PIIE PETERSON INSTITUTE FOR INTERNATIONAL ECONOMICS

POLICY BRIEF

PB 16-12 The US-EU Privacy Shield Pact: A Work in Progress

Gary Clyde Hufbauer and Euijin Jung
August 2016

Gary Clyde Hufbauer *is Reginald Jones Senior Fellow and* **Euijin Jung** *is research analyst at the Peterson Institute for International Economics.*

© Peterson Institute for International Economics.
All rights reserved.

The modern global economy is fueled by consumers, companies, and governments communicating and exchanging information via the internet. But as people around the world engage in e-commerce, seek jobs, and share intimate details about their lives via social media, concerns arise over the vast stores of personal data possessed by multinational companies—and the risk that information transmitted over cyber networks can become readily available to US intelligence and law enforcement agencies. To allay these concerns, the United States and the European Union signed the Privacy Shield Pact on July 12, 2016, aimed at protecting individual privacy while meeting the legitimate needs of companies and the government.[1]

This *Policy Brief* elucidates the elements of that pact, a revision of earlier agreements covering the same issues. It argues that the pact reflects a reasonable compromise between legitimate competing interests but that as commerce expands, as concerns about invasions of privacy grow, and as the United States faces increasing threats from terrorists, criminals, and hackers in the cyber world, some of its provisions may need to be adjusted, especially if new international agreements are reached on trade, investment, and e-commerce.

NEED FOR PROTECTION

There is little doubt that a new world of cyber-driven commerce has arrived. According to the McKinsey Global Institute, global data transfer rates expanded by a factor of more than 40 between 2005 and 2014, from 5 terabits to 211 terabits per second, with far more growth ahead (Manyika et al. 2016). Many economists argue that these activities are spurring growth in an otherwise sluggish world economy.[2]

Concerns about risks to personal privacy from the free flow of data and the possession of personal data by US corporations have troubled the European public for many years. To address them, in 1995 the European Union issued a Data Protection Directive to establish privacy norms for individuals engaging in e-commerce and communicating through social media and email systems run by large multinational corporations.[3] To ensure that these corporations respect European norms, in July 2000 the United States and the European Union negotiated the Safe Harbor Privacy Principles agreement. Under that accord, multinational corporations promised to respect the privacy of users' data in their possession. EU firms were already subject to the privacy norms set forth in the Data Protection Directive; the Safe Harbor Privacy Principles sought to establish the same protections for information held by US firms.[4] The principle meant that a European affiliate of a US firm that transferred personal customer data to its parent company in the United States was required to extend adequate data protection across the Atlantic.

The Safe Harbor Principles did not survive. In October 2015 the European Court of Justice invalidated them in a landmark decision (*Maximillian Schrems* v. *Data Protection*

1. See European Commission press release, http://europa.eu/rapid/press-release_IP-16-2461_en.htm (accessed on July 12, 2016).

2. The World Trade Organization projects trade to grow 2.8 percent in 2016, the same as 2015 (WTO press release, April 7, 2016, www.wto.org/english/news_e/pres16_e/pr768_e.htm). Manyika et al. (2016) describe slower flows in goods, services, and financial data in the decade since 2005.

3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 sets forth the rights of individuals with regard to the processing of personal data and the free movement (mainly electronic) of such data. See http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en.

4. The European Union subsequently negotiated similar pacts with several other countries.

Commissioner[5]), ruling that the Safe Harbor Principles did not prevent the leakage of corporate data files to unauthorized eyes—especially the eyes of the intelligence community—as contemplated in the 1995 Data Protection Directive.[6] The court's concerns were spurred by the disclosures of Edward Snowden, the former US intelligence contractor, who revealed that the National Security Agency (NSA) had engaged in bulk data collection from multiple corporate databases, such as those belonging to Apple, Microsoft, Facebook, Amazon, and Google. The Snowden revelations also documented data collection from private email messages and telephone calls, with the stated purpose of tracking security threats to the United States.

The newly negotiated Privacy Shield may temporarily satisfy the interests of individuals, companies, and intelligence agencies, but its provisions are likely to be challenged in future negotiations with other players in the world trading system.

After the Snowden disclosures, private firms were not in a position to demonstrate that their files were immune from intrusion by intelligence officials or hackers. But at a time of heightened concerns about terrorism, cyberespionage, and other crimes, the US intelligence community asserted that it had to retain the right to track the activities of such perpetrators.

In 2016 a new accord, the Privacy Shield Pact, was reached, but tensions between privacy advocates and intelligence agencies over these issues persist. The Obama administration argues that the new agreement protects the privacy of data on European and other citizens stored by multinational corporations while not obstructing the intelligence community's search for threats. Multinational corporations say they are pleased that the free flow of data has been enshrined as a high priority in US policy.[7] But privacy advocates in Europe and the United States still want greater protection from the potential for corporate abuse and intelligence surveillance than provided in the final terms of the pact.[8]

The Privacy Shield is hardly likely to be the last word. The USA Freedom Act of 2015 imposes new limits on the bulk collection of telecommunications metadata on US citizens by the NSA and other intelligence agencies. But critics in the United States and abroad are concerned that US intelligence agencies have too much power to obtain information from financial, telecommunications, and internet companies, which use their immense stores of private information to generate advertising and sell products. The Privacy Shield Pact created an oversight system to ensure corporate compliance and established an arbitration mechanism open to EU citizens' complaints about corporate lapses. It also established an oversight body, based in the State Department, to investigate EU complaints about intelligence collection methods. But these protections remain weak in the eyes of some Europeans.

New technologies are changing the landscape. Strong new encryption capabilities enable individuals to send and receive messages that seem beyond the decoding reach of the NSA. Major technology firms continue to resist bulk collection, by the NSA and its sister agencies, of corporate data troves held in the United States. A legal battle is ongoing over targeted discovery by the Justice Department (on behalf of the NSA) of data held abroad by US firms, such as Microsoft.

The newly negotiated Privacy Shield may temporarily satisfy the interests of individuals, companies, and intelligence agencies, but its provisions are likely to be challenged in future negotiations with other players in the world trading system. For example, the norms established in Chapter 14 (on electronic commerce) of the Trans-Pacific Partnership (TPP), which has been signed but not ratified by the United States, seem better suited for adoption by other members of the World Trade Organization (WTO). Those norms focus on ensuring the free flow of data and thwarting "data localization" (requirements that data remain on servers within one country and not spread to other countries) rather than limiting the reach of national intelligence agencies.

5. See the press release from the Court of Justice of the European Union, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

6. The *Schrems* decision built on prior European Court of Justice case law, which emphasized the fundamental right to respect for private life, guaranteed by Article 7 of the Charter of Fundamental Rights of the European Union, and the fundamental right to the protection of personal data, guaranteed by Article 8.

7. See, for example, Natalia Drozdiak, "U.S., EU Agree on Final Adjustments to Data 'Privacy Shield,'" *Wall Street Journal*, June 24, 2016 (accessed on July 6, 2016).

8. See, for example, Shawn Donnan and Duncan Robinson, "US, EU Data Deal Raises New Privacy Fears," *Financial Times*, February 29, 2016, www.ft.com/cms/s/2/5e9a1970-ded5-11e5-b67f-a61732c1d025.html?siteedition=intl#axzz4DXztxmTz (accessed on July 6, 2016).

LEGAL STRUCTURE OF THE PRIVACY SHIELD AND RELATED AGREEMENTS

The draft components of the Privacy Shield framework were agreed to on February 29, 2016, essentially as an executive branch compact between the European Commission and multiple senior US officials.[9] The components were wrapped into the US-EU agreement announced on July 12, 2016.[10] The final EU Decision on Adequacy was submitted and approved by the European Parliament and the European Council (a body consisting of representatives of all member governments). Ten such decisions have already been issued with respect to agreements with other EU partners, but the agreement with the United States overshadows all the others.

In the United States the Privacy Shield consists of a declaration on framework principles issued by the Secretary of Commerce,[11] plus six letters from cabinet officials. The declaration on the framework principles emphasizes that they apply solely to US organizations (mainly firms) that receive personal data from the European Union and wish to qualify for Privacy Shield privileges. The principles do not affect the processing of personal data within EU member states or change privacy obligations under US law.

The letters from the Secretary of Commerce (Annex I), the Secretary of State (Annex III), the Chairman of the Federal Trade Commission (Annex IV), and the Secretary of Transportation (Annex V) are all addressed to the European Commission, presumably giving them standing as executive agreements of the US government.[12] The letters from the Director of National Intelligence (Annex VI) and the Assistant Attorney General for the Criminal Division of the Department of Justice (Annex VII) are addressed to second-tier officials in the Department of Commerce, not to the European Commission. Accordingly, their standing as executive agreements appears slight or nonexistent. For the most part these letters simply recite existing legislation and procedures.

Complementary to the Privacy Shield is the US-EU "Umbrella" Data Privacy and Protection Agreement, signed on June 2, 2016, which establishes the framework for personal data transferred between US and EU intelligence and police authorities with respect to terrorism.[13] The Umbrella Agreement does not authorize such transfers or limit the quantity or type of personal data that can be transferred. It merely enumerates standards for handling data once transferred under a separate agreement.

On April 27, 2016, the European Union enacted the General Data Protection Regulation, which will take effect May 25, 2018. It will replace the 1995 Data Protection Directive with more ambitious and specific obligations for business firms.[14] This regulation is distinct from the Privacy Shield and Umbrella Agreement.

Complementing both the Privacy Shield and the Umbrella Agreement is the US Judicial Redress Act of 2015, signed by President Obama on February 24, 2016. This act enables the US Attorney General to extend the benefits of the US Privacy Act of 1974 to citizens of designated foreign countries. The Privacy Act permits US citizens (and now designated foreign citizens) to seek court relief if their personal data are wrongly used or disclosed by a company or the government. To be eligible to seek relief under the act, a foreign country must meet all three of the following conditions:[15]

1. strike a deal with the United States, akin to the Umbrella Agreement, regarding privacy protections for data shared in the course of joint investigations,
2. allow US companies to transfer the data of foreign citizens between the foreign country and the United States, and
3. ensure that the underlying data-transfer agreement does not "materially impede the national security interests of the United States."

As far as the United States is concerned, everything necessary has been done to implement the complex network

9. The Congressional Research Service offers a detailed account of the framework (Weiss and Archick 2016). For a good short overview, see Eduardo Ustaran, Harriet Pearson, Bret Cohen, and Katherine Gasztonyi, "First Look: EU-US Privacy Shield," *Hogan Lovells*, February 29, 2016, www.hldataprotection.com/2016/02/articles/international-eu-privacy/first-look-eu-u-s-privacy-shield/#more-8496 (accessed on July 6, 2016).

10. For the final EU-US Privacy Shield implementing decision, see http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

11. The declaration is Annex II in the draft EU Decision on Adequacy, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf.

12. The links to Annexes I–VII are provided at http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf.

13. See the US-EU Umbrella Data Privacy and Protection Agreement at http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.

14. The General Data Protection Regulation will impose four new requirements on all firms doing business in the European Union, which will have to (a) notify the public of any data breach; (b) give individuals the right to be forgotten; (c) assess the privacy impact of certain products, such as online marketing; and (d) build privacy into all products. In addition, the regulation requires firms with multiple subsidiaries to employ a data protection officer.

15. These conditions were added in a Senate amendment and quickly accepted by Congress and President Obama. The full text of the Judicial Redress Act of 2015 is available at www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf.

of Privacy Shield agreements without further congressional action. The agreement entered into force on July 12, 2016. The US Department of Commerce started receiving self-certifications by US firms on August 1, 2016. There is little chance that US courts will strike down any components of the overall pact.

The European situation differs. Both the European Parliament and Council ratified the final EU Decision on Adequacy, despite substantial European opposition. The European Parliament adopted the decision on May 26, 2016. EU member states (the Article 31 Committee) approved the final version of the agreement on July 8, 2016. The European Commission adopted the decision on July 12, 2016.

The Decision on Adequacy will almost certainly be challenged in the European Court of Justice.[16] Since the publication of draft documents on February 29, 2016, both the Article 29 Working Party of independent experts and the EU Data Protection Supervisors (EDPS), a group of national officials, have issued critical reports.[17] They argue that companies should both do more to protect individual privacy and be penalized more heavily when they fail to do so. They also question the latitude afforded for NSA surveillance, overlooking the fact that EU member state intelligence agencies often conduct surveillance on a similar scale.[18] The Working Party and EDPS reports to the European Parliament will serve as fodder for European opponents to challenge the final EU Decision on Adequacy in the European Court of Justice.[19] However, opponents have stated that they will give the Privacy Shield a one-year trial period before bringing a case.[20]

OBLIGATIONS OF US FIRMS

As a condition of permitting the free flow of personal data, the Privacy Shield places obligations on participating US firms. Like the Safe Harbor Principles, the Privacy Shield requires US firms that want to transfer personal data from the European Union to the United States (or other locations outside the European Union) to either enter a contractual agreement containing model clauses with the US Department of Commerce,[21] adopt corporate rules that embody the Privacy Shield principles, or enter into explicit consent agreements with individual European citizens (see Weiss and Archick 2016). Companies that handle human resource data must also commit to comply with advice from European data protection authorities. The Safe Harbor Principles covered 4,500 US firms; the Privacy Shield will probably start with that number.

The Privacy Shield includes an elaborate dispute settlement system, capped by an arbitration mechanism. US firms must self-certify their compliance with EU norms. In principle, they should resolve complaints from EU citizens within 45 days. If they do not, citizens can resort to a free alternative dispute resolution mechanism established by the European Union. Citizens can also go to their national data protection authorities, who will work with the US Department of Commerce and the Federal Trade Commission (FTC) to investigate and resolve complaints. The FTC has primary enforcement powers and can enter into consent decrees with individual firms to enforce the Privacy Shield Principles.[22] If a case is not resolved by any

16. Steve Rosenbush, "New Privacy Shield Could Face Legal Challenge in Europe, Experts Say," *Wall Street Journal*, July 8, 2016, http://blogs.wsj.com/cio/2016/07/08/new-data-shield-could-face-legal-challenge-in-europe-experts-say/ (accessed on July 10, 2016); Julia Fioretti, "EU Privacy Watchdogs Keep Open Mind on New US Data Pact," Reuters, July 26, 2016, www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN1061AY (accessed on July 26, 2016).

17. For the Article 29 Working Party and EDPS reports, see, respectively, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf and https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf. The Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy consisting of representatives from national governments, the European Commission, and the European Data Protection Supervisors. The Data Protection Supervisor and his or her assistant are appointed jointly by the European Parliament and the Commission for five-year terms. For a press summary of the Working Party's reaction, see Mark Scott, "Europe's Privacy Watchdogs Call for Changes to US Data-Transfer Deal," *New York Times*, April 13, 2016, www.nytimes.com/2016/04/14/technology/europe-us-data-privacy.html (accessed on July 6, 2016).

18. See, for example, a description of French intelligence at work in Julie Brill and Winston Maxwell, "Criticisms of Privacy Shield Fail to Recognize Shortcomings of Europe's Own Intelligence Laws," *BloombergBNA*, June 14, 2016, www.bna.com/criticisms-privacy-shield-n57982074106/ (accessed on July 6, 2016).

19. As might be expected, European NGOs have expressed their dissatisfaction with the Privacy Shield. See, for example, the letter dated March 16, 2016, from Access Now et al. to Isabelle Falque-Pierrotin, chairman, Article 29 Working Party; Claude Moraes, chair of the Committee on Civil liberties, Justice and Home Affairs; and Pieter de Gooijer, ambassador and permanent representative of the Netherlands to the European Union, https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf.

20. Julia Fioretti, "EU Privacy Watchdogs Keep Open Mind on New US Data Pact," Reuters, July 26, 2016, www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN1061AY (accessed on July 26, 2016).

21. Under the Safe Harbor Principles, the Federal Trade Commission (FTC) accepted privacy contracts with firms, but only FTC-regulated firms, such as telecoms companies, were required to sign up. Financial services firms, for example, were exempt. However, many US firms voluntarily signed up.

22. For a summary, see www.hldataprotection.com/2016/02/articles/international-eu-privacy/first-look-eu-u-s-privacy-shield/#more-8496 (accessed on July 6, 2016).

of these means, as a last resort an EU citizen can invoke an enforceable arbitration mechanism. The citizen must pay his or her own costs and attorney's fee, however, and the arbitration panel cannot award money damages.

Privacy Shield obligations will be reinforced by the EU General Data Protection Regulation when it takes effect in May 2018, along with a separate set of enforcement measures and penalties that will include money damages. EU firms transferring data to the United States or elsewhere will be required to follow the EU General Data Protection Regulation as well as existing EU norms. They are thus subject to essentially the same terms as US firms.

OBLIGATIONS OF THE INTELLIGENCE COMMUNITY

The underlying tension between demands for individual privacy and the needs of intelligence analysts is the main reason that the final Privacy Shield documents are so convoluted and that US-EU negotiations took so long to replace the Safe Harbor Principles. Both Americans and Europeans recognize the pervasive threat of terrorism and the near invisibility of individual terrorists and their networks.

The underlying tension between demands for individual privacy and the needs of intelligence analysts is the main reason that the final Privacy Shield documents are so convoluted and that US-EU negotiations took so long to replace the Safe Harbor Principles.

In the wake of Snowden, the NSA and other branches of the US intelligence community abandoned mass collection and surveillance techniques in favor of targeted approaches. Oversight is provided by the secret Foreign Intelligence Surveillance Act (FISA) Court, created in 1978. Applications for surveillance warrants and FISA hearings are highly classified. Neither the US Congress nor the US intelligence community will give EU officials an automatic say on the issuance of warrants, though case-by-case consultation with allies is always possible.

In light of these realities, the best the Privacy Shield approach could achieve (from the standpoint of privacy proponents) were declarations such as those contained in the letter from the Director of National Intelligence concerning limits on collection of electronic signals (known as signals intelligence or SIGINT) imposed by US statutes, presidential directives, and executive orders. A passage from the 18-page letter conveys its flavor:[23]

> U.S. signals intelligence activity must *always* be as tailored as feasible, taking into account the availability of other sources of information. This means, among other things, that whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk.

The Umbrella Agreement, some 14 pages of repetitive legal text, adds little to the self-imposed US limits on signals collection; it was criticized by European members of parliament.[24]

However, elsewhere in the Privacy Shield pact, the United States agreed to create a new ombudsman in the US State Department to investigate complaints from European authorities about abusive US intelligence practices.[25] Upon receiving a complaint, the ombudsman will either report back that intelligence agencies have respected their legal commitments or state that "such noncompliance has been remedied." The ombudsman will not disclose whether a person was actually under surveillance or the specific remedy applied.[26] When transferring their own troves of personal data to US intelligence, European member states can add conditions on their use or onward transfer.[27]

---

23. See the full letter at http://statewatch.org/news/2016/mar/eu-us-com-privacy-shield-annex6.pdf (the cited passage appears on page 3). Schrems, who challenged the Safe Harbor Principles in the European Court of Justice, characterized the Privacy Shield as "lipstick on a pig." See David Gilbert, "Safe Harbor 2.0: Max Schrems Calls 'Privacy Shield' National Security Loopholes 'Lipstick on Pig,'" *International Business Times*, February 29, 2016, www.ibtimes.com/safe-harbor-20-max-schrems-calls-privacy-shield-national-security-loopholes-lipstick-2327277 (accessed on July 7, 2016).

24. Elena Dal Monte, "While President Obama Signs the Judicial Redress Act, Are the European Commission and the Parliament Sharing the Same Umbrella?" *European Area of Freedom Security & Justice*, March 8, 2016, https://free-group.eu/2016/03/08/while-president-obama-signs-the-judicial-redress-act-are-the-european-commission-and-the-parliament-sharing-the-same-umbrella/ (accessed on July 6, 2016).

25. See Annex A: EU-US Privacy Shield Ombudsperson Mechanism, www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf.

26. See Sam Schechner and John D. Mckinnon, "U.S., EU Release Text of New Agreement on Protecting Data Privacy," *Wall Street Journal*, February 29, 2016, www.wsj.com/articles/u-s-eu-release-text-of-new-agreement-on-protecting-data-privacy-1456743603 (accessed on July 6, 2016).

27. This prerogative is stated in the Framework Principles letter issued by the Secretary of the US Department of Commerce. It applies to private firms as well as police and intelligence agencies.

ENCRYPTION AND WARRANTS

The intelligence community avoided onerous restrictions in the Privacy Shield pact. But two events since the Snowden revelations have limited the scope of NSA surveillance. First, the power of encryption has advanced to a level where even ordinary individuals can code their communications so that they are virtually impossible to decode. Facebook, for example, offers its users the option to send and receive encrypted messages that are unreadable to Facebook itself as well as investigators from the NSA and the Federal Bureau of Investigation (FBI).[28] If such technology becomes widely used, it might become the ultimate weapon of privacy advocates, terrorists, and criminals alike.

Second, major firms such as Google and Apple have declared that they will not cooperate with NSA searches in the absence of a warrant. While promising to expedite their responses to legal processes initiated by the government seeking data, the Reform Government Surveillance coalition, formed by 10 technology companies, strongly supported revisions in the USA Freedom Act of 2015 (which became law on June 2, 2015) to limit the NSA's collection of bulk data.[29]

Adding to this legal pushback, Microsoft recently prevailed against a Justice Department attempt to obtain email communications from its server in Dublin, Ireland. The Court of Appeals for the Second Circuit ruled that US warrants cannot be served to obtain data stored outside US territory. The Justice Department may appeal this ruling to the Supreme Court; it is also considering a mutual assistance pact with select foreign governments to serve warrants in the United States and abroad to obtain data stored in cooperating countries.[30]

IMPLICATIONS FOR THE TRANS-ATLANTIC TRADE AND INVESTMENT PARTNERSHIP

With the departure of the United Kingdom from the European Union (Brexit) and the short remaining tenure of the Obama administration, negotiations over the Trans-Atlantic Trade and Investment Partnership (TTIP) have entered uncharted waters.[31] EU Commissioner Cecilia Malmstrom and US Trade Representative Michael Froman continue to meet, but if Malmstrom played any role in the Privacy Shield negotiations it was small, and Ambassador Froman was a background figure at best (the US Trade Representative was not among the cabinet leaders who furnished letters addressed directly or indirectly to the European Commission). Under these circumstances, it seems unlikely that citizen privacy issues covered by the Privacy Shield will be revisited in the TTIP.

It seems likely, however, that the data flow and anti-localization features of TPP Chapter 14 will find their way into a TTIP chapter.[32] As far as personal data are concerned, any TTIP provisions will be subject to the Privacy Shield; companies will need to take the pledge before they can transmit such data across the Atlantic or to other destinations outside Europe. It seems likely that TTIP will formally adopt the e-commerce freedoms established in the TPP, as free data flows and antilocalization policies are already practiced on both sides of the Atlantic.

E-COMMERCE CHAPTER OF THE TRANS-PACIFIC PARTNERSHIP

Comparisons between TPP Chapter 14 and the Privacy Shield Pact are instructive (see appendix table A.1). The two agreements cover related terrain, but their origins differ, leading to different commitments. Privacy Shield negotiations were concerned principally with protecting privacy in the digital age; TPP Chapter 14 was designed to ensure the free flow of data and minimize data localization.

The Privacy Shield accords are lengthy; in contrast, TPP Chapter 14 is just a few pages. Country-specific exceptions

28. See Robert McMillan and Anne Steele, "Facebook Launches End-to-End Encryption Option for Messenger," *Wall Street Journal*, July 8, 2016, www.wsj.com/articles/facebook-launches-end-to-end-encryption-option-for-messenger-1467987394 (accessed on July 11, 2016).

29. The 10 companies are AOL, Apple, Dropbox, Evernote, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo. For coalition activities, see www.reformgovernmentsurveillance.com. The Obama administration signed Presidential Policy Directive 28 on January 17, 2014, to limit but not forbid bulk data collection by signals intelligence (SIGINT). See https://icontherecord.tumblr.com/ppd-28/2015/overview.

30. Devlin Barrett and Jay Greene, "Microsoft Wins Appeals Ruling on Data Searches," *Wall Street Journal*, July 14, 2016, www.wsj.com/articles/microsoft-wins-appeals-ruling-on-data-searches-1468511551; "U.S. to Allow Foreigners to Serve Warrants on U.S. Internet Firms," *Wall Street Journal*, July 15, 2016, www.wsj.com/articles/obama-administration-negotiating-international-data-sharing-agreements-1468619305 (both accessed on July 18, 2016).

31. According to the UK Information Commissioner's Office, the departure of the United Kingdom from the European Union will make upcoming EU reforms to data protection laws, including the US-EU Privacy Shield agreement, not applicable in Britain. See "Privacy Shield Developments and UK Data Transfers Post-Brexit," www.dataprivacymonitor.com/international-privacy-law/privacy-shield-developments-and-uk-data-transfers-post-brexit/ (accessed on July 21, 2016).

32. Because of EU sensitivity over the Privacy Shield agreement, the current EU draft text on digital trade in TTIP leaves out provisions on cross-border data flows. See "Cross-Border Data Provisions Not Included In Draft EU Digital Trade Chapter," *Inside US Trade*, July 19, 2016, http://insidetrade.com/daily-news/cross-border-data-provisions-not-included-draft-eu-digital-trade-chapter (accessed on July 20, 2016).

scheduled in TPP Chapter 14 cover only Brunei, Malaysia, and Vietnam. If ratified, new TPP obligations for the United States would be spelled out in implementing legislation. Chapter 14 would require few, if any, US statutory changes, although there could be regulatory modifications (for example, the Judicial Redress Act of 2015 would probably be extended to cover citizens of some TPP countries).

With respect to personal privacy, TPP Chapter 14 is less demanding than the Privacy Shield. After acknowledging the value of protecting personal information, Article 14.8 goes on to put responsibility on each TPP member country:[33]

> 2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.

This language enables TPP members to enact legislation akin to the Privacy Shield, but it does not require elaborate—or indeed any—protection for individuals or redress against firms. Moreover, while the provisions of Chapter 14 are subject to TPP Chapter 28 Dispute Settlement, relief is limited to state-to-state proceedings; neither individuals nor companies have standing under Chapter 28. It may be years before any TPP member state lodges a complaint about inadequate laws or enforcement effort in another TPP member state.

TPP Article 14.11 ("Cross-Border Transfer of Information by Electronic Means") strongly discourages but does not prohibit data localization:[34]

> 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
>
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
>
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
>
> (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

The reason for this provision is that the economic consequences of data localization requirements are very negative. Compliance costs can be high for both large and small firms. If local data centers do not own large public cloud systems, they may demand 30–50 percent more for server space.[35] Multinational corporations can handle the higher costs associated with forced data localization. In contrast, small and medium-sized enterprises may simply abandon plans to expand their market reach. Russia's data localization law, for example, forced Google and Apple to build data centers locally so that personal data could remain in local servers.[36] Bauer et al. (2015) estimate that enactment of its privacy law cost Russia 0.27 percent of real GDP (for the costs of data localization in various countries, see Bauer et al. 2014).

TPP Chapter 14 deals with the tension between intelligence needs and personal privacy by ducking. Article 14.2 ("Scope and General Provisions") places no burden on the intelligence community. The TPP does contain provisions designed to protect strong encryption technologies, which are set forth in an annex to Chapter 8 on Technical Barriers to Trade. As the Apple iPhone case revealed, strong encryption technology can create severe obstacles for law enforcement and intelligence agencies.[37] Indirectly, therefore, TPP can be said to promote privacy at the expense of the intelligence community.

MODELS FOR THE WORLD TRADE ORGANIZATION OR THE TRADE IN SERVICES AGREEMENT

Because privacy protection and e-commerce are global concerns, WTO members may consider a new multilateral agreement once the organization gets past its Doha Round

33. Brunei, Malaysia, and Vietnam are allowed extra time to implement this (and other) TPP chapters.

34. The definitions in Article 14.1 exclude financial firms from the class of "covered persons," so those firms get no benefit from strictures against data localization—or for that matter the free flow of data between TPP members. This exclusion is criticized by financial institutions, which argue that the right of free flow of data and the ban on data localization should apply to them.

35. Tech UK, "ITIC: How Data Localization Requirements Impact Entrepreneurship," April 14, 2016, www.techuk.org/insights/opinions/item/8289-itic-how-data-localization-requirements-impact-entrepreneurship (accessed on July 13, 2016).

36. Sam Schechner and Olga Razumovskaya, "Russia Puts off Data Showdown with Technology Firms," *Wall Street Journal*, August 31, 2015, www.wsj.com/articles/russia-puts-off-data-showdown-with-technology-firms-1441043618 (accessed on July 13, 2016).

37. See Branstetter (2016) and Cecilia Kang and Eric Lichtblau, "F.B.I. Says It Needs Hackers to Keep up with Tech Companies," *New York Times*, April 19, 2016, www.nytimes.com/2016/04/20/technology/fbi-iphone-apple-house-encryption-hearing.html (accessed on July 11, 2016).

pains. On a faster timetable, the 50 countries engaged in plurilateral Trade in Services Agreement (TiSA) negotiations may decide to include a chapter addressing both e-commerce and privacy.

On balance TPP Chapter 14 appears to offer a more suitable starting model than the Privacy Shield, for two reasons. First, it avoids frontal entanglement with intelligence communities. The United States and other lead countries in the intelligence world (Britain, France, Germany, China, and Russia) will fiercely resist proposals that subject the collection of signals intelligence to external oversight. Negotiations on this subject will not go farther than national versions of the Director of National Intelligence "comfort letter" appended as Annex VI of the Privacy Shield agreement. This letter is already a matter of public record; the clarifications it provides are available to all countries. Other intelligence powers can publish parallel letters without the need for WTO negotiations.

Second, TPP Chapter 14 may offer a better starting point because the elaborate EU system of enforcing Privacy Shield obligations of companies—culminating in binding arbitration—would represent a radical innovation for the WTO or TiSA. Compliance questions and dispute settlement in trade agreements are almost always handled on a state-to-state basis. If countries want to compel companies to protect individual data privacy, they can do so on a national basis, as permitted by TPP Chapter 14. By contrast, the Privacy Shield calls for US companies to self-certify to the US Department of Commerce and assigns the department and the FTC investigatory and enforcement roles. It ultimately looks to EU bodies to ensure compliance, however. The dual mandate seems cumbersome, especially if extended to 50 or more countries.

The Privacy Shield seems beyond the capacity of the WTO to adopt in the near future. However, a global framework protecting data flows and guarding against forced localization would go far to ensure that the most dynamic component of world commerce reaches its full potential. Individual countries can learn from the US-EU Privacy Shield and the EU's General Data Protection Regulation to fashion their own systems of privacy protection. There is no reason that the free flow of data needs to impede national measures to protect citizen privacy.

Reflecting these conclusions, on July 1, 2016, the US Trade Representative tabled a proposal in the WTO to update the General Agreement on Trade in Services (GATS) through an agreement on electronic commerce.[38] The three-page nonpaper listed subjects "that can contribute meaningfully to the flourishing of trade through electronic and digital means." These subjects included the following:

- prohibiting customs duties for digital products,
- establishing nondiscrimination principles between foreign and domestic firms,
- allowing companies and consumers to move data as they see fit,
- preventing localization barriers, and
- barring forced technology transfers.

It remains to be seen whether other WTO members will warm to this approach, which builds on TPP Chapter 14. If they do, it should be possible to conclude an agreement in two or three years. If instead a substantial number of WTO members insist that a GATS pact must contain privacy enforcement mechanisms directed at corporations—or try to limit intelligence gathering with an array of GATS rules—the negotiations will last a long time.

38. See "A US E-Commerce Proposal," *Washington Trade Daily*, July 5, 2016.

APPENDIX A

Table A.1 Comparison of Safe Harbor, Privacy Shield, and Trans-Pacific Partnership (TPP) e-commerce provisions

Item	Safe Harbor Privacy Principles (2000)	Privacy Shield Pact (2016)	TPP Chapter 14 on E-Commerce (2016[a])
Coverage	Firms and EU citizens	Firms and EU citizens	TPP member states
Cross-border data flows	A third-party recipient of personal information must either be subject to the 1995 Data Protection Directive or agree to the same level of privacy protection required by that directive.	Cross-border data transfers can take place only for limited and specified purposes, on the basis of a contract, and if that contract provides the same level of protection guaranteed by the Privacy Shield principles and General Data Protection Regulations.	Article 14.11: TPP member states should allow covered persons (excluding financial firms) to transfer data, including personal data, digitally across borders.
Privacy protection	Firms must reveal the purpose of data collection, the resolution mechanism for complaints, conditions for onward transfer, and individual choices for objecting to the use and disclosure of personal data by firms.	Firms must reveal the types of data collected, the purposes of data processing, right of access, conditions for onward transfer, and individual choices for objecting to the use and disclosure of personal data by firms. Firms must make public their privacy policies consistent with the Privacy Shield principles and provide links to the US Department of Commerce's website, the Privacy Shield list, and the website of an alternative dispute settlement provider.	Article 14.8: TPP member states should adopt nondiscriminatory practices (between foreign and domestic firms) when ensuring against the violation of personal privacy with respect to electronic commerce.
	The US Department of Commerce will either take noncomplying firms off the public list so that they no longer enjoy Safe Harbor privileges or impose alternative sanctions.	The US Department of Commerce will monitor compliance with Federal Trade Commission rules. Firms that fail to meet their obligations will be sanctioned or lose eligibility to transfer data across borders.	Article 14.8: TPP member states should publish information on personal information protections provided to subjects of e-commerce, including information on how individuals can pursue remedies and business can comply with legal requirements.
		Individuals can complain directly to companies, to the independent dispute resolution body, or to the EU data protection authority, which will work with the US Department of Commerce and the Federal Trade Commission to investigate complaints. As a last resort, they can seek binding arbitration by the Privacy Shield Panel.	
Intelligence	The Safe Harbor provides no principles that limit the collection of bulk data conducted by US intelligence community.	The United States provided assurances that bulk data collection will be limited and created a new ombudsman in the State Department to investigate complaints from European authorities about abusive US intelligence practices. An annual joint review between the European Commission and the US Department of Commerce will be held.	Annex 8-B of TPP Chapter 8 (on technical barriers to trade) encourages strong encryption technologies.

a. The TPP text was concluded in 2016 but has not been ratified.

Sources: US-EU Safe Harbor Framework (2009), European Commission Privacy Shield Decision on Adequacy (2016), TPP Chapter 14.

REFERENCES

Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde. 2014. *The Costs of Data Localization: Friendly Fire on Economic Recovery*. ECIPE Occasional Paper 3, Brussels: European Center for International Political Economy. Available at www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde. 2015. *Data Localization in Russia: A Self-Imposed Sanction*. ECIPE Policy Brief 6. Brussels: European Center for International Political Economy. Available at www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf.

Branstetter, Lee. 2016. TPP and Digital Trade. In *Assessing the Trans-Pacific Partnership. Volume 2: Innovation in Trading Rules*, ed. Jeffrey J. Schott and Cathleen Cimino-Isaacs. PIIE Briefing 16-4. Washington: Peterson Institute for International Economics.

European Commission. 2016. *Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield*. Brussels.

Manyika, James, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, and Dhruv Dhingra. 2016. *Digital Globalization: The New Era of Global Flows.* McKinsey Global Institute. Available at www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

US Department of Commerce. 2009. *US-EU Safe Harbor Framework*. Washington. Available at http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf.

Weiss, Martin A., and Kristin Archick. 2016. *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield*. May. Washington: Congressional Research Service. Available at www.fas.org/sgp/crs/misc/R44257.pdf.

© Peterson Institute for International Economics. All rights reserved.

This publication has been subjected to a prepublication peer review intended to ensure analytical quality. The views expressed are those of the authors. This publication is part of the overall program of the Peterson Institute for International Economics, as endorsed by its Board of Directors, but it does not necessarily reflect the views of individual members of the Board or of the Institute's staff or management.

The Peterson Institute for International Economics is a private nonpartisan, nonprofit institution for rigorous, intellectually open, and indepth study and discussion of international economic policy. Its purpose is to identify and analyze important issues to make globalization beneficial and sustainable for the people of the United States and the world, and then to develop and communicate practical new approaches for dealing with them. Its work is funded by a highly diverse group of philanthropic foundations, private corporations, and interested individuals, as well as income on its capital fund. About 35 percent of the Institute's resources in its latest fiscal year were provided by contributors from outside the United States. A list of all financial supporters for the preceding four years is posted at https://piie.com/sites/default/files/supporters.pdf.