Trans Atlantic Consumer Dialogue

DOC NO: INFOSOC 50/13 DATE ISSUED: October 2013

Resolution on Data Flows in the TransAtlantic Trade and Investment Partnership

Introduction

The Transatlantic Consumer Dialogue (TACD) strongly urges the Transatlantic Trade and Investment Partnership (TTIP) negotiators to leave data flows out of the trade negotiations. It is impossible to address the issue of data flows when the data protection regimes in the US and EU are starkly different and unbalanced. Without adequate oversight and transparency, any attempts to include data protections in the transatlantic trade negotiations could easily result in a significant weakening of consumer protections with little or no public input.

The TACD strongly believes that information on the Internet should freely flow to ensure freedom of expression and consumer choice. The principles of openness and neutrality are fundamental elements of the Internet's architecture and allow consumers and businesses to share vital information and spur innovation. The TTIP negotiators must strive to remove any restrictions to the free flow of information on the Web.

It is crucial to point out, however, that this free of flow of information that benefits us all should never be confused with the flow of commercially valuable personal information regulated under data protection and privacy frameworks on both sides of the Atlantic. Consumers are subject to increased tracking as they move through their online and offline worlds, and this tracking enables the creation of large personal profiles that can have the potential to undermine individual privacy and security. Today, sensitive personal data is also more likely to be stored in the cloud, exposing consumers to data breaches, unauthorized disclosure, and warrantless government surveillance.

The privacy frameworks recently proposed by the European Commission, the White House, and the Federal Trade Commission seek to enhance consumer protection and fairness. However, despite a common foundation, the privacy regimes from opposite sides of the Atlantic exhibit fundamental differences in approach and substance. The EU is currently undergoing a major revision of the data protection framework, while in the US, the Administration has pledged to implement a Privacy Bill of Rights - what form that will take and how it would compare to data protection rights in the EU are still unclear. A trade agreement cannot resolve the fact that the two systems are highly divergent and non-interoperable, nor should it be used to circumvent the legislative process.

The EU and the US should negotiate common data privacy standards, but do so outside of the proposed TTIP negotiations. It is impossible to address the issue of data flows within the context of trade negotiations when the data protection regimes in the US and EU are starkly different and unbalanced.

TACD Recommendations

The TACD urges the EU and US governments to:

1. Safeguard the right of consumers to send and receive content of their choice and the right to use services and run applications of their choice without any discrimination.
2. Pursue the legislative process to update their respective data protection and privacy frameworks to the 21st century.
3. Seek (for the US) congressional enactment of the Consumer Privacy Bill of Rights, clearly establishing these rights in law. In the absence of legislation, the US cannot offer the EU any assurance that there will be adequate protection for the personal data stored or used by US companies.
4. Ratify (for the US government) the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).
5. The EU should refrain from negotiating substantive privacy rules pending approval of the data protection reform package by the European Parliament and the Member States.
6. Improve cooperation between regulatory authorities to enforce privacy laws in cross-border cases; such co-operation shall include the development of alert systems and information sharing regarding illegal privacy practices.
7. Agree on common data privacy standards outside of the proposed TTIP negotiations. Such standards must meet the requirements of EU laws.
8. Independently assess the effectiveness of the US-EU Safe Harbour Privacy Framework and make necessary changes to ensure that it is adequately harmonized with the provisions in the EU data protection legislation.
9. Ensure that companies cannot evade a jurisdiction's privacy laws merely by transferring personal data to servers located in another jurisdiction.

Background

The privacy frameworks on both sides of the Atlantic are different and hard to reconcile. In the EU general data protection legislation is underpinned by the fundamental Right to Privacy as enshrined in the Charter of Fundamental Rights, as well as the constitutions of several of the member countries. In the US there is no such statutory recognition of privacy as a fundamental right.

Both the EU and US are in the process of formally reviewing their data privacy regimes. In January 2012, the European Commission proposed comprehensive reform of existing consumer data protection laws. A new proposed EU law would regulate how personal data can and cannot be used by companies when consumers shop, email, use social networks, etc. The law would apply to all companies doing business with EU consumers, even if they are located outside the EU territories. A new proposed Directive will apply general data protection principles and rules to the processing of personal data for the purposes of prevention, detection, investigation or prosecution of criminal offences.

While the US has for many years regulated government collection, retention and use of personal information, commercial data collection and use remains largely unregulated except in certain

narrow sectors such as health care providers, schools, video rental shops, and financial institutions. In February 2012, the Obama Administration released a white paper, “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.” The paper features “A Consumer Privacy Bill of Rights” which consists of seven principles: individual control, transparency, respect for the context in which the data is being collected, security, access and accuracy, focused collection (minimization), and accountability. The Administration also has convened multi-stakeholder meetings to develop voluntary industry codes of practice to address specific privacy concerns. To date, the development of a single code of conduct for a single principle (transparency) in a single industry (mobile applications) has taken more than a year due to the divisiveness of stakeholder input. The difficulty in arriving at consensus among stakeholders underscores the need for comprehensive privacy legislation in the US.

The recent revelations regarding US and EU surveillance of digital communications and collection of information from commercial digital data entities have raised serious concerns about the lack of transparency and due process. The actual extent of these data collection practices, whether they were lawful, or the range of activities involving companies such as Google, Facebook, and Yahoo are still unclear. Until the new US and EU joint group of experts tasked with examining privacy in the light of the National Security Agency’s PRISM Internet data program and related disclosures makes a report to the respective governments and the public, it would be unwise for the negotiators to address data and e-commerce-related trade matters at all. The public on both sides of the Atlantic deserves a full and frank discussion of what actually transpired, and what policies or safeguards should be required as a consequence.

Under existing EU data protection rules, companies with operations in Europe are generally prohibited from transferring data about EU residents to US jurisdiction, unless they undertake certain obligations. One way to become exempt from this ban is to be a signatory to the US-EU "Safe Harbor" framework. This prohibition exists because EU regulators do not recognize the US data privacy regime as providing "adequate" protections.

The Safe Harbor framework is a voluntary system based on self-certification under a number of basic principles. Organizations that decide to participate in the US-EU Safe Harbor program must comply with the US-EU Safe Harbor Framework's requirements and publicly declare that they do so. To be assured of Safe Harbor benefits, organizations must self-certify annually to the Department of Commerce in writing that they agree to adhere to the US-EU Safe Harbor Framework's requirements, which include elements such as notice, choice, access, and enforcement. Organizations must also state publicly in their published privacy policies that they adhere to the Safe Harbor Privacy Principles.

More than ten years after these ground rules were established, there are significant problems with the Safe Harbor Framework, mainly with false claims regarding membership and certification, transparency and accessibility of privacy policies, independence of dispute resolution mechanisms and absence of effective enforcement by regulatory authorities. Additional work is necessary to ensure that any Safe Harbor Framework is adequately harmonized with the provisions in the EU data protection legislation.

The TTIP is not the appropriate forum to address data protection rights and it is impossible to treat data flows as a separate issue. Strong data protection regimes should be developed on both sides of the Atlantic through the respective democratic processes in the US and EU.