Informal Comment on the Draft General Data Protection Regulation and Draft Directive on Data Protection in Law Enforcement Investigations

The United States and the European Union share a commitment to protecting privacy, and we are both engaged in significant efforts to reinforce our strong, pre-existing privacy protections. These efforts advance the common goal of protecting individual privacy in ways that also enable innovation and economic growth, promote interoperability across national borders, and protect the safety and integrity of our citizens. The United States understands and respects that the EU is still in the early stages of considering data protection proposals to strengthen and update its framework. At the same time, however, we have heard reports that, based on inter-service consultation, the widely-available versions of the draft Regulation on the processing of personal data and the draft Police and Criminal Justice Data Protection Directive (together, "the draft proposal") may undergo further review before it is released.

We would welcome further review and consultation. As circulated in December, the draft proposals indicate that the proposed legislation is intended to regulate – and indeed would have a significant impact on – several key areas of international cooperation. In light of the draft proposal's potentially negative consequences for international commerce, law enforcement cooperation, cooperation between regulatory authorities, and the privacy of U.S. citizens, we raise the following observations. The issues discussed in this paper are not intended to be comprehensive, and we would very much welcome the opportunity to understand the EU's intentions on these and associated matters in further detail – as the Commissioners consider the final content of proposals to the European Parliament.

As circulated, the draft proposal includes some important steps to promote interoperability in the global commercial sphere and has significant points in common with the forthcoming White House statement on consumer privacy policy. Nonetheless, as discussed below, we are concerned with:

- how the draft Regulation could hinder commercial interoperability while unintentionally diminishing consumer privacy protection;
- its potential impact on human rights, including in particular the right to freedom of expression;
- its impact on law enforcement and public security cooperation;
- its impact on cooperation between government authorities enforcing consumer protection, financial services and even privacy laws, as well as conducting market oversight; and
- its impact on civil litigation.

More generally, the issues discussed in this paper raise questions about whether the regulatory system proposed is sufficiently flexible to address the challenges we already know it will face: fostering the innovation that has made the Internet an economic engine for the world; addressing changing consumer privacy demands and expectations; facilitating the free flow of information; enabling law enforcement on both sides of the Atlantic to pursue criminals and fight terrorism; enabling effective government oversight of financial markets, international financial institutions, payment systems, and the promoting of effective government protection of individuals rights.

I. COMMERCIAL INTEROPERABILITY

Increasing interoperability is a shared objective that is important to mutual economic growth, but the specific obligations imposed by the draft Regulation may decrease interoperability between the U.S. and EU.

The Internet has proven to be an extraordinary platform for global communications and economic growth. For the Internet to continue its evolution, we must sustain interoperability among different national and regional privacy frameworks, which will facilitate the cross-border data flows that allow the Internet to flourish as a global network. For more than a decade, the U.S.-EU Safe Harbor Agreement ("Safe Harbor") has been the premier example of interoperability between the United States and the EU. Safe Harbor has enabled more than 3,000 companies to transfer personal data from the EU to the U.S. and is a vital component of transatlantic trade.

To increase global interoperability further, the U.S. Government has also been working actively with countries in the Asia-Pacific region to create a framework for interoperability among the 21 member economies of the Asia-Pacific Economic Cooperation forum. APEC's system of Cross-Border Privacy Rules (CBPRs) includes privacy principles that APEC member economies have agreed to recognize. We anticipate that the APEC commitments will lead to increased trade and economic opportunities throughout the Pacific region in the coming years. The success of Safe Harbor and the keen interest in the APEC CBPRs demonstrate that companies are willing to commit to privacy practices that go significantly beyond their domestic legal obligations if these commitments enable them to do business in more countries at acceptable administrative costs.

The gains from Safe Harbor, APEC CBPRs, and similar frameworks, however, are contingent on a) mutual recognition of different countries' substantive privacy protections, based on reasonable consistency among these protections; b) requirements that are flexible and adaptive to the dynamic Internet environment; and c) exercise of jurisdiction that is consistent with global practice. The draft Regulation poses concerns in all three of these areas.

A) MAINTAINING REASONABLE CONSISTENCY OF PROTECTIONS

We are encouraged by the draft Regulation's treatment of Binding Corporate Rules and Codes of Conduct, although we believe some enhancements would improve international interoperability and protect consumers in the EU, the U.S., and worldwide.

The draft Regulation takes the noteworthy step of explicitly recognizing binding corporate rules (BCRs) as a legal basis for transferring personal data to a third country in the absence of an adequacy finding. Importantly, Article 40 establishes a single process, led by the supervisory authority of the Member State in which an entity is established, for Union-wide recognition of BCRs. This structure will afford efficiency for companies while ensuring that BCRs implement consistent interpretations of the draft Regulation's data protection standards. Article 40 also sets forth many elements of accountability that can be effective in creating a culture of privacy awareness within organizations. As a result, BCRs could become a more attractive and widely used option for organizations that deal with personal data flows that are well-specified in terms of data categories, purposes of processing, and destination.

The BCR provision could be enhanced to provide more details about how supervisory authorities, the European Data Protection Board, and the Commission should assess the adequacy of proposed BCRs and the verification and monitoring mechanisms specified in BCRs. The entities that may wish to adopt BCRs could vary significantly in size and in the privacy risks their personal data practices entail. To take verification as an example, possible mechanisms could range from self-certification (i.e., an entity conducts a review of its operations to determine whether the entity complies with the assertions in BCRs) to full audits. It would be helpful if the draft Regulation provided more information on what type of verification data protection authorities should regard as sufficient.

As stakeholders have indicated to us, we believe codes of conduct developed in multi-stakeholder processes can be used as mechanisms to increase global interoperability and to protect consumers in the face of rapidly evolving privacy challenges. We are encouraged by the provision on codes of conduct in the draft Regulation. Stakeholders have indicated to us that global interoperability could be further enhanced if the draft Regulation explicitly linked codes of conduct and BCRs. There does not appear to be a mechanism for organizations to efficiently convert codes of conduct into BCRs. Codes of conduct that apply to specific sectors (e.g., mobile device applications) or address specific issues (e.g., accountability) could include not only practices that comply with the draft Regulation's substantive provisions but also mechanisms for robust monitoring and oversight. Input from stakeholders in civil society, academia, and enforcement agencies could further strengthen these aspects of codes of conduct. The result would be consistent sets of practices that organizations could adopt and make the basis for BCRs, with relatively low burden to EU data protection authorities. We look forward to exploring these ideas with the EU.

B) Requirements Should Be Flexible and Adaptive to the Dynamic Internet Environment

As a uniform rule, explicit consent could pose serious obstacles to the provision of Internet services and the interoperability of other privacy frameworks with the EU, while providing questionable privacy protection benefits in many instances.

Providing individuals with control over the collection, use, and disclosure of data about them is a central element of privacy protection. Historically, individual control has been a key element of the globally recognized Fair Information Practice Principles (FIPPs), and it will be included within the Administration's Consumer Bill of Rights. Individual control is equally important in the digital economy. Though some kinds of personal data collection strongly implicate individual privacy interests, with other forms of collections, consumer expectations fit squarely in the context of the collection. Distinguishing between these cases, and offering individuals more explicit choices in cases of greater privacy risk, provides effective protections and prevents individuals from being overburdened.

The risk of requiring explicit consent in nearly all cases is that individuals will lose sight of which choices are most significant to them. This insight is an element of preliminary privacy frameworks presented in 2010 by the U.S. Department of Commerce and the FTC. Both

frameworks embrace the idea that individual choices should be simplified and *meaningful* and take into account the complex environment that individuals face in the digital age. To this end, 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, as well as the sensitivity of the uses made of personal data. A single standard for consent does not serve this purpose.

Moreover, the single standard chosen by the draft Regulation may be particularly ill-suited to certain types of online commerce, such as financial products and services. Consumers and company managers both rely crucially on the online delivery of financial products and services, which typically are delivered through multiple networks managed by one or more financial institutions. The demands of the draft Regulation could substantially impair access to and use of those products and services. This is particularly true of the requirement that consumer consent be obtained only for specific purposes. The level of specificity demanded for collecting and processing data could unreasonably interfere with the activities of a financial institution that provides services to consumers both directly and indirectly. The cost of specificity is only exacerbated when the financial institution provides services through multiple databases that are designed to allow consumers to move payments or credits from one system to another (for example, between a pension plan and personal banking). The detailed disclosures apparently contemplated for the data being collected and the consumer's right of access are similarly problematic in this context. They could pose significant challenges to a business such as a financial institution that provides services through multiple channels and changes its information systems and interconnections from time to time – none of which is uncommon or unreasonable for businesses to do.

The draft Regulation proposes that the European Commission should be given broad authority to prescribe uniform technical standards for achieving data protection, which is inconsistent with the approach mandated in international commitments and could stifle innovation.

The draft Regulation correctly recognizes that technical mechanisms have an important role to play in protecting individual privacy. For example, the draft Regulation specifies that appropriate technical measures (as well as organizational measures) are part of achieving privacy "by design," maintaining safeguards among data processors, and keeping personal data secure. But the draft Regulation takes a significant step beyond requiring "appropriate" technical mechanisms by giving the Commission broad authority to specify what these mechanisms should be. For example, under the draft Regulation, the Commission could choose to set technical standards to ensure that personal data "processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." The Commission has similar authority under the data security provision.

The Commission should consider very carefully whether to go down this prescriptive path. Open technical standards developed within consensus-based, multi-stakeholder organizations are the bedrock of the open, globally-interconnected Internet that the United States and a majority of EU Member States have committed to protect and advocate through the OECD's Internet Policymaking principles and the G8 Declaration entitled "Renewed Commitment for Freedom

and Democracy." The openness, transparency, and user choice of today's Internet can best be sustained and advanced in a world in which all stakeholders participate in relevant decision making, rather than one in which governments, or particular groups of stakeholders, dominate. The proposal as currently drafted is inconsistent with this approach.

Additionally, privacy regulations that focus on achieving policy objectives are often more effective than those mandating particular technologies. By requiring a particular technology, a regulator may preclude the implementation of a better privacy solution and stifle innovation that benefits consumers and the economy. For example, the Apple iPhone has been widely acclaimed for providing new and exciting ways for providing members of the blind community with access to communications and content services. In the past, however, some policy experts advocated for a "nub" on the number five to be required on every phone to enhance accessibility for the blind. Such a technological mandate would have made infeasible the iPhone's flat screen interface. Granting the Commission the power to specify technical mechanisms may have significant unintended consequences because technological developments outpace government regulation. Poorly considered or overly prescriptive technical mandates may create a barrier to entry for products seeking to enter the EU market as well as inhibit the evolution of the Internet economy, while at the same time they may fail to anticipate emerging technologies.

By imposing infeasible requirements, the draft Regulation may undermine consumer privacy protections while imposing undue burdens on businesses

The draft Regulation provides for a data breach notification requirement. We strongly support such notification requirements and note that laws in 47 states provide for such notifications in the United States. Various federal laws in the United States also contain breach notification requirements that are applicable to U.S. government agencies as well as particular sectors of industry; the Obama Administration has gone further to propose federal breach notification legislation that would provide uniform consumer protections. Moreover, in the health care sector as well as other sectors, federal law already require notification when there is a breach of personally identifiable health information. Based on this experience with these breach notification requirements, we are concerned that certain of the requirements in the draft Regulation are impractical and would impose significant burdens without enhancing consumer protection.

For example, the draft Regulation requires that a data controller notify a Data Protection Authority (DPA) not later than 24 hours after the personal data breach has been established, with "personal data breach" defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed". Moreover, if the breach is "likely to adversely affect the protection of personal data or privacy of the data subject" the controller must notify the data subject within 24 hours.

In practice, 24 hours is simply too short a period in many cases for businesses to adequately identify the scope of a breach and its potential impact on consumers, in order to be able to satisfy requirements to inform adversely affected data subjects. Electronic breaches may involve millions of records and multiple databases that would need to be analyzed within a day.

Companies facing the massive fines contemplated in the draft Regulation would likely err on the side of over-notification to avoid potential liability. Moreover, consumers may be confused and flooded by notices that later prove to have been prematurely sent or, worse yet, grow complacent as a result of even a few "false alarms" and be unable to identify when their information is truly at risk. Such notifications would also be costly and may adversely and inappropriately impact the reputation of companies. Finally, there are times when delay of notice is appropriate to allow law enforcement to investigate and pursue a criminal. Premature and indiscriminate notification may adversely impact such efforts.

The "right to be forgotten," discussed below, is another example of a well intentioned concept that is infeasible as drafted.

In addition to the problems or impracticalities of specific requirements, we must also consider the cumulative effects of even the technically feasible requirements of the draft Regulation. For example, customers of service providers in information-intensive sectors, such as financial services or human resources management – whether based in the United States or the EU –may face challenges to maintain service relationships without degradation if they move or travel to the other jurisdiction.

Articles 81 and 83 of the draft Regulation may pose serious obstacles to the use of health information for research and quality improvement purposes.

Article 81 requires Member States to ensure that data concerning health may be processed only if it is necessary for a limited list of specified purposes. In general, we agree that it is appropriate to place some limitations on the use and disclosure of health information in order to protect individuals. However, we are concerned that the proposed draft Regulation over-restricts the processing of health information for legitimate purposes which would improve health and health care. Article 81 of the draft Regulation does not mention health research specifically as a permitted justification for processing health data. Neither does it expressly permit the processing of health information for the purpose of improving and measuring the quality of *health care* (although it does permit processing for ensuring quality *payment* purposes). Article 83 which does permit processing for *scientific* research purposes, does not specifically mention *health* research. To the extent scientific research may be construed as including health research, Article 83 would appear to require the data subject to give consent for such research. The utilization of health data is crucial to improving health and health care through research and quality improvement activities and will only increase with the accelerated adoption of electronic health records. The proposed regulation does not adequately provide for the legitimate use of health data for these purposes in an evolving environment and would have a chilling effect on United States research and quality improvement activities done in Europe or involving European patients.

C) ASSERTIONS OF JURISDICTION SHOULD BE CONSISTENT WITH THE GLOBAL NATURE OF THE INTERNET

The draft Regulation asserts EU jurisdiction over the majority of global websites, which would negatively affect global businesses and consumers.

Under the draft Regulation, the EU could assert jurisdiction over a person operating a website that otherwise has no legal nexus with Europe. The unintended consequences of such a sweeping jurisdictional reach could negatively affect the Internet economy.

The draft Regulation would apply to persons outside the EU whose "processing activities are directed to such data subjects, or serve to monitor the behaviour of such data subjects." The draft Regulation does not define "directed to," but the commentary in introductory Clause 15 of the draft suggests a very broad scope. Specifically, Clause 15 states that a data controller's use of "a language or a currency other than the language or currency generally used in the controller's country of establishment" and "the use of a top-level domain name other than that of the country in which the controller is established" will be considered to weigh in favor of finding the data controller to be subject to the Regulation.

These factors suggest that an entity's failure to tailor its online presence exclusively to the country in which it is incorporated makes it subject to the draft Regulation. For example, an organization in the United States that runs a .org website, written in Hindi, and oriented toward allowing expatriates to stay in touch with family members in India would appear to meet the criteria in the draft Regulation. While the draft Regulation sets a limiting principle—"mere accessibility of the controller's website by a data subject residing in the Union is insufficient"—this limitation does not go far enough to ensure that basic notions of fairness are taken into account in the assertion of jurisdiction.

II) ERASURE OF DATA AND FREEDOM OF EXPRESSION

Compelling data controllers to ensure the erasure of data online ignores the open and decentralized nature of the Internet and may undermine freedom of expression. This requirement, as it is described in the draft Regulation, is more likely to hurt citizens than help them.

Under the draft Regulation, individuals could compel a data controller not only to ensure "the erasure of personal data relating to them" but also to "ensure the erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service which allows or facilitates the search of or access to this personal data." As noted above, individual control has been a key element of the FIPPs and is strongly supported by the Administration in its upcoming policy statement. Such control, however, must be considered in the context of the technical limitations of the Internet and the human right to freedom of expression.

Imposing an obligation on a data controller to erase links to, or copies or replications of personal data on "any publically available communication service" would require data controllers to erase data that is most likely not under their control. The data controller at that point may have no ability to compel erasure of the data but nevertheless face large fines for failure to do so. As importantly, consumers who do not understand the technical limitations of the purported "right to be forgotten" may rely upon it to their detriment. Consumers may casually provide data controllers with personal information under the mistaken perception that it will be "erased" from

the Internet upon demand. Indeed, the "right to be forgotten" could have a great many unintended consequences, including the impact on law enforcement and other investigations of empowering those who would commit crimes or violate the rights of others with the ability to erase the evidence of their misdeeds.

A second concern is that the proposal contains only limited exceptions to what is otherwise a sweeping new "right to be forgotten." One such exception provides that the "right to be forgotten" gives way to the freedom of expression only to the extent that the retention of personal data is "necessary" to exercise the freedom of expression "in accordance with Article 79." The draft Regulation actually appears here to be referencing Article 80, which allows derogations for the processing of personal data "carried out solely for journalistic purposes or the purpose of artistic or literary expression," and even then "only if they are necessary to reconcile the right to the protection of personal data with the rules governing freedom of expression."

This approach presents potentially serious concerns regarding the extent to which the proposed Regulation is consistent with the internationally recognized right to freedom of expression. First, Article 80's protection only for the processing of data for "journalistic purposes or the purpose of artistic or literary expression" is considerably narrower than the right to freedom of expression generally, which refers to "information and ideas of all kinds." *See, e.g.*, International Covenant on Civil and Political rights (ICCPR), Article 19.

Second, the internationally recognized right to freedom of expression presumes that individuals may freely express themselves, and allows a narrow range of permissible limitations on expression. In contrast, the proposed regulation appears to establish a regime in which expression containing "any information relating to a data subject" is presumptively subject to being banned unless affirmatively to be "necessary" to the right to freedom of expression. Such a scheme turns freedom of expression on its head as an exception rather than a rule. Under the ICCPR, the right is quite broad and the restrictions are quite narrow and must be "necessary," *i.e.* the least restrictive means to accomplish one of the listed purposes in Article 19(3). That is, under the ICCPR, it is the restrictions on freedom of expression that must be necessary, not the expression.

Third, requiring data subjects, data controllers, supervisory authorities, and courts to undertake the problematic task of judging whether the use of personal data is "solely" for "journalistic", "artistic", or "literary" purposes, and whether the data is "necessary" to the freedom of expression, opens the door to potential censorship and content regulation. Moreover, as a practical matter, data controllers may be more concerned with potential liability than preserving freedom of expression. As a result, they would likely err on the side of deleting information, thereby inhibiting protected expression.

We note as a final matter that there is no internationally recognized human right to be forgotten. In general, the sweeping nature of the so-called "right to be forgotten" as it is set forth in the proposed regulation raises concerns regarding freedom of expression that merit serious consideration, and should be resolved before such a "right" is set forth in legislation.

III) LAW ENFORCEMENT AND PUBLIC SECURITY COOPERATION

The draft Police and Criminal Justice Data Protection Directive would significantly weaken existing international criminal cooperation regimes.

The overriding principle in modern international law enforcement and public safety cooperation regimes is one of broad cooperation, with only narrow grounds for refusal of assistance, which are themselves to be exercised with restraint. By contrast, the draft Directive would limit sharing of evidence and information in penal and investigative matters to the "minimum necessary" and would severely curtail ordinary cooperation with countries whose privacy system varies from that of the EU. In particular, the draft Directive would prohibit the transfer of personal information unless: 1) the European Commission has found the non-EU receiving state "adequate" for data protection purposes; or 2) the transfer is done pursuant to certain binding legal instruments. Although the United States of course has many binding, and recently concluded, legal instruments in place with EU Member States, the draft Directive contains troubling language suggesting that existence of such binding treaty obligations would not, in and of itself, suffice under the Directive as a basis for Member States to share such information outside the European Union. Rather, Article 36 draft Directive suggests that such sharing may only take place if such agreement contains "appropriate safeguards" for data protection. In the context of the Directive, that appears to mean that such existing instruments must meet very specific and problematic privacy protection requirements set out in the Directive—in short, an EU-style system of data protection will be the standard applied by the European Commission for permissible sharing of information by Member States.

The only exceptions to this rule in the Directive are both narrow and vague. For example, there is a public security exception to the ban against providing personal information to third states, but it only allows transfers for an "immediate and serious threat to public security" without further elaboration. Moreover, such information exchanges appear to be possible on only an ad hoc basis, after scrutiny, which will greatly slow down and limit exchanges during circumstances when they are most urgently needed. Notably, the draft Directive contains no exceptions for law enforcement, international security, or foreign affairs considerations of Member States seeking to share information with non-EU partners.

The Directive's limitations on cooperation will have a far reaching and extremely serious impact on U.S. authorities seeking assistance from EU Member States. They would have an equally negative impact on EU Member States seeking assistance from the United States, other third countries and international organizations, such as Interpol. Moreover, the Directive will seriously limit the ability of EU police and judicial authorities to investigate and prosecute crime within their own borders.

The result of these limitations is extremely serious: the United States has a strong system of privacy protection that has developed under the legal, political and cultural conditions present in the United States, just as the EU data protection system has emerged from the conditions prevailing in Europe. However, the provisions of the draft Directive suggest that unless the United States adopts the particular style of data protection regime adopted in the European Union, most existing cooperation between Member States with the United States would be

viewed as inconsistent with its provisions. The result of such limitations, were they to be adopted and observed by Member States, would appear to prohibit providing the United States any personal information in response to requests for assistance.

Moreover, it is not just the law enforcement assistance to the United States that is at stake. The draft Directive will certainly interfere with Member States getting assistance from the United States, and from every other country in the world that does not have a data protection system that mirrors the European Union system. For example, the only way Member State MLAT requests for extraditions or other requests for law enforcement assistance can be carried out in the United States is through providing personal data sufficient to justify the request— e.g., the identity of someone under investigation for money laundering or fraud for the purpose of obtaining bank records, or, facts showing probable cause to obtain email content, or to obtain extradition of a fugitive. If the United States is not deemed "adequate" by the Commission due to variations in our respective legal regimes, or if existing binding agreements between the United States and various Member States are not deemed to contain "appropriate safeguards" for data protection, then the draft Directive would appear to prohibit a Member State from sharing the personal information with the United States to allow us to carry out its request—so the EU Member State will not be able to effectively request extraditions from the United States, and mutual assistance will be dramatically curtailed, whether by Mutual Legal Assistance Treaties or Customs Mutual Assistance Agreements. Civil liberties could be harmed by this restriction, as will law enforcement, with evidence demonstrating innocence or guilt potentially not being discovered.

Interpol cooperation provides another example of the potentially crippling effect of the draft Directive. Like most states, EU Member States use the Interpol system frequently to request various types of police assistance, and in particular, to circulate notices about the identity of criminal suspects and fugitives wanted in their jurisdictions. If, however, the Directive were to permit Member States to provide information through Interpol only to those countries that have been found "adequate," the value of the red notices will be negligible, as only a few countries outside of Europe have been found to be adequate (Argentina, Canada, and Israel).

The provisions of the draft Directive also seek to limit the type and amount of information the Member States can collect within their own jurisdiction for investigative purposes by setting a new standard much higher than the "relevance" standard currently in place in most countries. Instead, under Article 4 of the draft Directive, law enforcement officials must collect and use only "the minimum necessary" personal data to accomplish a specific purpose. This standard will put police and prosecutors in the difficult position of judging how much evidence is "just enough" for an investigation, enforcement or counterterrorism action, or conviction and, for example, when to stop trying to corroborate existing witness statements or when to seek evidence of additional crimes. This is particularly threatening to public servants because the draft Directive also provides for joint and several liability for all "processors" who violate the Directive and cause damage to data subjects (Article 58.2). "Processors" include individuals under Article 3(6). Moreover, the Directive would create a large cadre of new data protection officials whose function it will be to ensure that such limitations are strictly observed. In combination, such provisions would have an inevitable "chilling effect" on the willingness of law enforcement officials to collect information required for complete and fair prosecutions.

Article 21 appears to authorize the Commission to dictate periods that data can be retained by police and judicial authorities in Member States, as well as pass other data protection regulations to implement the Directive without regard for how these actions may impact the ability of law enforcement and judicial authorities to carry out their duties. These provisions are concerning given the lack of traditional law enforcement experience and expertise within the Commission, and police and judicial authorities should be included in determining effective retention periods and other implementing regulations.

As mentioned above, the Directive creates a large cadre of new data protection officials whose function it will be to oversee its implementation. If not carefully handled, the establishment of such officials could both slow and restrict cooperation, since officials lacking law enforcement expertise and with only a data protection mandate may subordinate legitimate law enforcement interests to the protection of privacy. It is critical that these officials be well equipped to participate in meaningful deliberation about the proper balance between the need to protect society against crime and the protection of privacy. Yet, the draft Directive's requirements for data protection officers and supervisory authorities (Art. 33-35, 43 et. seq.) is silent as to whether such officials would be required to have significant experience in law enforcement information gathering and maintenance including international cooperation, nor does it suggest the desirability of finding ways to implement the Directive without lessening the critical and timely flow of information and evidence necessary to do effective, appropriate police work.

Member State compliance with the draft Directive would undermine pre-existing treaty obligations with the United States and other third countries.

Several provisions of the draft Directive would be in conflict with obligations of the Member States toward the United States and other third countries under existing bilateral and multilateral law enforcement treaties, agreements, and conventions, including the UN Conventions against transnational organized crime, corruption and drug trafficking which have achieved near universal ratification. In particular, the draft Directive purports to limit the ability of EU Member States to transfer personal information to third countries in ways directly contrary to the binding legal obligations of EU Member States under the terms of Mutual Legal Assistance Treaties (MLATs) with the United States as well as the Council of Europe Cybercrime Convention. In particular, the U.S.-EU MLATs and the COE Cybercrime Convention create binding treaty obligations on the Member States to provide legal assistance in which Member States are expressly prohibited from denying or conditioning on the basis of general data protection standards. Article 36 of the draft Directive would do just that, prohibiting Member States from transferring personal information to third countries unless the draft Directive's data protection standards are met, in violation of both the U.S./EU MLATs and the COE Cybercrime Convention.

Article 9.2 (b) of the U.S./EU Mutual Legal Assistance Agreement specifically bars "[g]eneric restrictions with respect to the legal standards . . . for processing personal data" as a condition for granting assistance. This provision has been incorporated into the bilateral MLAT's between the United States and Member States, which were re-negotiated in concert with the European Union in a decade long process that culminated in 2010.

The Explanatory Report to the Cybercrime Convention specifically instructs that a "broad, categorical, or systematic application of data protection principles to refuse cooperation is . . . precluded" (Par.269 of explanatory report).

Speaking more broadly, since the Directive would require Member States to limit the processing of personal data "to the minimum necessary in relation to the purposes for which they are processed," and limit sharing with countries that did not meet EU data protection standards, the Directive would significantly alter current practice in the area of mutual assistance in criminal matters. The current norm is exemplified by the language of the widely ratified United Nations conventions on illegal narcotics, organized crime, corruption and terrorism, whereby the parties "shall afford to one another the widest measure of mutual legal assistance" in combating criminality. Under these and other conventions, the overriding principle is broad cooperation and refusal of or limitations on assistance should be narrow and exercised with restraint; the strict limitations proposed in the draft Directive steps backward significantly from this principle. As a result, the draft Directive threatens to put law enforcement authorities at an even greater disadvantage in addressing the increasing threat posed by transnational criminal organizations.

Article 42 of the draft Regulation purports to subject the judgment of foreign courts, government officials, and supervisory organizations to the consent of Member State data protection supervisory authority.

Although it is unclear precisely how this provision of the Regulation would operate, draft Article 42 purports to subject any requirement for the provision of personal information imposed by any foreign court, government body, or enforcement agency to the consent of a Member State data protection authority. More specifically, Article 42 purports to require all data controllers within its scope – including, for example, data controllers located in the United States who store personal information about EU persons (e.g., U.S. located banks, internet service providers, and other businesses who have European clients) – to receive the consent from the supervisory data protection authorities before the data controller can comply with a U.S. administrative or court-issued subpoena or court order. This restriction could have a substantial impact on law enforcement and regulatory oversight in the United States. At its most extreme, the Regulation could block or delay access to information held by U.S. firms and located in the United States necessary to investigate conduct that occurred in the United States in violation of U.S. law, let alone its potential impact on legitimate investigations of EU firms and citizens. Such a provision is inconsistent with traditional practices of reciprocity and judicial comity and will inevitably place data controllers in the middle of irreconcilable conflicts of laws in criminal, civil, and administrative proceedings.

Likewise, it seems possible that the Regulation would enable residents of one jurisdiction to intentionally exploit the variation between different data privacy frameworks and intentionally search for internet service providers that would be subject to a particular data privacy framework that would best hide that data from legitimate requests from other state's law enforcement requests. Efforts must be made to ensure that, while an individual's legitimate privacy expectations are protected, data protection rules are not susceptible to purposeful manipulation in that way.

IV) COOPERATION AND COORDINATION AMONG REGULATORY AUTHORITIES, PARTICULARLY IN FINANCIAL SERVICES, ENFORCEMENT OF LAWS AND SUPERVISION OF ENTITIES AND INDIVIDUALS

Data transfer provisions contained in the draft Regulation would undermine cooperation among U.S., EU, and Member State regulatory authorities and hinder their enforcement and supervisory efforts thereby harming both EU, Member State, and U.S. persons and markets.

The need for effective financial market regulatory oversight has been heightened in the aftermath of the financial crisis. Timely exchange of information including personal data is critical for U.S., Member State, and EU financial regulators to protect the public from fraud and manipulation and to safeguard financial markets from abusive practices and systemic risk as well as for U.S. and EU financial regulators to cooperate in the supervision of cross-border entities and activities.

The ability of U.S. regulators to uphold their missions hinges on the ability of such regulators to obtain and exchange information by: (1) relying on established information-sharing arrangements with EU jurisdictions, (2) accessing information held by EU-based entities registered with the U.S. regulators in order to conduct business in the United States, and (3) communicating with various entities and individuals in the EU who may have information regarding violations of U.S. laws or who may have been harmed as a result of such violations.

U.S. regulators are currently parties to a multitude of cooperative arrangements with EU Member States. For example, the Securities and Exchange Commission (SEC) has almost 20 cooperative arrangements with EU Member States or other EU authorities, including 9 enforcement cooperation arrangements (in addition to the International Organization of Securities Commission's Multilateral Memorandum of Understanding) and 10 regulatory cooperation arrangements and the Commodity Futures Trading Commission likewise has nearly 20 such arrangements (including 9 enforcement cooperation arrangements and 9 regulatory cooperation arrangements, in addition to the IOSCO Multilateral Memorandum of Understanding). In these bilateral and multilateral arrangements, EU Member States and other EU authorities have committed to sharing certain information with U.S. regulators about the activities of persons in the EU and assisting in the obtaining of information from these persons. As a result of these cooperative arrangements, EU entities have been more easily able to operate across the U.S. and European markets, to interact with U.S. clients, investors and customers, and to conduct capital raising and other business activities in the United States

Certain provisions of the draft Regulation threaten to undermine well established processes for obtaining and sharing information. For example, Articles 37-41 threaten to undermine the international regulator-to-regulator data sharing processes pursuant to various information-sharing and cooperative arrangements. Heightened requirements on information sharing may undermine cooperation on specific cases and obstruct coordinated action by regulators in multiple countries. As some of these information-sharing arrangements are based on reciprocity, the proposed Regulation would harm U.S., Member State and EU interests. Article 42 appears to inhibit oversight of U.S.-registered entities located in the EU. As these entities and individuals

would be obligated to produce certain information to U.S. supervising regulators and self-regulatory organizations, Article 42 may affect their ability to conduct business in the United States. Finally, Article 42 may have the unintended consequence of restricting direct contact between U.S. regulators and various entities and individuals in the EU who may be suffering from a wrongdoing as a result of a violation of U.S. laws.

These provisions of the draft Regulation appear to significantly limit information sharing between U.S. regulatory agencies and their counterparts in the EU and EU Member States and may be inconsistent with existing information-sharing and cooperative arrangements. Such limitations may impede the flow of information that must take place between and among regulators and market participants, making it more difficult for EU-based entities to access the U.S. financial markets, and undermine international cooperation to protect U.S. and indeed EU persons.

Thus, provisions of the draft Regulation pose significant challenges to international regulatory cooperation, particularly for highly regulated, highly internationalized sectors, such as financial services, consumer protection, and competition.

Given the potential impact the draft Regulation may have on investor protection, capital formation, market regulation, and the operation of cross-border financial services, the SEC and the Commodity Futures Trading Commission may seek to provide to the European Commission a more comprehensive analysis of the problems raised by the draft Regulation.

V) IMPACT ON CIVIL LITIGATION

Article 42 of the draft Regulation is also of significant concern as it potentially affects all United States civil litigation in U.S. domestic cases where the evidence or one of the parties has an EU presence.

As intimated, Article 42 prevents the enforcement of any court order or administrative ruling for the disclosure of personal data in the EU without obtaining prior authorization by "the supervisory authority." In a change from the current procedures under the Hague Evidence Convention, the supervisory authority, independent of the court's order or any judicial analysis, would assess whether "the disclosure is necessary *and* legally required."

Civil litigation in the United States includes a wide range of matters, from contract disputes to civil fraud investigations to copyright infringement cases to employment actions. Under U.S. rules of civil procedure, the ability to obtain documents relating to a party's claim or defense is central to the U.S. litigation process. If Article 42 were enacted, there would be a risk that the United States and U.S. litigants would be unable to obtain, pursuant to the Hague Evidence Convention or otherwise, evidence sought by civil investigative demands (CIDs), civil subpoenas, civil discovery requests, or court orders when the information sought or a litigant is located in the EU.

For example, in a U.S. civil litigation involving purely U.S. domestic parties, Article 42 could prevent a U.S. litigant from obtaining U.S. data stored by a cloud provider in the EU. EU citizen

data would not be at issue. However, due to the location of the information, the information might not be discoverable and the litigants would risk court sanctions for not providing discovery.

U.S. courts currently possess and exercise the power to protect sensitive materials from public disclosure. There are controls and protections in the discovery process. Article 42, unfortunately, creates a means by which parties in a civil litigation, either intentionally or unintentionally, could avoid the legitimate discovery of information.

* * *