sharing your mailing address with a shipping company to enable delivery of a purchased item, and does not always require active opt-in consent to the use of personal data when consent can be reasonably inferred.

Similarly, the EU has not understood consent to be exclusive of other bases permitting the usage of data. To the contrary, the EU has recognized that, in some instances, an unvarying requirement of opt-in consent can actually diminish effective privacy protections, as users habituate to too many notices. As the Article 29 Data Protection Working Party has stated:

> Consent is one of several legal grounds to process personal data. It has an important role, but this does not exclude the possibility, depending on the context, of other legal grounds perhaps being more appropriate from both the controller's and from the data subject's perspective. If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing.[6]

The existing Directive defines consent as "any freely given specific and informed indication" of agreement,[7] whereas the proposed Regulation requires a "freely given specific, informed *and explicit* indication" of agreement.[8] We believe that, in the digital age, consumers need to be presented with simplified but *meaningful* opportunities to consent, and with choices

[6] Opinion 15/2011 on the Definition of Consent, Article 29 Data Protection Working Party, 01197/11/EN WP187.
[7] 95/46/EC (24 October 1995) at Art. 2(h).
[8] Proposal for a Regulation 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 (25 January 2012) at Art. 4(8) (emphasis added).

that match the scale, scope, and sensitivity of the information itself or its uses. The United States recommends changes to the draft Regulation to indicate that consent need not always be active opt-in consent, and that the means for individuals to communicate their choices should match the scale, scope, and sensitivity of the personal data that organizations collect, use, or disclose, and should also match the sensitivity of the uses made of the personal data.

The United States also recommends that Parliament carefully examine the so-called right to be forgotten and the right to erasure and make appropriate modifications to avoid hampering the ability to innovate, compete, and participate in the global economy. The proposed right to be forgotten permits individuals to have their personal data erased where the data is no longer necessary in relation to the purposes for which the data were collected, where consent for processing data has been withdrawn, or where there is an objection to processing of personal data.

This generally aligns with the Consumer Privacy Bill of Rights. Our principle of Respect for Context mirrors the concerns that data processing must have a relation to the purposes for which the data were collected. Our principle of Individual Control reflects the concern that individuals must be able to withdraw consent for a company to use their personal data. And our principles of Access and Accuracy and Individual Control work together to enable an opportunity to object to processing of inaccurate personal data in a manner that is appropriate to the sensitivity of the data and the possible consequences to the individual.

The Consumer Privacy Bill of Rights would not allow consumers to demand a full deletion of data from United States companies in all circumstances. Similarly, the proposed EU regulation does not suggest the right to be forgotten is an absolute right, as it permits further retention of data "where it is necessary for historical, statistical and scientific research purposes,

for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them."[9]

But the right to erasure as articulated in the proposal would oblige a data controller that made personal data public, with an individual's consent, to inform third parties when consent is withdrawn. Furthermore, the proposal recommends that the data controller be considered responsible for authorized third party publications or republications. Such obligations would require data controllers to be responsible for data that is not under their control, and potentially expose them to large fines for failing to compel erasure of data regardless of their ability to direct the third party.

Furthermore, consumers may not understand any limitations to the right to be forgotten, and rely to their detriment on the belief that personal information they provide may be "erased" from the Internet upon future demand, unaware that technical limitations may effectively preclude the desired deletion. The right to erasure could, therefore, have the unintended consequence of encouraging consumers to disclose personal data that they might otherwise safeguard better, thus actually lowering effective privacy protections. There are likely other unintended consequences from the proposed rights. Wrongdoers could erase evidence of their misdeeds, impacting the ability of companies to perform internal risk management such as credit card fraud detection and regulatory and non-criminal enforcement investigations. The proposed rights may interfere with record preservation requirements outside of the EU.

Furthermore, the protection afforded to freedom of expression when it stands in conflict to these proposed rights extends only to where the retention of personal data is "necessary" to

[9] COM(2012) 11 at recital 53.

exercise of expression "in accordance with Article 80."[10] By proposing a regime where information may presumptively be banned unless affirmatively determined to be "necessary" to freedom of expression, the regulation positions freedom of expression as the exception rather than the rule. Article 80 also allows derogations for the processing of personal data "solely for journalistic purposes or the purpose of artistic or literary expression," a standard well short of the general right to freedom of expression.[11]

We recommend that when you examine the right to be forgotten and the right to erasure, you consider the feasibility of placing obligations on a data controller for publications made by others after consent is withdrawn, and the appropriateness of providing derogations of the right to erasure with full deference to the full right of freedom of expression as defined by the International Covenant of Civil and Political Rights or similar multilateral convention.

A fifth issue of concern is the notification period for informing supervisory authorities and consumers of data breaches. Article 31 mandates notifications to supervisory authorities "without undue delay" and, where possible, within 24 hours. Article 32 mandates notification to consumers "without undue delay." Currently, the United States has breach notification laws in 47 States, the District of Columbia, and several Territories, and federal government agencies are subject to breach notification requirements. The Obama Administration's privacy blueprint calls for a national notification standard. In our experience, detecting breaches and assessing their scope may require more than 24 hours. Furthermore, requiring businesses to provide notice if possible within 24 hours could lead to over-notification of consumers as businesses will include and notify consumers before the scope of the breach is fully defined. Such a practice could lead consumers to ignore notifications or act on information later determined to be erroneous.

[10] COM(2012) 11 at Art. 17(3)(a).
[11] *See*, *e.g.*, International Covenant on Civil and Political Rights ("ICCPR") at Art. 19, which defines freedom of expression to include "information and ideas of all kinds."

The United States seeks clarification about what is considered “without undue delay,” and questions whether more time should be allowed for breach notification than 24 hours if additional time may permit a better assessment of the nature and extent of the breach.

We appreciate the opportunity provided today for a transatlantic perspective on the EU's proposed data protection framework, and to continue our dialog on our different approaches to protecting privacy, mutual recognition, accountability, compliance, and enforcement. We look forward to continued efforts to promote interoperability of our privacy laws.