

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE

Proposed Transatlantic Trade and Investment Partnership Agreement

“Docket No. USTR–2013–0019”

May 10, 2013

By notice published on April 1, 2013 the Office of the United States Trade Representative (“USTR”) has requested comment on the Administration’s intention to enter into negotiations for a Transatlantic Trade and Investment Partnership (“TTIP”) agreement with the European Union.¹ Pursuant to this notice, the Electronic Privacy Information Center (“EPIC”) submits these comments and recommendations. EPIC believes that trade agreements are not the appropriate mechanism for determining international privacy standards, and thus the TTIP should exclude privacy and data protection entirely. To the extent that TTIP provisions impact cross-border data flows, they should allow governments to provide exceptions or limitations that strengthen the protection of their citizens’ privacy. Finally, draft texts should be made publicly available, and a mechanism should be created to ensure equal participation by consumer groups, privacy groups, and other members of civil society.

EPIC is a public interest research center located in Washington, D.C., that focuses on emerging privacy and civil liberties issues. EPIC has a strong interest in consumer

¹ Request for Comments Concerning Proposed Transatlantic Trade and Investment Agreement, 78 Fed. Reg. 19,566 (Apr. 1, 2013), *available at* <http://www.gpo.gov/fdsys/pkg/FR-2013-04-01/pdf/2013-07430.pdf>.

privacy,² and has written in support of the Administration’s Consumer Privacy Bill of Rights.³ EPIC has also written to public officials in both the United States and the European Union in support of the European Data Protection Regulation.⁴ It is EPIC’s view that the EU privacy initiative is a natural evolution of modern privacy law and creates a “ratcheting up” effect that is favorable to consumers in the United States and around the world.⁵

The USTR’s Federal Register notice follows a March 20, 2013 letter⁶ to Congress and the Final Report of the U.S.-EU High Level Working Group (“HLWG”) on Jobs and Growth.⁷ The letter and HLWG Report indicate that the Administration intends to

² See, e.g., Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm’r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., *FTC* File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, *FTC* File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., *FTC* File No. 052-3069 (2004) (Request for Investigation and for Other Relief), <http://epic.org/privacy/choicepoint/fcraltr12.16.04.html>.

³ EPIC, Comments of the Elec. Privacy Info. Ctr. to Nat’l Telecomm. Info. Admin, Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, RIN 0660-XA27, Docket No. 120214135-2135-01, Apr. 2, 2012, *available at* <https://epic.org/apa/comments/EPIC-NTIA-Comments-FINAL.pdf>.

⁴ Testimony and Statement of Marc Rotenberg, President, EPIC, before the Comm. of the Eur. Parl. on Civil Liberties, Justice, and Home Affairs, Eur. Parl., Oct. 10, 2012, *available at* https://epic.org/privacy/Rotenberg_EP_Testimony_10_10_12.pdf; Letter from Julian Knott, TACD Head of Secretariat to the Hon. Mary Bono Mack, Chair, S.Comm. on Commerce, Mfg. and Trade and Hon. G.K. Butterfield, Ranking Member, S.Comm. on Commerce, Mfg. and Trade (Sept. 14, 2011), *available at* http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=329&Itemid=40; Letter from U.S. Consumer Organizations on EU Gen. Data Prot. Regulation to Jan Philipp Albrecht, Rapporteur, Comm. on Civil Liberties, Justice and Home Affairs, and Lara Comi, Rapporteur, Comm. on Internal Mkt. and Consumer Prot., European Parliament (Sept. 5, 2012), *available at* <https://epic.org/privacy/intl/US-Cons-Grps-Support-EU-Priv-Law.pdf>; Letter from U.S. NGOs to the Hon. Eric Holder, U.S. Attn. Gen., Hon. John Kerry, Sec’y of State, Rebecca Blank, Acting Sec’y of Commerce, Ambassador Ron Kirk, U.S. Trade Representative, Ambassador William Kennard, U.S. Mission to E.U. (Feb. 4, 2013), *available at* <https://epic.org/privacy/intl/NGOs-to-US-Gov-re-EU-US-Privacy.pdf>.

⁵ Marc Rotenberg and David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, 36 Harv. J.L. & Pub. Pol’y 605 (2013).

⁶ Letter from Ambassador Demetrios Marantis, Acting U.S. Trade Rep to the Hon. John Boehner, Speaker, U.S. House of Representatives (Mar. 20, 2013), *available at* <http://www.ustr.gov/sites/default/files/03202013%20TTIP%20Notification%20Letter.PDF>.

⁷ Press Release, USTR, Final Report High Level Working Group on Jobs and Growth (Feb. 11, 2013), *available at* <http://www.ustr.gov/about-us/press-office/reports-and-publications/2013/final-report-us-eu-hlwg>.

negotiate a broad agreement that covers a range of trade and investment issues. Although neither the Report nor the March letter explicitly discuss privacy or data protection, they mention issues that might nevertheless impact data protection. For example, the Report discusses “reducing costs stemming from regulatory differences in specific sectors, including consideration of approaches relating to regulatory harmonization, equivalence, or mutual recognition, where appropriate,”⁸ and the letter lists the goal of “[s]eek[ing] to include provisions that facilitate the movement of cross-border data flows.”⁹

I. The U.S. Has Made Some Progress in Recent Years on Privacy Issues

Both the U.S. and EU have undertaken and promoted data protection independently and collaboratively. With the Privacy Act of 1974, the U.S. laid the foundation for strong privacy protection in the modern era. Moreover, the U.S. has recently underscored its commitment to consumer privacy with the Consumer Privacy Bill of Rights. Set out early in 2012 by the Department of Commerce, the Consumer Privacy Bill of Rights (“CPBR”), if enacted into law, would provide substantive privacy protections for users.¹⁰ Likewise, the EU has taken great strides to promote and protect individual privacy. And through collaborative efforts such as the Madrid Declaration, NGOs, privacy experts, and advocates in both the U.S. and the EU have committed to promoting international standards for privacy protection.¹¹ The TTIP, therefore, should not disturb or distract from U.S. and EU data protection progress currently underway.

⁸ *Id.*

⁹ Letter from Ambassador Marantis, *supra* note 5, at 4.

¹⁰ See EXEC. OFFICE OF THE PRESIDENT, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012) [Hereinafter “CPRB Report”], available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

¹¹ The Public Voice, “The Madrid Privacy Declaration,” <http://thepublicvoice.org/madrid-declaration/>

In 1980, the Organization for Economic Co-operation and Development (“OECD”) released its Privacy Guidelines, widely regarded as among the most influential privacy frameworks in the world.¹² The OECD Privacy Guidelines promote eight privacy principles: data collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability.¹³ The United States was among the countries that supported the creation of the OECD Privacy Guidelines.

The U.S. has recently affirmed its commitment to these foundational privacy principles. Last year, the Obama Administration released Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy.¹⁴ The report contains the Consumer Privacy Bill of Rights (CPBR), which outlines the following principles: individual control; transparency; respect for context; security; access and accuracy; focused collection; and accountability. The CPBR principles mirror the OECD guidelines.

In addition to the CBPR, the Administration’s report discusses several high-profile privacy issues, including online advertising, data brokers, and children’s privacy. The report encourages online advertising companies to “refrain from collecting, using, or disclosing personal data that may be used to make decisions regarding employment,

¹² OECD, *Thirty Years After the OECD Privacy Guidelines* (2011).

¹³ Organisation for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm> (last visited May 9, 2013).

¹⁴ White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*, Feb. 23, 2012, <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>. [hereinafter CPBR].

credit, and insurance eligibility” and cites a “Do Not Track” mechanism as an example of a beneficial privacy-enhancing technology.¹⁵

President Obama expressed his support for adoption of the principles articulated in the CPBR.¹⁶ He stated:

My Administration will work to advance these principles and work with Congress to put them into law. With this Consumer Privacy Bill of Rights, we offer to the world a dynamic model of how to offer strong privacy protection and enable ongoing innovation in new information technologies.

In the year since the CPBR’s publication, following the President’s statement, many executive agencies, including the Department of Commerce and the Department of State, have expressed their support for the CPBR and their intention to advocate for its adoption in international cooperative environments, such as the Working Party on Information Security and Privacy.¹⁷ Cameron Kerry, Commerce Department general counsel, applauded the CPBR for its “baseline privacy protections for those areas not covered today by sectoral regimes.”¹⁸

Moreover, Secretary of State John Kerry has repeatedly stated his support for new laws to protect privacy. Just two years ago, then Senator Kerry and Senator McCain introduced the Commercial Privacy Bill of Rights Act of 2011, which would impose new rules on companies that gather personal data, including offering people access to data about them, or the ability to block the information from being used or distributed.

¹⁵ CPBR. at 12.

¹⁶ CPBR Report, Introduction.

¹⁷ FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 3 (2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

¹⁸ Natasha Singer, *An American Quilt of Privacy Laws, Incomplete*, NY TIMES (March 30, 2013), http://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html?pagewanted=all&_r=0.

Companies would have to seek permission before collecting and sharing sensitive religious, medical and financial data with outside entities.¹⁹

At the bill's introduction, Senator Kerry stated:

John [McCain] and I start with a bedrock belief that protecting Americans' personal, private information is vital to making the Information Age everything it should be. Americans have a right to decide how their information is collected, used, and distributed and businesses deserve the certainty that comes with clear guidelines. Our bill makes fair information practices the rules of the road, gives Americans the assurance that their personal information is secure, and allows our information driven economy to continue to thrive in today's global market.²⁰

In 2012, the European Commission proposed the “EU General Data Protection Regulation,” (“GDPR”) which has gained support from numerous U.S. consumer organizations. U.S. groups support the Regulation because it “establishes single, national data protection authorities in each [EU] member state,” “adopts several innovative approaches to privacy protection, such as privacy by design and privacy by default,” and “builds on the right to data deletion.”²¹

And collaboratively, privacy stakeholders in both the U.S. and EU support the Madrid Declaration. Issued in November 2009, the Madrid Declaration is an international “commitment to privacy protection” that “reaffirms international instruments for privacy

¹⁹ Julia Angwin, *Senators Offer Privacy Bill to Protect Personal Data*, THE WALL STREET JOURNAL, (Apr. 13, 2011), *available at*

<http://online.wsj.com/article/SB10001424052748703385404576258942268540486.html>.

²⁰ Press Release, Senator John McCain, Kerry, McCain Introduce Commercial Privacy Bill of Rights: Bi-Partisan Legislation Would Enhance Protection and Control of Personal Information (April 12, 2011), *available at*

http://www.mccain.senate.gov/public/index.cfm?FuseAction=PressOffice.PressReleases&ContentRecord_id=4a92a6f4-daf7-2f4a-84e7-3eb83276af23&Region_id=&Issue_id.

²¹ Letter from U.S. Consumer Organizations on EU General Data Protection Regulation to Jan Philipp Albrecht, Rapporteur, Comm. on Civil Liberties, Justice and Home Affairs, and Lara Comi, Rapporteur, Comm. on Internal Market and Consumer Protection, European Parliament (Sept. 5, 2012), *available at* <https://epic.org/privacy/intl/US-Cons-Grps-Support-EU-Priv-Law.pdf>.

protection, identifies new challenges, and call[s] for concrete actions.”²² Formally endorsed by hundreds of domestic and international civil society groups, privacy experts, and individuals, the Declaration promotes ten propositions concerning data protection.²³ For example, it reaffirms support for Fair Information Practice global implementation, genuine Privacy Enhancing techniques and Privacy Impact Assessments, and “independent data protection authorities.”²⁴ It calls for a moratorium on mass surveillance technology, including body scanners, facial recognition, and RFID tracking, “subject to a full and transparent evaluation by independent authorities and democratic debate.”²⁵ And it urges countries to ratify Article 108 “as expeditiously as possible.”²⁶

II. The TTIP Negotiations Should Exclude Privacy and Data Protection

Even though the United States has made some progress on the privacy front, EPIC believes that the TTIP should not attempt to create transnational privacy rules. A trade agreement is not the right venue for addressing international privacy protections. Trying to resolve privacy in the TTIP will hold up the negotiations, so that ultimately, either the TTIP or international privacy standards will suffer. In a study conducted by the Bertelsmann Foundation, a privately operated non-profit research group based in Germany, and the Atlantic Council, a Washington, D.C.-based international affairs think tank, 120 trade policy experts answered questions about their expectations for the TTIP negotiations.²⁷ The survey gauged the participants’ views on seventeen “specific sectoral

²² Madrid Privacy Declaration: Global Privacy Standards for a Global World, The Public Voice (Nov. 3, 2009), *available at* <http://thepublicvoice.org/madrid-declaration/>.

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ Bertelsmann Foundation and Atlantic Council, *The Transatlantic Trade and Investment Partnership: Ambitious but Achievable: A Stakeholder Survey and Three Scenarios*, April 2013, *available at* http://www.bfna.org/sites/default/files/TTIPReport2_FINAL%20%282%29.pdf.

and horizontal issues,” one of which was “significant alignment in regulations addressing data protection and privacy.”²⁸ When asked to rank the seventeen issues “by degree of importance to the successful negotiation of an overall agreement,” the respondents ranked alignment of data protection and privacy regulations as the sixth most important issue. However, the participants also ranked data protection and privacy alignment as the third most difficult issue to resolve in the context of an overall agreement. The researchers noted that due to the significance and degree of difficulty attached to the alignment of privacy policies, that issue “has the potential to derail negotiations if not handled effectively.”²⁹ As a result, the study concluded that an effective TTIP negotiation would “avoid the most contentious and longest-standing points of divergence.” The study explains that for the TTIP negotiations to be successful, “even if the two sides cannot agree in all areas, they should not let these minor differences curtail the entire deal in the name of comprehensiveness.”³⁰ In other words, those issues like data privacy, which are very important and very difficult to resolve in a trade agreement context, should not be forced into the agreement.

This principle has been recognized in trade agreements for the past twenty years—most notably in the Article XIV exceptions to the GATS. The General Agreement on Trade in Services, or the “GATS,” is a World Trade Organization treaty that became effective contemporaneously with the creation of the WTO. The goal of the WTO generally is to remove barriers to trade, and to liberalize the international market

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

economy.³¹ The GATS specifically focuses on the service sector of international trade – that is, manufacturing, agriculture, fishing, mining, and, increasingly, information services. Cognizant of the conflicts that can arise when different countries attempt to harmonize their civil liberties policies, the WTO deliberately excluded any data privacy compliance rules from the GATS. Instead, the GATS specifically carves out an exception that overrides any other conflicting part of the Agreement.³² The exception reads: “nothing in this agreement shall be construed to prevent the adoption or enforcement by any Member of measures... necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to... the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.” In other words, the GATS is structured around the understanding that signatory countries might have conflicting approaches to protecting individual data privacy. Rather than trying to force each of these approaches into a single privacy rule within the framework of a trade agreement, the WTO created an agreement that was adaptable to individual privacy regimes. This trend toward excluding privacy from the language of trade agreements finds extensive support in the current discussions about TTIP. The Transatlantic Consumer Dialogue, or TACD, an independent network of EU and U.S. consumer organizations which puts forward joint policy recommendations to the U.S. Government and the European Commission, recently expressed its support for excluding the regulation of privacy rights in a letter to the U.S. Trade Representative and

³¹ World Trade Organisation: What is the WTO? (last accessed May 9, 2013) *available at* http://www.wto.org/english/thewto_e/whatis_e/whatis_e.htm.

³² World Trade Organisation: General Agreement on Trade and Services (last accessed May 9, 2013) *available at* http://www.wto.org/english/res_e/booksp_e/analytic_index_e/gats_02_e.htm.

a Commissioner of the European Union.³³ The letter stated,

Privacy Rights: Measures related to personal information and privacy should ensure the highest level of data protection for both EU and US consumers, and permit nations to establish more robust privacy-enhancing measures that include new and evolving digital technologies. Comprehensive legislative data protection reforms are ongoing in the EU, and more privacy-friendly mechanisms are being developed in the US, therefore data flows and data protection must not be included in free trade negotiations.

Similarly, Public Citizen responded to the proposed inclusion of “regulatory convergence” provisions in TAFTA, a proposed U.S.-EU Trade agreement. In a statement prepared for TAFTA stakeholder session, Public Citizen asserted that “advancement of consumer well-being must be the primary goal of any U.S.-EU pact.”³⁴ Public Citizen explained: “It is not apparent that any efficiency gains resulting from regulatory convergence would ... outweigh consumers’ loss of ability to set and modify, through democratic processes.” The letter urged, “Before adopting a regulatory convergence approach in TAFTA negotiations, the United States and EU should establish a transparent process to study and provide answers to these critical questions, inviting early and consistent input from a diverse array of consumer groups and other stakeholders.”³⁵

Consistent with the principle of exclusion illustrated in the GATS, and supported by international consumer and privacy groups, EPIC recommends that TTIP avoid an attempt at regulatory convergence of U.S. and European privacy policies. However, EPIC supports strong international privacy protection frameworks and urges the USTR to allow the Department of Commerce and the Department of State to move forward in this area.

EPIC strongly supports the Council of Europe Convention 108, and has launched a campaign urging the U.S. Government to support the Council of Europe Privacy

³³ Letter from TACD to Ambassador Kirk and Commissioner De Gucht, Mar. 5, 2013, *available at* http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=353&Itemid=40.

³⁴ Comments of Public Citizen, Apr. 10, 2013, *available at* <http://www.citizen.org/documents/public-citizen-TAFTA-comments-reg-coop-forum.pdf>.

³⁵ *Id.*

Convention.³⁶ EPIC renews that recommendation now.

The Council of Europe Convention 108 is an agreement, signed by the member states of the Council of Europe in 1995, which “protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data.”³⁷ Convention 108 imposes certain rules regarding the methods by which signatory countries must regulate personal data collection and retention, and also forbids processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also “enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.”³⁸ As of 2010, Convention 108 had been ratified by 41 European countries, and was under consideration for ratification by three European and non-European countries.³⁹ The Convention still remains the only binding international legal instrument with a worldwide scope of application in the field of data privacy, open to any country, including countries which are not Members of the Council of Europe.⁴⁰

While Convention 108 itself originated in the Council of Europe, the United States' demonstrated interest in the privacy principles protected by the Convention align perfectly. The principles underlying Convention 108 are directly based on the Universal

³⁶ EPIC: Council of Europe Privacy Convention (last accessed May 9, 2013), *available at* <http://epic.org/privacy/intl/coeconvention>.

³⁷ Council of Europe: Treaty Office: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (last accessed May 9, 2013), *available at* <http://conventions.coe.int/Treaty/en/Summaries/Html/108.htm>

³⁸ *Id.*

³⁹ Council of Europe: Treaty Office: Member States of the Council of Europe (last accessed May 9, 2013), *available at* <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=12%20&DF=25/01/2010&CL=ENG>

⁴⁰ *See supra* note 35.

Declaration of Human Rights, adopted by the United Nations in 1948.⁴¹ It was the United States and Eleanor Roosevelt that helped craft the Universal Declaration, and it was the United States that ratified the Council of Europe Convention on Cybercrime and urged its allies to do the same.

Moreover, many civil society and civil liberties groups have expressed support for the U.S. ratification of Convention 108. On January 28, 2010, twenty-nine members of the EPIC Advisory Board wrote to then Secretary of State Hillary Rodham Clinton to urge that the United States begin the process of ratification of Council of Europe Convention 108.⁴² In that letter, EPIC explained, “Just as communications networks can be used for good and ill, so too can computer technology. It can help sustain aid programs, spur innovation, and encourage economic growth. Or it can track the activities of dissidents, monitor the private lives of citizens, and maintain elaborate systems of identification for laborers and immigrants... the protection of privacy is a fundamental human right. In the 21st century, it may become one of the most critical human rights of all. Civil society organizations from around the world have recently asked that countries which have not yet ratified the Council of Europe Convention 108 and the Protocol of 2001 to do so as expeditiously as possible.”⁴³ The next day, the U.S. Privacy Coalition, comprised of twelve privacy groups, including EPIC, also signed a resolution to the U.S. Senate endorsing Convention 108.⁴⁴ On January 25, we reiterated that recommendation to

⁴¹ Letter from EPIC Advisory Board to Secretary Clinton, January 28, 2010, available at http://epic.org/privacy/intl/EPIC_Clinton_ltr_1-10.pdf.

⁴² *Id.*

⁴³ *Id.*

⁴⁴ Privacy Coalition, Resolution, United States Senate, Jan. 29, 2009 *available at* http://privacycoalition.org/resolution-privacy_day.pdf.

the Department of Commerce during its “comprehensive review of the nexus between privacy policy and innovation in the Internet economy.”⁴⁵

By establishing an independent, comprehensive privacy protection framework that is not tied to the terms of an international trade agreement, the U.S. can encourage business and technological innovation. Viviane Reding, the European Commissioner for Justice, Fundamental Rights, and Citizenship has addressed the contention that a strong European privacy rule would restrict international trade by pointing out that, for the purposes of trade, the most valuable data privacy policy is one that is stable and reliable. She addressed the NY Times:

Another important issue that our proposed [privacy] rules address and which matters for countries outside Europe is the issue of international data transfers. The new E.U. data protection rules will improve the current system of binding corporate rules to make these types of exchanges less burdensome and more secure. And under the new legislation the adequacy procedure will better specify the criteria and requirements for assessing the level of data protection in a third country or an international organization. Rules which recognize the adequacy of data protection standards make life easier for businesses by providing legal certainty in their international operations. There are benefits for the economy and trade.⁴⁶

EPIC agrees with Reding's analysis that strong, stable data privacy rules actually strengthen a country's ability to trade internationally and to innovate online. In EPIC's January 2011 letter to the Commerce Department, EPIC noted, “without privacy technology such as public key encryption, there would simply be no commercial Internet. It would not be possible to conduct commerce without HTTPS, to take payments, or to transfer credit card numbers. Public key encryption is a significant example of a privacy-

⁴⁵ Comments of EPIC to the Department of Commerce, “Information Privacy and Innovation in the Internet Economy,” Jan. 25, 2011, *available at*

http://epic.org/privacy/internet/EPIC_Comments_DOC_Internet_Privacy_Report.pdf/

⁴⁶ Natasha Singer, “Q. and A. with Viviane Reding,” *The New York Times*, Feb. 2, 2013, *available at* http://www.nytimes.com/2013/02/03/business/q-and-a-with-viviane-reding.html?_r=0

enhancing technique that allowed businesses to innovate in a myriad of ways that would have been unthinkable without the encryption system.”⁴⁷ EPIC also pointed out that privacy protection promotes trust and confidence in the deployment of new services. In the absence of clear privacy safeguards, public protest and consumer backlash becomes the norm. Furthermore, privacy regulation can promote the development of privacy solutions that help safeguard consumers and promote innovation. As consumers place more value on privacy, companies compete over privacy, which leads to innovation.⁴⁸ Strong data protection rules promote trust in commercial exchanges and encourage online and international interactivity and innovation. And once those rules are established, as Commissioner Reding has pointed out, it makes “life easier for businesses” to rely upon that “legal stability.”⁴⁹

III. Any Provisions on Cross-Border Data Flows Should Ensure High Levels of Privacy Protection for Consumers

Although the TTIP should exclude privacy and data protection at the outset, several provisions of the agreement might nevertheless impact privacy. For example, the Report discusses “reducing costs stemming from regulatory differences in specific sectors, including consideration of approaches relating to regulatory harmonization, equivalence, or mutual recognition, where appropriate,”⁵⁰ and the letter lists the goal of

⁴⁷ *Supra* note 44.

⁴⁸ *Id.*

⁴⁹ Reding, *supra* note 45.

⁵⁰ UNITED STATES OFFICE OF TRADE REPRESENTATIVE, FINAL REPORT OF HIGH LEVEL WORKING GROUP ON JOBS AND GROWTH 2013, *available at* <http://www.ustr.gov/about-us/press-office/reports-and-publications/2013/final-report-us-eu-hlwg>.

“[s]eek[ing] to include provisions that facilitate the movement of cross-border data flows.”⁵¹

Any provision that impacts privacy must ensure a high level of data protection for consumers. In particular, the USTR should avoid allowing TTIP to become a vehicle for weakening stronger European privacy laws, such as the proposed Data Protection Regulation.⁵² The proposed Regulation is currently more protective than U.S. law, and because of this it has been targeted by members of the U.S. business community, which has lobbied furiously to weaken the law.⁵³ Previous trade agreements have contained provisions that threatened the privacy and consumer protections of participating countries. For example, ACTA undermined privacy laws by “depriving countries of the freedom to adopt laws protecting the rights to privacy and personal data protection, and by requiring the implementation of measures that will negatively affect those rights.”⁵⁴ Thus, any provisions on cross-border data flows that impact privacy should clearly set a floor that allows governments to create stronger standards in response to the demands of their citizens, rather than a ceiling that limits responsiveness and suppresses more protective standards. Governments must retain the power to provide exceptions or limitations that strengthen the protection of their citizens’ privacy.

⁵¹ Letter from Demetrios Marantis, Acting United States Trade Representative, to John Boehner, Speaker, United States House of Representatives, Mar. 20, 2013, <http://www.ustr.gov/sites/default/files/03202013%20TTIP%20Notification%20Letter.PDF>

⁵² Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), available at http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf.

⁵³ See Jennifer Baker, *EU data protection bill threatens citizens' rights, warns civil rights coalition*, INFO WORLD (Apr. 25, 2013), <https://www.infoworld.com/t/federal-regulations/eu-data-protection-bill-threatens-citizens-rights-warns-civil-rights-coalition-217310>; Liat Clark, *MEPs copied US lobbyists' Data Protection Regulation amendments verbatim*, WIRED UK (Feb. 14, 2013), <http://www.wired.co.uk/news/archive/2013-02/14/lobbyplag-eu-plagiarises-us-lobbyists>

⁵⁴ Alberto J. Cerda Silva, *Enforcing Intellectual Property Rights by Diminishing Privacy: How the Anti-Counterfeiting Trade Agreement Jeopardizes the Right to Privacy*, 26 AM. U. INT'L L. REV. 601, 616 (2011).

Many U.S. consumers favor greater privacy protection, with public opinion polls consistently showing that users value privacy and take steps to enhance the security of their information.⁵⁵ And recently, twenty-two U.S. consumer, privacy, and civil liberties groups wrote to the European Parliament in support of the Regulation.⁵⁶ The groups wrote that the Regulation “provides important new protections for the privacy and security of consumers” and will “benefit consumers around the globe, as businesses improve their privacy practices and security standards.”⁵⁷ Ensuring that any provisions related to data protection provide a floor, not a ceiling, would leave the European Union free to continue the development of its privacy laws.

IV. The Negotiations Should Emphasize Transparency and Provide for Regular Civil Society Involvement

Finally, EPIC recommends that all drafts of negotiating texts and all country submissions be made publicly available. Any U.S.-EU free trade agreement will impact millions of consumers on both sides of the Atlantic, and these individuals should be able to meaningfully participate in the negotiation process. Access to negotiating documents is a necessary condition for meaningful public participation. Previous trade negotiating documents have been kept secret, with corresponding losses in legitimacy and the opportunity for meaningful public input. For example, the secrecy surrounding the Anti-

⁵⁵ See Jan Lauren Boyles et al., Privacy and Data Management on Mobile Devices Pew Internet & American Life Project (2012), http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx?utm_source=Mailing+List&utm_campaign=2251646e41-Mobile_privacy_09_05_2012&utm_medium=email; Mary Madden, Privacy management on social media sites, Pew Internet & American Life Project (2012), <http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx>.

⁵⁶ Letter from Twenty-Two Consumer, Privacy, and Civil Liberties Organizations to Jan Philipp Albrecht, Rapporteur, Committee on Civil Liberties, Justice and Home Affairs, and Lara Comi, Rapporteur, Committee on Internal market and Consumer Protection, Sept. 5, 2012, <https://epic.org/privacy/intl/US-Cons-Grps-Support-EU-Priv-Law.pdf>.

⁵⁷ *Id.*

Counterfeiting Trade Agreement was severely criticized by public interest groups.⁵⁸

Similarly, in the case of the Trans-Pacific Partnership, Senator Ron Wyden reported that “he and his staff were denied access to even the U.S. TPP text proposals submitted during negotiations.”⁵⁹ Although some confidentiality insulates negotiators from undue outside pressure, excessive secrecy will backfire by “fueling concerns, fears, rumors, allegations, speculations, and paranoia and by distracting them from focusing on substantive discussions.”⁶⁰ More importantly, it is illegitimate to keep the text of the agreement secret from the people whose rights will be impacted by it. Thus, the negotiating drafts and background documents should be publicly available.

EPIC further recommends that a mechanism be created—such as a Consumer Advisory Committee—to ensure equal participation by consumer groups, privacy groups, and other members of civil society. Although the USTR has established formal advisory committees,⁶¹ there are several limitations to the advisory committee system. First, it is not clear which, if any, of the advisory committees would include a representative from a consumer privacy or data protection organization.⁶² And nonbusiness members who do serve on committees report feeling marginalized or relegated to lower-tiered committees

⁵⁸ Peter K. Yu, *Six Secret (and Now Open) Fears of ACTA*, 64 SMU L. Rev. 975, 998-99 (2011).

⁵⁹ Lori Wallach & Todd Tucker, Public Interest Analysis of Leaked Trans-Pacific Partnership (TPP) Investment Text, PUBLIC CITIZEN, June 13, 2012, <http://www.citizen.org/documents/Leaked-TPP-Investment-Analysis.pdf>; *See also Trans Pacific Partnership Agreement*, Electronic Frontier Foundation, <https://www.eff.org/issues/tpp> (“Like ACTA, the TPP is being negotiated rapidly with little transparency”).

⁶⁰ Yu, *supra* note 50, at 999-1000.

⁶¹ *See Advisory Committees*, United States Office of Trade Representative, <http://www.ustr.gov/about-us/intergovernmental-affairs/advisory-committees>.

⁶² *See id.* (listing Advisory Committee for Trade Policy and Negotiations (ACTPN); Agricultural Policy Advisory Committee (APAC); Agricultural Technical Advisory Committee for Trade (ATAC); Industry Trade Advisory Committees (ITAC); Intergovernmental Policy Advisory Committee (IGPAC); Labor Advisory Committee (LAC); Trade Advisory Committee on Africa (TACA); Trade and Environment Policy Advisory Committee (TEPAC)).

with infrequent meetings.⁶³ To its credit, the Administration has “stresse[d] the importance of stakeholder input and of the engagement of regulators on both sides to the achievement of ambitious outcomes,”⁶⁴ but it should implement this commitment through a concrete and detailed plan for engagement with civil society. In negotiating the Trans-Pacific Partnership, the USTR conducted a fifty-state domestic outreach effort⁶⁵ and held a number of question and answer sessions on the Internet.⁶⁶ Such efforts should form the minimum level of outreach when negotiating the TTIP.

EPIC notes in passing that it has recently undertaken a new Freedom of Information Act project to obtain records, including memorandum, communications, and talking points, of U.S. officials who represent the United States overseas on matters involving privacy protection. The first round of requests went to the State Department. If the USTR chooses to pursue data protection issues in the context of the TTIP, we will of course be interested in the views expressed by agency officials.

V. Conclusion

Because trade agreements are not the appropriate mechanism for determining international privacy standards, the TTIP should exclude privacy and data protection. To

⁶³ GENERAL ACCOUNTING OFFICE, REPORT TO THE RANKING MINORITY MEMBER, COMMITTEE ON FINANCE, U.S. SENATE: ADVISORY COMMITTEE SYSTEM SHOULD BE UPDATED TO BETTER SERVE U.S. POLICY NEEDS 40-42 (2002), <http://www.gao.gov/new.items/d02876.pdf>.

⁶⁴ UNITED STATES OFFICE OF TRADE REPRESENTATIVE, FINAL REPORT OF HIGH LEVEL WORKING GROUP ON JOBS AND GROWTH 2013, *available at* <http://www.ustr.gov/about-us/press-office/reports-and-publications/2013/final-report-us-eu-hlwg>.

⁶⁵ TPP Outreach and Updates, United States Office of Trade Representative, <http://www.ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-outreach-and-updates>

⁶⁶ Transcript of USTR's TPP Online Chat, United States Office of Trade Representative (May 21, 2010, 11:00 AM), <http://www.ustr.gov/about-us/press-office/blog/2010/may/ustrs-tpp-online-chat>; Transcript of TPP Question and Answer: Colombia and TPP, United States Office of Trade Representative (Jun. 15, 2010, 7:06 PM), <http://www.ustr.gov/about-us/press-office/blog/2010/june/tpp-question-and-answer-colombia-and-tpp>; Transcript of TPP Question and Answer: Customs, United States Office of Trade Representative (Jun. 18, 2010, 5:21 PM), <http://www.ustr.gov/about-us/press-office/blog/2010/june/tpp-question-and-answer-customs>; Transcript of TPP Question and Answer: Legal Services, United States Office of Trade Representative (Jun, 17, 2010, 1:30 PM), <http://www.ustr.gov/about-us/press-office/blog/2010/june/tpp-question-and-answer-legal-services>.

the extent that TTIP provisions impact cross-border data flows, they should allow governments to provide exceptions or limitations that strengthen the protection of their citizens' privacy. Finally, draft texts should be made publicly available, and a mechanism should be created to ensure equal participation by consumer groups, privacy groups, and other members of civil society.

We request an opportunity to participate in the public hearing on the TTIP.

Respectfully Submitted,

Marc Rotenberg, EPIC President and Executive Director
David Jacobs, EPIC Consumer Protection Counsel
Khaliah Barnes, EPIC Administrative Law Counsel
Julia Horwitz, EPIC Open Government Fellow

Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)