PROTECTING PRIVACY WHILE MAINTAINING GLOBAL TRADE AND SECURITY REQUIRES FLEXIBLE SOLUTIONS

The United States and the European Union (EU) are both committed to protecting privacy and our respective legal regimes are founded on the same core principles. We have a long-standing relationship of cooperation on data privacy and a deep understanding of the robust privacy protections both of our frameworks provide.

However, the European Commission has proposed a draft data protection framework that will generally require third countries to either be deemed "adequate" or adhere to "appropriate safeguards," a standard that essentially necessitates countries to mirror the EU system for enforcing privacy protections, as a prerequisite for maintaining the free flow of personal data in the commercial, regulatory and law enforcement contexts.

Instead of approaching international privacy protection as a legal harmonization exercise, we should work towards the interoperability of our privacy frameworks based on common principles and accountability mechanisms, as we have always done.

In their current form, the Regulation and Directive can have far-reaching negative effects. Economically, they could stifle innovation and inhibit growth. The legislation could also jeopardize the ability of regulators to maintain global financial market stability, and protect consumers, health and safety. On the law enforcement front, it could endanger the flow of information that is critical to our joint efforts to fight international terrorism and transnational crime, including human trafficking, child pornography and cybercrime.

Above all, given the complex and unpredictable effects the EU legislation may have and the enormous implications for global trade and security, a careful, thorough examination of all of the potential consequences should be carried out and the legislation revised to ensure that security and commerce are not adversely affected.

THE REGULATION: IMPACT ON TRADE, COMMERCE AND INTEROPERABILITY

Like the EU, the United States recognizes the need to apply our privacy principles to new, rapidly evolving technologies. To achieve this goal, we are strengthening our already robust system by initiating multi-stakeholder processes to develop codes of conduct based on the Consumer Privacy Bill of Rights introduced by the Obama Administration. (http://www.whitehouse.gov/sites/default/files/privacy-final.pdf) Nonetheless, our framework will contain variations from EU law and it is critical that these differences not impede transatlantic commerce. Interoperability of our respective privacy regimes 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. Both the U.S. and the EU seek to achieve the same outcomes, including empowering and protecting consumers, despite our different privacy frameworks. We urge the EU to look more toward outcomes that provide

meaningful protection for privacy and focus less on formalistic requirements.

The U.S.-EU Safe Harbor Framework is a concrete example of a flexible mechanism that enables interoperability of our respective regimes. We are pleased that the proposed EU Data Protection Regulation ensures the Safe Harbor Framework will continue to enable trade and privacy protection by keeping its existing adequacy determination in place, and also endorses the use of Binding Corporate Rules. The EU could do more in the new legislation, however, to facilitate cross-border data flows. The United States recommends that the EU encourage the development and adoption of cross-border codes of conduct and other accountability mechanisms as an independent basis for data transfers to third countries. These mechanisms would strengthen privacy protections while promoting innovation and enhanced trade.

THE REGULATION: APPLYING PRIVACY PROTECTIONS TO NEW TECHNOLOGIES AND THE CIRCUMSTANCES OF OUR TIMES

The Internet operates on standards that are developed in voluntary consensus-based multi-stakeholder processes, allowing all stakeholders to voice their concerns and opinions. As a result, these standards are adaptable to a quickly changing technological environment. The OECD recently affirmed the importance of these multi-stakeholder bodies in the Council Recommendation on Principles for Internet Policy-Making. We urge the EU to encourage the development of standards in multi-stakeholder processes, rather than regulatory processes that may lack the flexibility to adapt to rapid technological advancements. We recommend a more flexible approach to consent than currently appears in the draft legislation. The United States believes that consent should be meaningful and that the methods of expressing such consent take into account the context in which it is being given as well as the relevant privacy risks in that context. For example, consent need not always be express, affirmative consent, and 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.

The United States also recommends that the EU carefully examine the proposed "right to be forgotten" and "right to erasure" and make appropriate modifications to avoid hampering the ability to innovate, compete, and participate in the global economy. For example, we suggest that the EU reconsider the feasibility of placing obligations on a data controller for publications made by others after consent is withdrawn. Modifications to these rights are necessary to ensure consistency with the right to freedom of expression enshrined in the Universal Declaration of Human Rights and the International Covenant of Civil and Political Rights.

Based on our extensive experiences with data breach laws in the United States, we believe the proposed notification period for informing supervisory authorities and individuals of data breaches is too short. In our experience, the process of 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 to consumers as businesses will include and notify consumers before the scope of the breach is fully assessed. Such a practice could lead consumers to ignore notifications or act on information later determined to be erroneous.

THE REGULATION: IMPACT ON INFORMATION EXCHANGES AND TRANSFERS TO REGULATORS, LITIGANTS IN CIVIL CASES, AND LAW ENFORCEMENT AUTHORITIES

The Regulation's provisions regarding the transfer of data to third countries or international organizations have potentially disastrous ramifications for regulatory enforcement and private litigation, which depend on transfer of information and personal data among regulators or other government authorities, or between private entities and third country government entities, or litigants in civil and administrative cases.

By the terms of Chapter V, the continued robust sharing of information between our regulatory agencies may be jeopardized unless the scope of the Regulation is clarified to exclude it, or the EC bestows a finding of adequacy or "appropriate safeguards" that applies to sharing among such regulators. We also note with concern that Chapter VI appears to provide data protection authorities with unlimited ability to suspend the transfer of information to third countries, apparently at their sole discretion. We are equally concerned that the sanctions imposed under Chapter VIII will discourage processors and controllers from making transfers in cases where the precise application of the Regulation is unclear.

This Regulation will seriously weaken international regulatory cooperation. U.S. and EU regulators are parties to various bilateral and multilateral informal arrangements and they follow principles of international organizations pursuant to which they collect and share certain information. To the extent that the Regulation restricts how EU and Member State regulators collect, process and transfer data on behalf of U.S. or other non-EU regulators, it may run contrary to their longstanding arrangements.

Similarly, information needed in civil and administrative litigation in third countries often contains personal data, which may include personal data of EU residents. Were the Regulation to encumber the national rules, international agreements and practice that have developed in this area, it would weaken the ability of litigants, including EU persons and businesses, to enforce their claims.

In addition, under the draft Regulation, data controllers may process and transfer personal data if it is done pursuant to a legal obligation or in the public interest, but only if the obligation or public interest is set forth in Union or Member State law. There are several problems with this approach.

First, the proposed Regulation does not fully delineate which matters fall within the public interest, providing instead for the European Commission to further specify this important concept in a delegated act. The Regulation should clarify under what circumstances government authorities (e.g., EU financial regulators, consumer protection regulators, or even data protection authorities) or private entities may share data with regulators in third countries without an adequacy determination. These activities are generally in the public interest and should not be subject to the level of uncertainty found in the proposed Regulation.

Second, even if the scope of the public interest exception were clarified, the requirement that the obligation or public interest be set forth in Union or Member State law ignores the practical reality that data transfers will continue to be necessary for enforcement and compliance with non-EU laws and other public interests not currently contemplated. For example, many multinational entities are subject to existing legal obligations to process and transfer data under both EU and non-EU laws, which arise from regulation, civil and criminal law enforcement requests and compliance monitoring, and discovery requests or court orders associated with civil litigation. These obligations are often crucial for regulators worldwide to safeguard financial markets from abusive practices and systemic risk for market stability purposes, to protect the public through export/import regulations and to enforce competition, consumer protection, privacy, and other laws.

The same serious legal obligations and concerns related to restrictions on the transfer of data to third countries will apply to private parties, including EU persons and entities, in the adjudication of their cases before U.S. civil or administrative courts. These provisions of the draft Regulation would also restrict voluntary reporting of criminal conduct to third country authorities, thereby endangering third country public interests and inhibiting EU persons and entities' ability entities to obtain leniency from third country authorities.

Third, while we believe it inadvertent, Article 3(2) on scope can be read as implicating the activities of third country regulatory agencies where an EU resident engages in certain activities they regulate. It should be modified to remove this ambiguity.

There is also great uncertainty about the extent to which regulatory functions fall into the scope of the proposed Regulation or the proposed Directive. While the Regulation appears to apply to data processing in civil contexts, Recital 16 of the Regulation states that "data processed by public authorities under this Regulation when used for the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, should be governed by [the Directive]." U.S. regulators who solely exercise civil enforcement powers often cooperate with criminal authorities, such that the line between "civil" and "criminal" is not clearly defined. Moreover, U.S. and European legal systems sometimes differ as to which offenses are considered criminal and which are civil regulatory matters. It appears that the Directive could be read to impose restrictions on those regulators without consideration for any of the exceptions, derogations or other protections that the Regulation may offer.

The proposed Regulation affects law enforcement activities of third countries. U.S. law enforcement agencies - including the Departments of Justice, Treasury and Homeland Security - also exercise regulatory functions (e.g., with respect to immigration, financial transactions, importation of drugs or weapons). The administrative investigations they and other U.S. regulators carry out can be referred for prosecution and the data they gather are often crucial evidence in civil and criminal cases. The Regulation's detrimental impact on third country regulatory activities is therefore also of concern to law enforcement authorities of non-EU countries. It is also unclear how the Regulation will apply when conduct is treated as a civil violation in some jurisdictions and a criminal violation in others. For instance, price fixing by international cartels is treated as a criminal violation under U.S. law and under the law of some EU Member States but as a civil violation under EU law.

THE DIRECTIVE: IMPACT ON LAW ENFORCEMENT RELATED ACTIVITIES

Similarly, we are concerned that the Directive will have a detrimental impact on global law enforcement cooperation. A number of these concerns are similar to those discussed above regarding the Regulation's impact on regulatory cooperation. Specifically, (1) Chapter V of the Directive appears to require third countries to adopt an EU-style data protection system in order to ensure continued robust information sharing; (2) Chapter VI gives data protection officials - who by and large will have no law enforcement experience - the final say on whether cooperation should be provided; and (3) Chapter VIII provides for joint and several liability for failure by law enforcement officials to meet the Directive's requirements, even where these requirements are not particularly clear and where the purported violation was not intentional; a penalty that will undoubtedly have a chilling effect on transfers.

In addition, Article 60 would require Member States to renegotiate international agreements to conform with the detailed provisions of the Directive. This would entail the re-opening of hundreds of bilateral and multilateral agreements in force in the criminal justice area, which would be onerous in terms of its resource implications. We also note that renegotiation and modification of international agreements, by definition, require the consent of the other party. Such agreements should instead be "grandfathered", along with the numerous other international cooperation systems in which EU Member States currently participate, including the Interpol system, the Egmont Group of financial intelligence units, the Financial Action Task Force recommendations, and the 24/7 High Tech Crime Network.

The current negotiations of an umbrella agreement on exchanges related to criminal law enforcement between the U.S. and EU that you have undoubtedly heard about will not alone solve the problems with the proposed Directive described above. The implications of the
Directive go well beyond the relationship between the U.S. and the EU; the adverse impact on other non-EU countries will weaken our collective efforts to protect the public.