SIDLEY AUSTIN LLP
SIDLEY

SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
(202) 736 8000
(202) 736 8711 FAX

araul@sidley.com
(202) 736 8477

BEIJING
BRUSSELS
CHICAGO
DALLAS
FRANKFURT
GENEVA
HONG KONG
HOUSTON
LONDON
LOS ANGELES
NEW YORK
PALO ALTO
SAN FRANCISCO
SHANGHAI
SINGAPORE
SYDNEY
TOKYO
WASHINGTON, D.C.

FOUNDED 1866

Trade Policy Staff Committee
Office of the US Trade Representative
Docket No. USTR-2013-0019

May 10, 2013

Comments of an Informal Coalition of Tech and Internet Companies in Support of Digital Trade and Privacy ("Digital Trade Coalition")

On behalf of an informal coalition of tech and Internet companies ("Digital Trade Coalition"), we are pleased to submit these comments to USTR in connection with the free trade negotiations between the United States and the European Union under the aegis of the Transatlantic Trade and Investment Partnership ("TTIP"). We also respectfully request an opportunity to provide testimony at your upcoming hearings. (These comments serve as a summary of such testimony.)

We commend USTR for specifically inviting comments regarding ecommerce and cross-border data flow issues. This digital dimension to international trade between the world's two largest trading partners is obviously critical to future economic growth, opportunities for innovation and the social well-being of citizens and consumers on both sides of the Atlantic. Enhancing regulatory cooperation between the US and EU on digital trade could provide very significant benefits to both sides without compromising either side's fundamental values.

To account for the full range of digital trade, the Digital Trade Coalition recommends that USTR focus directly on opportunities to promote greater cooperation, coordination and

consistency regarding the regulation of privacy and data protection – as well as cooperating on ecommerce and cross-border data flows. While both jurisdictions share a common objective to protect the privacy and personal information of their citizens, perceived and procedural differences in the respective data protection regimes have resulted in counter-productive conflicts and burdensome inconsistencies. These burdens on digital trade do not primarily reflect material differences in fundamental values or substantive objectives. Rather, the obstacles that US tech and Internet companies face in the EU are analogous to classic technical barriers to trade – they disfavor US business in cloud computing, social media, mobile apps, and other Internet services without any substantial justification.

To date, US businesses operating online in the EU or engaged in transatlantic digital trade have encountered significant obstacles and impediments. Many are well know, including of course the difficulties that US companies have in exchanging data between their European and American operations due to the EU's view that the US does not provide "adequate" privacy protection. This unjustified, unduly negative view of the US regulatory and enforcement regime results in American businesses facing explicit and implicit barriers to doing business in and with Europe. These adverse perceptions as well as the corresponding actions of EU regulators do have real impacts; TTIP can and should help ameliorate these digital constraints to the mutual benefit of both sides.

While the "General Exceptions" in Article XIV of the General Agreement on Trade in Services contemplate national regulation of privacy and protection of personal data, "such measures are not [to be] applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail." Given the

extensive constitutional, statutory and common law regulation of privacy in the US, at both federal and state levels, and the robust – even aggressive – enforcement of privacy standards by the Federal Trade Commission, Department of Health and Human Services, Consumer Financial Protection Bureau, Department of Education, Department of Justice, Federal Communications Commission, fifty state Attorneys General (and DC), private plaintiffs, numerous self-regulatory organizations, and corporate privacy and compliance personnel, we believe it can be plainly demonstrated that substantially "like conditions" of privacy protection prevail today between the US and the EU. However, we believe that greater understanding, consistency and interoperability of such standards and policies can be achieved through the TTIP process.

Accordingly, by seeking to reconcile privacy and data protection standards – and by promoting digital interoperability – TTIP can meaningfully reduce non-tariff barriers to US companies conducting ecommerce and Internet activity across the Atlantic and within the EU. The timing for such recognition is opportune. Privacy policy in both the US and EU is very much in play today – with both sides seeking to enhance protections for their citizens while also promoting innovation, flexibility and economic growth.

In Europe, the EU Commission has proposed a draft Regulation to overhaul privacy and data protection law in the EU. This initiative is of course complex and will have far reaching impacts and implications. But there is hardly unanimity about how much regulation is appropriate even among the relevant EU authorities – the Commission's different Directorates, Member States, Parliamentary Committees, national Data Protection Authorities, EU Data Protection Supervisor, etc. The extensive debate within the EU itself about the draft

Regulation's costs and benefits demonstrates uncertainty about how best to achieve dual objectives: protecting individuals while also providing them with robust digital opportunities.

In the US, we have seen, just since 2012, new privacy frameworks proposed by the White House, FTC, and Commerce Department; Congress is actively considering reform of the Electronic Communications Privacy Act as well as Cybersecurity legislation and other privacy-related bills; and, the National Association of Attorneys General established "Privacy in the Digital Age" as its year-long initiative for 2013. And the Privacy and Civil Liberties Oversight Board is also, as of this week, fully reconstituted with a Senate-confirmed executive Chairman.

These domestic regulatory developments indicate that there is very serious attention to privacy policy right now in both Europe and America. This acute focus on privacy and data protection provides a great opportunity for greater regulatory cooperation and coordination going forward. There is a real possibility today of clearing away much of the regulatory misunderstanding that has heretofore generated unfortunate and unnecessary conflict on matters of digital trade. TTIP can help ensure that future privacy rules are smarter than they are today: simpler, better coordinated, more cost-effective and efficient, and less burdensome and discriminatory. This will lead to more digital trade and ecommerce without sacrificing consumer protection. Indeed, greater clarity and coordination of rules that have well analyzed and justifed, and are consistenly enforced, can lead to higher compliance and better protection with lower costs to society.

At the APEC Summit on November 13, 2011, the President stated that "streamlining and coordinating regulations [to] encourage trade and job creation" would be one of the APEC

leaders top three priorities. These goals that impelled President Obama to issue Executive Order 13609, "Promoting International Regulatory Cooperation," on May 1, 2012.[1] ("International Regulatory Cooperation Order"). In that International Regulatory Cooperation Order, President Obama specifically directed "the promotion of good regulatory practices internationally, as well as the promotion of U.S. regulatory approaches." The Order seeks to advance "appropriate strategies for engaging in the development of regulatory approaches through international regulatory cooperation, particularly in emerging technology areas." The Order states:

> The regulatory approaches taken by foreign governments may differ from those taken by U.S. regulatory agencies to address similar issues. In some cases, the differences between the regulatory approaches of U.S. agencies and those of their foreign counterparts might not be necessary and might impair the ability of American businesses to export and compete internationally. In meeting shared challenges involving health, safety, labor, security, environmental, and other issues, international regulatory cooperation can identify approaches that are at least as protective as those that are or would be adopted in the absence of such cooperation. International regulatory cooperation can also reduce, eliminate, or prevent unnecessary differences in regulatory requirements.

Significantly, Executive Order 13609 requires US agencies **to** submit a "Regulatory Plan" to the Office of Management and Budget that "include[s] in that plan a summary of… international regulatory cooperation activities that are reasonably anticipated to lead to significant regulations." The Executive Order further requires agencies to identify regulations that would have "significant international impacts" and, as part of a mandatory regulatory **"**look-back initiative,**"** to "consider reforms… that address unnecessary differences in regulatory requirements between the United States and its major trading partners." Through these mechanisms, the US is actively seeking to promote ongoing regulatory alignment and develop

[1] 77 Fed. Reg. 26413 (May 4, 2012).

common approaches regulation in ways that will benefit consumers and industry across international borders.

Before offering a number of concrete suggestions, we would note that the perception that EU privacy and data protection standards can operate as regulatory barriers and burdens is by no means exclusively a US point of view. For example, on October 23, 2012, the EU Parliament adopted a Resolution that:

> Recognises that overly burdensome regulatory standards serve as significant barriers to trade ...; underlines the need to avoid creating new (even if unintended) barriers to trade and investment, especially in key emerging technologies and innovative sectors …; regulatory differences [can] unnecessarily impede trade …;[and]interoperability and standards in the domain of e-commerce, recognised at global scale, can help to promote more rapid innovation by lowering the risks and costs of new technologies.[2]

In a May 18, 2011 speech about the impact of the proposed draft EU Data Protection Regulation on business, Viviane Reding, EC Vice-President and EU Justice Commissioner, also expressed support for greater transatlantic cooperation.[3]

The EU's recognition that unnecessary regulatory differences impede trade and investment is the right starting point to find common ground on privacy and data protection. Building on this point, the Digital Trade Coalition offers a number of concrete suggestions for USTR's consideration.

[2] European Parliament resolution of 23 October 2012 on trade and economic relations with the United States, *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2012-388.
[3] "The reform of the EU Data Protection Directive: the impact on businesses, *available at* http://europa.eu/rapid/press-release_SPEECH-11-349_en.htm.

1. Seek TTIP Confirmation of the EU's Proposed "One-Stop-Shop"

Among the key burdens that foreign regulatory schemes can exact on US trade interests are fragmentation, inconsistency, redundancy and procedural complexity. These barriers often entail disparate and disproportionate impacts for foreign businesses who are less familiar with diverse local bureaucracies, and who may be less sympathetic candidates for regulatory assistance, coordination and accommodation.

The TTIP offers an excellent opportunity to mitigate these regulatory barriers to trade. Indeed, we believe that TTIP can help further transatlantic standards that will promote the type of regulatory efficiency principles expressed in President Obama's Executive Order on "Promoting International Regulatory Cooperation." For example, that Order acknowledges:

> In an increasingly global economy, international regulatory cooperation, consistent with domestic law and prerogatives and US trade policy, can be an important means of promoting the goals of Executive Order 13563. *** In meeting shared challenges involving these goals international regulatory cooperation can identify approaches that are at least as protective as those that are or would be adopted in the absence of such cooperation. International regulatory cooperation can also reduce, eliminate, or prevent unnecessary differences in regulatory requirements.

In Executive Order 13563, "Improving Regulation and Regulatory Review," the President identified the importance of avoiding "regulatory requirements … which may be redundant, inconsistent, or overlapping." These are precisely the type of impediments to trade that US companies operating in the fragmented regulatory systems of the EU face today. To combat these barriers, the President called for "[g]reater coordination ... to promote such coordination, simplification, and harmonization."

In previous free trade negotiations, the US secured commitments from trade partners to make significant reforms designed to enhance regulatory coherence in specific sectors. For

example, Korea committed in the context of the US-Korea FTA financial services chapter to "undertake modifications in its regulatory regime" to facilitate greater cross-border transfer of information by financial institutions, and "expressed its intent that these modifications will result in its adoption of approaches that are similar to those of the United States." However, here the US and EU should agree to commitments with respect to data flows that go beyond the hortatory language that the United States has used in previous agreements with respect to data flows, such as Article 15.8 of the US-Korea FTA.

We believe TTIP can and should be deployed to benefit all businesses and consumers in the US and EU by developing specific agreements and standards that would (1) help avoid redundant, inconsistent or overlapping requirements for privacy, data protection and ecommerce, (2) promote regulatory cooperation, and (3) advance coordinated, simplified and better aligned regulation on these issues in both jurisdictions.

There is a particular, compelling opportunity for TTIP to advance US trade interests by lowering EU regulatory barriers: the concept of a "lead" data protection regulator for US companies doing business in the EU would serve this objective. This regulatory reform is congruent with the domestic and international regulatory principles articulated by President Obama – and has already been proposed by the EU in the current draft of the new EU Data Protection Regulation.

We respectfully submit that USTR should support this regulatory discipline through the TTIP process as a specific means of reducing non-tariff barriers to US trade. A meaningful effective lead "supervisory" privacy regulator, or "one-stop-shop" model, for US multinationals doing business throughout the EU, based on the company's main establishment in the EU, would

significantly reduce some of the counter-productive burdens that can arise in the EU today due to the redundant, inconsistent and overlapping regulatory interpretations by different data protection authorities. The DPAs outside the country where a company has its main establishment in the EU will inevitably have less knowledge about and responsibility for the company in question. Promoting better coordination, more simplification and greater harmonization would enhance thus transparency as well as efficiency, and reduce potential discrimination against US entities.

Today, as noted by EU authorities themselves, businesses operating across the EU are impeded by the many varied, sometimes contradictory data protection requirements, due to different national laws, different ways the national data protection authorities apply these laws, and duplicative notification requirements. This leads to legal uncertainty and fragmentation, and makes it difficult for companies, especially innovative start-ups, to do business in the Single Market. The proposed "one-stop-shop," where the "lead" regulator would be charged with the responsibility for investigating and holding US businesses established in the EU accountable for privacy and data protection compliance, would enhance substantive protection while reducing the costs of fragmentation. Other Member State Data Protection Authorities would defer to the "lead" regulator. This would help eliminate unnecessary and counter-productive administrative burdens, as well as the many costs linked to the different reporting requirements that currently exist throughout the EU.

This sensible, efficient approach is particularly valuable, indeed essential, for online and digital commerce for which business models, practices and data flows tend to be inherently less territorial. Therefore, we submit that the US should seek a commitment from the EU that there

can be only one lead national data protection authority for a business with authority to investigate a company's compliance with data protection law. This approach is particularly appropriate for foreign businesses established in the EU because experience and reality indicate that non-local entities are often likely to experience discriminatory treatment. Indeed, a disproportionate number of the leading privacy enforcement actions in the EU have been brought against American companies. ("Diversity" jurisdiction in US litigation is based on this same premise: non-local companies – meaning those that are headquartered in different states or different countries – are protected from discrimination by a broad entitlement to have their cases heard in federal court instead of state courts. 28 U.S.C. 1332.)

The United States should thus actively support principles and disciplines in the TTIP process like this "one-stop-shop" for EU privacy and data protection regulation. If the US obtained a commitment from the EU to adopt this approach, it would promote coordinated, simplified and more consistent regulation to enhance trade and digital commerce. American trade and investment interests would clearly benefit, as would US and EU citizens and consumers. No one wins when rules and regulatory structures are needlessly complex and conflicting.

2. Make the Case for US Privacy "Adequacy" in order to Mitigate Trade Conflicts

The United States data protection regime is likely the oldest privacy scheme in the world. In 1791, the Fourth Amendment, to the US Constitution, as part of the Bill of Rights (building on English legal doctrine), guaranteed the "right of the people to be secure in their … papers, and effects, against unreasonable searches and seizures" by the government. Legal protection of

privacy in civil society has been recognized in the US common law since at least 1890 when the seminal article "The Right to Privacy" was published in the Harvard Law Review (4 Harv. L. Rev. 193) by Professors Samuel D. Warren and (future Supreme Court Justice) Louis D. Brandeis.

The Warren/Brandeis right to privacy, along with the right to be let alone, was followed in 1973 by the first affirmative government undertaking to protect privacy in the computer age. The new philosophy was expressed in "The Secretary's Advisory Committee on Automated Personal Data Systems," published by the US Department of Health, Education, and Welfare (now the Department of Health and Human Services). This HEW Report developed the principles for "fair information practices" that were subsequently adopted by the US in the 1974 Privacy Act, and ultimately, by the European Union in 1995 in its Data Protection Directive. The "fair information practice principles" established in the US in 1973-74 remain largely operative around the world today in regimes and societies that respect information privacy rights of individuals.

With this policy background, the current judgment of the EU that the US does not provide "adequate" privacy protection is not reasonable. The misimpression derives from a failure to appreciate the extensive, pervasive and consequential nature of the US data protection regime. While Europe and countries whose data protection regimes have been deemed "adequate" by EU regulators, have established one comprehensive and omnibus framework law for protecting privacy, it is certainly not clear that this approach provides greater privacy protection in practice (or in theory) than the US model of protecting privacy and information

security through a comprehensive, complementary and well-enforced array of federal and state statutes, and common law theories.

The combined enforcement muscle of the US Federal Trade Commission, Federal Communications Commission, Consumer Financial Protection Bureau (and other financial and banking regulators), the Department of Health and Human Services, Department of Education, fifty-plus state Attorneys General, the relentless US plaintiffs' bar, consumer advocacy groups, and others, constitute an effective check on invasions of privacy and the misuse of personal data.

While the EU Draft Regulation on Data Protection includes draconian potential penalties of 2% of annual, global turnover (or sales revenue) for privacy violations (with few assurances of proportionality and due process), the fact is that to date privacy enforcement outside the US has been relatively minimal.

Indeed, Professor Jeffrey Rosen commented in the Stanford Law Review, in February 2012 (64 Stan. L. Rev. Online 88), that there has long been a dichotomy in Europe between strict laws on paper and loose enforcement in practice. Addressing the dramatic impact that the proposed new 2% annual revenue penalty could have on freedom of expression on the Internet when combined with the new "right to be forgotten," Professor Rosen wrote as follows:

> It's possible, of course, that although the [proposed draft] European regulation defines the right to be forgotten very broadly, it will be applied more narrowly. Europeans have a long tradition of declaring abstract privacy rights in theory that they fail to enforce in practice.

In the US, however, regulatory requirements tend to be enforced as written. Moreover, the so-called *Caremark* standard established for corporate boards of directors impels US companies to establish elaborate internal compliance programs to promote adherence to applicable laws and regulations.[4]

To be sure, regulatory policy is generally thought to be enhanced by taking account of what is reasonable, fair and balanced; what is efficient and cost-effective; what benefits overall consumer welfare; and what promotes consumer protection while preserving economic growth and innovation, and respecting property rights? In other words, competing objectives often need to be reconciled with each other. This cost-benefit perspective will likely be applied to privacy policy in the future as well since President Obama – like his predecessors in the Executive Branch – has expressly embraced this type of analysis for new regulations.

On February 23, 2012, the Obama Administration released an important policy initiative embodied in a white paper setting forth a comprehensive privacy framework – the first ever such framework ever introduced by any presidential administration. The white paper, titled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (the "White Paper"), is the culmination of extensive policy development by the US Commerce Department and Federal Trade Commission. The White Paper also represents a significant US response to the European Union's proposed Regulation to replace the EU Data Protection Directive (95/46/EC). The White Paper should help reestablish US leadership among international privacy policy makers, and perhaps help

[4] *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).

demonstrate that the US framework for data protection is substantively strong and worthy of "mutual recognition" by the EU.

As noted by many knowledgeable parties in the EU, however, the Impact Assessment prepared by the Commission with respect to the draft Regulation is not adequate, and may seriously understate the resulting costs. For example, the government of the United Kingdom stated in its "Government response to Justice Select Committee's opinion on the European Union Data Protection framework proposals" (Jan. 2013),[5] "that while there are benefits from the proposed Regulation, such as a reduction in legal fragmentation, these benefits are outweighed by the costs of additional administrative and compliance measures that the draft Regulation introduces. . . . The Government is seriously concerned about the potential economic impact of the proposed Regulation. At a time when the Eurozone appears to be slipping back into recession, reducing the regulatory burden to secure growth must be the priority for all Member States. It is therefore difficult to justify the extra red-tape and tick box compliance that the proposal represents."

Overall, the new framework adopts a balanced approach to the contentious debate about privacy as a fundamental human right versus privacy as a hindrance to innovation. First, the White Paper expressly affirms the administration's stated commitment to the Internet as an open, decentralized user-driven platform for communication, innovation and economic growth. The White Paper acknowledges the clear benefits to consumers of promoting and preserving

[5] *Available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/162249/response-eu-data-protection-framework-proposals.pdf.pdf.

openness, flexibility and innovation in connection with collecting and using data. Second, while proposing some changes to US privacy law, it essentially confirms that the existing model of US privacy law is working reasonably well both to protect privacy and to promote innovation. And third, it recognizes that the substantive values underlying the US approach to privacy as expressed in the framework itself are substantially equivalent to those expressed by the EU Data Protection Directive and the Asia-Pacific Economic Cooperation ("APEC") Privacy Framework.

The White Paper sets forth four "key elements" to protecting privacy. These elements include: (1) the first ever "Consumer Privacy Bill of Rights" ("CPBR"); (2) development of "appropriate, legally enforceable codes of conduct" through the cooperation of private and public stakeholders; (3) FTC enforcement of the Consumer Privacy Bill of Rights; and (4) "mutual recognition" and "enforcement cooperation" aimed at "global interoperability." Current perceptions of substantive differences have stymied digital trade, ecommerce and international data transfers to the detriment of consumers and businesses between different EU Member States, on both sides of the Atlantic, as well as for multinational businesses. We also believe that technology development and deployment, and innovation has been impeded in the EU itself by EU rules.

Accordingly, the Digital Trade Coalition respectfully submits that TTIP could be a vehicle for the US Administration to make the case to the EU that the US privacy regime is "adequate" relative to the rest of the world. This reasonable outcome would help mitigate perceived conflicts of laws that inhibit the ability of US businesses to engage in ecommerce and

Internet activity in the EU, as well as facilitate cross-border transfers of personal information relating to a company's own employees or customers.

3. Establish a US-EU Privacy and Data Protection Working Group

While the discussion above proposes that the TTIP process should result in recognition of US privacy "adequacy," there are of course substantive, procedural and stylistic differences between the US and EU and various issues important to Internet activity and ecommerce. The Digital Trade Coalition recommends that TTIP include the establishment of a bilateral "US-EU Privacy and Data Protection Working Group" with the specific purpose to identify and reconcile key differences in order to promote interoperability. While the Working Group would not have regulatory authority, it could help develop bilateral interpretations and understandings that avoid conflicts and promote mutual recognition.

For example, the Working Group could address and help ameliorate perceived and actual conflicts regarding jurisdiction over cloud computing, government access to stored communications, international data transfers related to corporate human resources data, legal process or internal investigations, and numerous other areas of current transatlantic tension. The Working Group could also harmonize approaches and standards for data security and data breach notification and help encourage the development of transatlantic codes of conduct for Internet business. Perhaps most importantly, the Working Group could help ensure that US and EU businesses can be assured of obtaining due process and fair treatment in enforcement actions, and that privacy and data protection rules are developed through transparent processes with adequate public and stakeholder involvement, and that such rules are adopted pursuant to reliable regulatory impact assessments.

Another important issue related to transatlantic jurisdiction over privacy is the potentially inordinate extraterritorial jurisdiction contemplated in the proposed EU Data Protection Regulation. It would apply not only to EU businesses established and carrying out business in the EU, but also to those not established in the EU where the processing activities are aimed at the offering of goods and services to individuals in the EU or monitor individuals in the EU. This will mean that a vast number of US businesses, particularly Internet companies, that have no form of establishment in the EU, will become subject to EU data protection requirements and possible EU enforcement including fines of up to 2% of annual, global revenues.

The approach of the EU to the proposed Data Protection Regulation does not adequately consider its expansive extraterritorial effects. European jurisdiction over companies that lack a physical presence in the EU should be exercised more thoughtfully than currently set forth in the draft Regulation, and in a manner consistent with the complex considerations of international comity and mutual recognition. The United States, for example, has long recognized the demands of comity in suits involving foreign states, either as parties or as sovereigns with a coordinate interest in the litigation. See Hilton v. Guyot, 159 US 113 (1895). The Supreme Court in Societe Nationale Industrielle Aerospatiale v. United States District Court, 482 US 522, 544 (1987) and in other cases has required United States regulatory agencies to consider international comity interests.

Of course, in order to promote digital harmony, the US will have to address EU concerns. To that end, the Administration could consider promoting policy initiatives that would protect non-US persons, including EU citizens, under the federal Privacy Act; confirm that non-US persons are entitled to the protections of the Electronic Communications Privacy Act for data

within the jurisdiction of the US; strengthen and expand the mandate of the Privacy and Civil Liberties Oversight Board to cover (a) the interests of non-US persons and (b) governmental cybersecurity activities generally (i.e., beyond impacts related solely to US government efforts to combat terrorism); and, establish a central, federal privacy policy coordinator that could be established as a senior official, perhaps at the Deputy Director level, within the Office of Management and Budget or at the Commerce Department.

* * *

SIDLEY AUSTIN LLP
SIDLEY

In closing, on behalf of the Digital Trade Coalition, we appreciate your consideration of these perspectives and recommendations. We would welcome an opportunity to continue working with the Administration throughout the TTIP process, and would also respectfully request and opportunity to provide testimony at your upcoming hearings.

Sincerely,

Alan Raul

Alan Charles Raul