



Internet Association

The Honorable Michael Burgess
Chairman, Commerce, Manufacturing, and Trade
Subcommittee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Greg Walden
Chairman, Communications & Technology
Subcommittee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member, Commerce, Manufacturing, and
Trade Subcommittee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member, Communications & Technology
Subcommittee
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

November 3, 2015

Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows

Chairmen Burgess and Walden and Ranking Members Schakowsky and Eshoo:

The Internet Association writes to express our views on recent events impacting the U.S./EU Safe Harbor. Cross-border data flows between the U.S. and Europe are the highest in the world and the free movement of data creates jobs and enhances growth on both sides of the Atlantic.¹ It is therefore imperative that data flows between the U.S. and the EU be supported in a way that provides legal certainty and continuity to businesses and consumers alike.

The Internet Association is the unified voice of the Internet economy, representing the interests of leading Internet companies² and their global community of users. The Internet Association is dedicated to advancing public policy solutions to strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. Important to our mission is the advancement of public policies that support the free flow of data globally. Until recently, the U.S./EU Safe Harbor framework served this policy goal effectively. Over 4,400 US companies relied on Safe Harbor to validate the transfer of data from the EU to the U.S., including both U.S. headquartered companies and U.S. based subsidiaries of EU headquartered companies. Over half of these companies are small and medium sized enterprises.

¹ Joshua Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, Global Economy and Development at Brookings Research Paper (Oct., 2014), <http://www.brookings.edu/research/papers/2014/10/internet-transatlantic-data-flows-meltzer>.

² The Internet Association's members include Airbnb, Amazon, auction.com, Coinbase, Dropbox, eBay, Etsy, Expedia, Facebook, FanDuel, Gilt, Google, Groupon, Handy, IAC, Intuit, LinkedIn, Lyft, Monster Worldwide, Netflix, Pandora, PayPal, Pinterest, Practice Fusion, Rackspace, reddit, Salesforce.com, Sidecar, Snapchat, SurveyMonkey, TripAdvisor, Twitter, Yahoo, Yelp, Uber, Zenefits, and Zynga.



Internet Association

Like the thousands of U.S. and EU companies who complied with the Safe Harbor in good faith, our members were disappointed when the European Court of Justice recently invalidated the Safe Harbor effective immediately. While the Internet Association respects that ECJ opinion in the Schrems case as binding and final in nature, we think it important to flag two issues with the court's analysis of U.S. law since they should be factored into the ongoing negotiations between the EU and the U.S. around the renewed Safe Harbor framework. These two issues are the court's analysis of U.S. surveillance law as well as its treatment of U.S. commercial privacy law.

First, the ECJ Schrems opinion is premised on inaccurate assumptions about U.S. surveillance law that do not capture the significant surveillance reforms undertaken by the U.S. government since 2013. The Internet Association and its members have consistently supported these reform measures, which should inform negotiations to revitalize the Safe Harbor.

In the aftermath of the Snowden revelations, President Obama's Review Group on Intelligence Communications and Technology drafted a comprehensive report with a set of 46 recommendations concerning reforms to U.S. surveillance programs, laws, and intelligence agencies. Some of these recommendations formed the basis for subsequent legislation while others continue to inform the debate about broader surveillance reform measures. Separately, the Privacy and Civil Liberties and Oversight Board (PCLOB) published comprehensive reports with concomitant recommendations related to key sections of the Foreign Intelligence Surveillance Act (FISA) and the PCLOB is currently undertaking a review of Executive Order 12333.

In June this year, President Obama signed the USA Freedom Act into law. The USA Freedom Act prohibits the bulk collection of telephony and Internet metadata under various U.S. legal authorities, allows companies to publish transparency reports with further granularity around the volume and scope of national security demands issued by governmental entities, and codifies new oversight and accountability mechanisms.

The USA Freedom Act was preceded by Presidential Policy Directive PPD-28. PPD-28 provides that signals intelligence collected about non-U.S. persons may no longer be disseminated solely on the basis that the information pertains to a non-U.S. person. To the extent that signals intelligence is collected about non-U.S. persons in bulk, it must be for one of six specified purposes³ and no others.

More recently, on October 20, 2015, the House of Representatives passed the Judicial Redress Act (H.R. 1428) by a voice vote. This legislation, if enacted by the Senate, would ultimately enable non-U.S. persons to enjoy judicial redress rights given to U.S. citizens under the Privacy Act of 1974.

Unfortunately, none of these significant changes to U.S. surveillance law and oversight were analyzed by the ECJ in its recent Safe Harbor opinion. Moreover, these undertakings by the U.S. government

³ These purposes are counter-espionage, counterterrorism, counter-proliferation, cybersecurity, detecting and countering threats against U.S. armed forces or allied personnel, and to combat transnational criminal threats.



stand in stark contrast to the ECJ's view that the U.S. engages in "indiscriminate surveillance and interception carried out [] on a large scale."⁴

Separate and apart from surveillance reforms, the ECJ Safe Harbor opinion did not acknowledge today's layered and effective U.S. commercial privacy enforcement regime. Since the late 1990s, the Federal Trade Commission has enforced its broad authority under Section 5 of its enabling statute almost 100 times against data privacy and security violations that constitute "unfair or deceptive acts or practices in or affecting commerce."⁵ Beyond this broad FTC jurisdiction, Congress has enacted several sector specific statutes protecting children's, financial, and healthcare information. And beyond Congress, the states have enacted over 300 privacy laws controlling a diverse array of privacy and data security issues - from data breach to employer access to their employees' social media accounts.

The U.S. Department of Commerce and European Commission have spent nearly two years negotiating a renewed Safe Harbor agreement to address the Commission's concerns regarding the protection of EU citizens' privacy. The revised framework will strengthen protections for EU citizens' data while facilitating transatlantic data flows that bring significant benefits to the U.S. economy and the EU economy alike.

It is important to the Internet Association that the ongoing Safe Harbor negotiations between the U.S. and the EU are premised on a fair and current understanding of U.S. law. In its Safe Harbor opinion, the ECJ laid out the standard for "adequacy" that would allow for continuing data flows between the EU and the U.S. and we are confident the U.S. regime, when fairly examined, would satisfy this standard. We therefore urge the Department of Commerce and the European Commission to take into consideration the current state of *both* U.S. surveillance law and commercial privacy law in finding the common ground needed to reach agreement on a new Safe Harbor framework.

We urge the Department of Commerce to conclude the ongoing Safe Harbor negotiations as soon as possible and, in conjunction with the European Commission, announce the revised framework. The announcement of this framework will represent an important step in providing businesses with certainty and stability in their transfer of data across the Atlantic, and will reassure European citizens that their personal data will continue to be afforded the highest level of protection when it is transferred to the United States.

Respectfully submitted,

Michael Beckerman
President & CEO
The Internet Association

⁴ Schrems v. Data Protection Comm'r, Case C-362/14 (October 6, 2015).

⁵ 15 USC §45(a).