www.privacyandtrade.org

Comments of the Coalition for Privacy and Free Trade

to the

Trade Policy Staff Committee of the United States Trade Representative

Docket No. USTR-2013-0019

May 9, 2013

The Coalition for Privacy and Free Trade ("Coalition" or "CPFT") represents the views of businesses from an array of industry sectors and welcomes the invitation to provide input on the critical issues to be addressed in the upcoming negotiations for a Transatlantic Trade and Investment Partnership ("TTIP") between the United States and the European Union. As the Coalition explains in this submission, the stability and growth of the transatlantic economy depend upon durable and predictable cross-border data flows and necessary disciplines to safeguard the privacy of personal data contained in the data flows. The resulting expansion in "digital trade" made possible by durable data flows that safeguard personal privacy will benefit both businesses (large and small) and individuals. 1/

The TTIP presents a "once-in-a-generation" opportunity to progress the interoperability of data privacy frameworks in a way that endures. It is thus imperative that this important issue be included in the TTIP negotiations as a priority.

I. Importance of Trusted Cross-Border Personal Data Flows to Trade

The Coalition seeks to safeguard the cross-border personal data flows that have been made possible through technological advances and increased use of the Internet. The ability of data to flow or be accessed across borders, subject to necessary government restraints to safeguard

---

1/ For a comprehensive discussion of the economic value of data to consumers and economic prosperity, and the vital role of cross-border data privacy policy, see M. Mandel, *Beyond Goods and Services: The (Unmeasured) Rise of the Data-Driven Economy*, Progressive Policy Institute Policy Paper (Oct. 2012), *available at* http://www.progressivepolicy.org/wp-content/uploads/2012/10/10.2012-Mandel_Beyond-Goods-and-Services_The-Unmeasured-Rise-of-the-Data-Driven-Economy.pdf.

privacy, is essential to the 6.8 billion people globally and the more than 800 million people in the United States and European Union alone that benefit from the digital economy and digital trade. The TTIP can play an important role in establishing practical mechanisms of interoperability that will have a global influence.

More and more, modern international trade, economic and employment growth, and industrial competitiveness depend on the ability of companies to manage digital trade and cross-border data flows. The role of interconnected information technology in almost every significant economic sector means that international commercial activity of all kinds now involves cross-border data access, sharing, management, and analysis. Unfortunately, businesses often face fragmented, inconsistent, and redundant regulation of cross-border data that unnecessarily complicate their multi-national operations. An examination of how to lessen such impacts is urgently needed. The stakes thus go far beyond the Internet, software, and high-technology sectors; the future competitiveness of the US and European banking, pharmaceutical, life sciences, retail, insurance, health care, automotive, and manufacturing sectors also depends on their future capability to manage cross-border data flows to provide goods and services to customers worldwide.

Of course, digital trade frequently includes personal data. Accordingly, in order to enable the global free flow of information, it is fundamental for governments to strike an appropriate balance between supporting the movement of data across borders while ensuring appropriate respect for data protection and privacy. In contrast, overbroad, unduly restrictive, or isolationist government policies would cripple future US or European economic growth and stymie future job creation at a time when the US and European economies are struggling to recover from a deep recession that has cost millions of jobs.

This is not just an issue for large businesses. Digital trade – and the responsible collection and use of personal data that underlies and enables it – benefits all, including small businesses and individual consumers.

The Obama Administration already has recognized the importance of interoperable privacy frameworks to global economic progress and prosperity:

> Though governments may take different approaches…, it is critical to the continued growth of the digital economy that they strive to create interoperability between privacy regimes…. *The United States is committed to engaging with its international partners to increase interoperability in privacy laws* by pursuing mutual recognition, the development of codes of conduct through multistakeholder processes, and enforcement cooperation. It is also committed to including international counterparts in these multistakeholder processes, to enable global consensus on emerging privacy issues. 2/

Moreover, the US and EU aligned in 2012 to express "a commitment to promoting the rights of individuals to have their personal data protected and to facilitating interoperability of our commercial data privacy regimes." 3/ EU Vice-President Viviane Reding and then-US Secretary of Commerce John Bryson jointly declared:

> The European Union and the United States are global leaders in protecting individual freedoms, including privacy, while at the same time fostering innovation and trade that are so critical to the world economy, notably in the present times. Stronger transatlantic cooperation in the field of data protection will enhance consumer trust and promote the continued growth of the global Internet economy and the evolving digital transatlantic common market. 4/

The Coalition believes that prioritizing cross-border personal data flows in the TTIP, in addition to being consistent with Administration policy and the 2012 joint US-EU declaration, is essential in light of the size, importance, and leadership roles of the United States and European Union. The global competitiveness of the US and EU economies and a wide range of US and European industries depends on whether the TTIP can articulate workable and credible rules to support the future ability of US and European firms to efficiently access and manage cross-border data flows in order to provide goods and services effectively to customers. Economies that enable industries and firms to perform this function will provide opportunities for those organizations to gain a major advantage in the global marketplace; conversely, economies that stifle cross-border

---

2/ The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, at 31 (Feb. 2012) (emphasis added), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

3/ Joint European Statement on Data Protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson (Mar. 19, 2012), *available at* http://www.commerce.gov/news/press-releases/2012/03/19/us-eu-joint-statement-privacy-eu-commission-vice-president-viviane-re.

4/ *Id.*

data flows through unduly restrictive, administratively burdensome, or isolationist policies will experience lower levels of economic growth, employment, and technological innovation. 5/

Consumers and business also must trust that data that transits borders will be protected. At the same time, the US and EU must recognize that multiple types of policy and legal frameworks can interoperate to enable such protection. These predicates have led to the development of several cross-border data privacy mechanisms, including contracts, binding codes of conduct, and the bilateral Privacy Safe Harbor program (negotiated between the United States and the European Commission in 2000). The US-EU Safe Harbor has proven useful to firms seeking to demonstrate compliance with the cross-border privacy elements of EU law by certifying to their adherence with internationally accepted data privacy principles backed by US enforcement. The recently launched APEC Cross-Border Privacy Rules program is another example of an interoperability mechanism based on widely accepted privacy principles (albeit not officially including the European Union). However, none of these mechanisms provides both the breadth and durability necessary to ensure free flows of data.

The international community is working to adapt widely recognized privacy principles such as the *OECD Privacy Guidelines* to the challenges of the global, digital marketplace. 6/ In this context, the TTIP provides the United States and the European Union an opportunity to lead the development of a contemporary, reasonable, and sustainable policy framework for cross-border personal data flows – one that will have influence around the world – while at the same time promoting digital trade.

II. The US Privacy Framework

Achieving interoperability between the US and EU privacy frameworks requires an appreciation of how the two respective systems currently work.

The US privacy framework – like its European counterpart – is premised generally on underlying principles of fairness known as "Fair Information Practice Principles" (or "FIPPs"), which were first developed in the United States in the 1970s and have influenced every privacy law, regulation or code of conduct since adopted. The FIPPs (and the *OECD Privacy Guidelines* that incorporate them) focus on empowering individuals to exercise control over personal information that pertains to them, and on ensuring that measures are taken to achieve adequate data security.

5/ Mandel, *supra* note 1, at 12-13.

6/ More formally known as the *OECD Guidelines on the Protection of Privacy and Transborder Personal Data Flows*, the *OECD Privacy Guidelines* were adopted in 1980. Consistent with and substantially derived from the FIPPs, the *OECD Privacy Guidelines* remain widely recognized and supported. The full text of the *OECD Privacy Guidelines* is *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

The FIPPs generally provide for the following:

1. ***Individual Control:*** Individuals should be able to exercise appropriate control over what personal data organizations collect from them and how they use it.

2. ***Transparency:*** Individuals should have access to easily understandable information about privacy and security practices.

3. ***Respect for Context:*** Individuals should be able to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.

4. ***Security:*** Individuals should be able to expect the secure and responsible handling of personal data.

5. ***Access and Accuracy:*** Individuals should be able to access and correct personal data, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to them if the data are inaccurate.

6. ***Focused Collection:*** Individuals should be able to expect that reasonable limits on the personal data organizations collect and retain.

7. ***Accountability:*** Individuals should be able to expect that personal data will be handled by organizations with appropriate measures in place – such as redress and enforcement – to ensure accountability. 7/

Implementation of the FIPPs in the United States takes into account the right to free expression and the value of commerce, and inherently assumes that not every piece of personal information or set of activities involving personal information should be subject to direct government regulation. Rather, codified law and regulation and targeted enforcement act in the US framework primarily to defend against governmental intrusion, deceptive or unfair practices, and the collection and use of sensitive personal information, including financial, health, and children's data. 8/ Regulation and enforcement at both the federal and state levels, consistent with US federalism, provide layers of accountability for the handling of personal data.

7/ For a side-by-side comparison of several governmental statements of the FIPPs, see *Consumer Data Privacy in a Networked World*, *supra* note 2, at pp. 49-52.

8/ For example: (1) financial privacy laws, including the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley (GLB) Act regulate how credit reporting agencies and financial institutions collect, disclose, share, and protect personally identifiable financial information; (2) the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its recently updated regulations govern the use and disclosure of "protected health information" by such entities as physicians, hospitals, and health

A key feature of the American approach to data privacy is the seriousness with which US firms take their privacy obligations. Privacy and data protection professionals (whether called Chief Privacy Officers (CPOs) or another title), as well as IT security professionals, have become critical and commonplace components of US firms. CPOs ensure that their companies have documented and enforceable compliance and training programs in order to provide physical, administrative, and technical protections for personal data. They also ensure that new products, services, and activities account for privacy considerations. In addition, professional organizations (such as the International Association of Privacy Professionals) facilitate the sharing of accepted best practices, guidelines, and policies for privacy among their membership.

Heightened regulatory and public attention (by the media, privacy advocates, and NGOs) on the appropriate collection and use of personal data, enforceable self-regulatory measures, and codes of conduct created by multi-stakeholder groups complement US privacy laws and play an important role in the US commercial privacy framework. 9/ These additional safeguards are voluntary; however the commitments undertaken by volunteering companies typically are enforceable. For example, thousands of US companies have subjected themselves to Federal Trade Commission (FTC) enforcement oversight by voluntarily posting privacy policy statements on their websites and enrolling in self-regulatory programs sponsored by organizations like the Network Advertising Initiative and the Digital Advertising Alliance. The FTC is authorized under section 5 of the FTC Act to take action against "unfair or deceptive" practices. Relying on this authority, the FTC effectively has created a "common law" of what is expected from business by taking punitive action against companies that have breached their privacy policy commitments with respect to the collection, use, or protection of personal information. 10/

US implementation of the FIPPs is particularly noteworthy for its strong data security focus. Legal and enforcement actions in the United States have to date focused, and rather effectively, on the prevention, remediation, and punishment of data security breaches. An example is the

---

insurers; and (3) the Children's Online Privacy Protection Act of 1998 (COPPA) and its recently updated regulations govern online collection and use of the personally identifiable information of children.

9/ The White House's 2012 Report on Consumer Data Privacy in a Networked World noted the continued importance of such self-regulation, even as it called for the enactment of a Consumer Privacy "Bill of Rights" in the form of baseline privacy legislation applicable to the collection, use and handling of all types of personal data. The Report is *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

10/ A recent speech by FTC Commissioner Julie Brill summarized the Commission's approach to data privacy and the differences and similarities between the US and EU on this topic. *See* J. Brill, Remarks to the Mentor Group, Forum for EU-US Legal-Economic Affairs (April 16, 2013), *available at* http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf.

FTC's enforcement actions against companies that have suffered data breaches. 11/ State notification laws force the disclosure of data-security breaches involving personal data, frequently leading to enforcement actions by regulators and private litigants. 12/ Finally, state attorneys general across the United States have been proactive on their own – and in coordination with the FTC – in bringing enforcement actions against companies for data privacy and security lapses. 13/

These elements described above – targeted statutes; enforceable codes and self-regulation; strong enforcement; an emphasis on data security; and privacy professionalism – combine to create a uniquely American approach to privacy, an approach fundamentally based on the unique legal system here although consistent with the internationally recognized FIPPs. The US approach has demonstrated the ability to adapt to changing individual privacy choices and preferences while addressing the effect of new technologies and data uses.

III. The EU Privacy Framework

As previously noted, the FIPPs also underlie Europe's privacy framework. The keystone of Europe's approach to privacy is the Data Protection Directive. 14/ The Directive was first enacted in 1995 and subsequently transposed into law in each of the EU Member States. In effect, it applies the FIPPs directly via the force of law to nearly all personal data that an organization may collect or process. Among the requirements imposed on organizations that collect and process personal data is a duty to maintain records of such data processing and, depending on the Member State, to register the existence and details of such processing with the appropriate data protection authority.

11/ With the advent of breach notification laws, the FTC developed new targets for enforcement: inadequate information security programs. A number of FTC enforcement actions have resulted in consent decrees requiring comprehensive data security programs that are regularly assessed and reported upon by independent outside auditors.

12/ Forty-six states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have data breach notification laws. The National Conference of State Legislatures maintains a list of these laws at http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx. Data security breach notification also is required under federal health and financial privacy laws, and proposals for an omnibus federal data breach notification law are pending.

13/ The current leadership of the National Association of Attorneys General ("NAAG") has prioritized privacy and helped to coordinate and inform the enforcement and outreach efforts of multiple state attorneys general. See, for example, the agenda of the 2013 Winter/Spring NAAG Conference, *available at* http://www.naag.org/assets/files/pdf/meetings/2013_wint-spr/2013%20Winter-Spring%20Meeting%20Final%20Printed%20Agenda.pdf.

14/ Formally known as Directive 95/45/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT.

A central tenet of Europe's privacy law is that personal data processing that occurs outside of Europe, and was originally under European jurisdiction, must be done in a jurisdiction or in manner that is deemed "adequate." Mechanisms have emerged over the years to help establish the "adequacy" of either individual nations or organizations, including the US-EU Safe Harbor, model contracts, binding corporate rules, and nation-level adequacy determinations. The existence of a national privacy law applicable to every type of personal data collection has to date been a key factor in the EU's view of whether a national scheme can be deemed "adequate" – and a key reason that the United States, with its unique implementation of FIPPs involving sectoral laws complemented by multistakeholder initiatives and multi-layered enforcement – has not been deemed "adequate" by the EU.

Europe has not seen the wide variety of multistakeholder and other private sector privacy initiatives that have emerged in the United States to complement direct regulation. EU-level efforts to coordinate and guide implementation of the Directive include an advisory body of data protection regulators (the "Article 29 Working Group") and the office of the EU Data Protection Supervisor. 15/ There is considerable variation of approach among the 27 Member States at a practical level, however. This is similar to the US federalist system.

Enforcement of European data privacy laws, despite their expansive scope, is significantly less frequent than what occurs in the United States. In addition, the development of a privacy compliance discipline within the private sector has not been as robust as we have seen here. 16/

In January 2012, the European Commission unveiled a new proposal for privacy in the EU, the General Data Protection Regulation (GPDR). Just like the Directive, the proposed GPDR is based on the FIPPs and would apply to nearly all types of personal data. New provisions would impose additional mandates on organizations that collect and process personal data; impose higher penalties for violations; require US-style data security breach notification; and expand the jurisdiction of European privacy law.

IV. The TTIP Can Promote Privacy and Free Trade

The TTIP provides a once-in-a-generation opportunity to progress the interoperability of data privacy frameworks between the US and EU. The Coalition is thus strongly of the view that this important issue should be included in the TTIP negotiations as a top priority.

15/ These bodies regularly meet to discuss and issue opinions on the application of existing European privacy law to new technologies and data uses.

16/ For a detailed study of and comparison between the US and EU approaches to compliance with data privacy obligations, *see* K. Bamberger and D. Mulligan, *Privacy on the Books and on the Ground*, 63 Stanford Law Review (Jan. 2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385.

The Coalition recommends that USTR seek the development of trade disciplines in the TTIP that promote a single, global digital information marketplace and include adherence to enforceable data privacy practices. These disciplines can benefit US and EU businesses and consumers by limiting inconsistent and redundant regulation of cross-border data access, sharing, management, and analysis and by streamlining the business practices of firms operating in both the EU and US. The TTIP should focus primarily on interoperability, *i.e.*, enabling companies from different jurisdictions to share data across borders while providing necessary protections for privacy. In doing so, the TTIP process should recognize, respect, and seek to reconcile fundamental differences between the US and EU privacy frameworks in order to establish international standards for the 21st Century.

Accordingly, the Coalition requests that USTR follow these principles as the TTIP negotiations commence:

- *Support digital trade*. The TTIP should promote a single, global digital information marketplace by liberalizing cross-border data flows.

- *Respect privacy.* Interoperability mechanisms should be available to US and EU organizations.

- *Enhance cross-border enforcement cooperation*. The US and EU should work together to strengthen cross-border enforcement of data privacy laws.

- *Achieve durable agreement that sets global baseline.* Substantive and procedural commitments by both the US and EU should be durable over time to increase regulatory predictability and business certainty.

- *Avoid discriminatory enforcement practices.* US companies should not be held to higher or different standards than those actually enforced against European companies (national treatment) or companies from other countries (most-favored nation treatment).

* * *

The Coalition looks forward to working with USTR on these important issues during the negotiation of the TTIP. We can be contacted at info@privacyandtrade.org and would be pleased to answer any questions.