Analysis

TTIP and TiSA: big pressure to trade away privacy

Ralf Bendrath,
Senior Policy Advisor to Jan Philipp Albrecht MEP (Greens/EFA), Brussels

September 2014

The negotiations between the U.S. and the EU on the "Transatlantic Trade and Investment Partnership" (TTIP) will address e-commerce and transatlantic data flows. In this context, there are more and more indications that European data protection standards could be undermined by such a trade agreement. Civil society and consumer organisations both in the EU and the United States [1] warn that draft provisions in the chapter on e-commerce and electronic data flows pose a threat to European privacy and data protection rights. Provisions in the proposed Trade in Services Agreement (TiSA) also threaten to radically undermine the rights to privacy and data protection.

EU: "Keep data protection out of trade talks"

The trade negotiators of the EU Commission have insisted repeatedly and publicly (e.g. at a hearing of the Greens/EFA in the European Parliament on 5 March 2014 [2]), that they have no mandate to negotiate over data protection rules. This was also emphasised by EU justice commissioner Viviane Reding during a speech in Washington in October 2013:

> *"(…) there are issues that will easily derail [TTIP]. One such issue is data and the protection of personal data. This is an important issue in Europe because data protection is a fundamental right. (…) This is why I warn against bringing data protection to the trade talks. Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable."* [3]

The negotiation mandate for the EU Commission instead refers to Article XIV of the General Agreement on Trade in Services (GATS) of the World Trade Organization, which contains a general exception clause:

> *"Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services,* ***nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures****:*
>
> *(…)*

> *(c)* ***necessary to secure compliance with laws or regulations*** *which are not inconsistent with the provisions of this Agreement including those* ***relating to****:*
>
> *(…)*
>
> *(ii)* ***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; (…)"* [4] (emphasis added)

The EU Commission's negotiation mandate states in Article 18:

> *"The Agreement will* ***not preclude the enforcement of exceptions on the supply of services justifiable under the relevant WTO rules*** *(Articles XIV and XIVbis GATS)."* [5] (emphasis added)

Article XIV of GATS was indeed copied verbatim into a draft text of the TTIP agreement proposed by the EU Commission negotiators in July 2013 and leaked in February 2014. [6]

So all is well? Surely it's not. This is only the mandate for the EU negotiators. But in any international agreement, it takes at least two to tango.

"Interoperability" or "adequacy"?

On the American side, there have been numerous attempts to undermine European data protection rules in the context of the trade talks. New lobby organisations have been set up - for example, the "Coalition for Privacy and Free Trade", coordinated by US law firm Hogan Lovells and including a number of political heavyweights. [7] A recurring theme in these lobbying efforts over the last few years has been to push for "interoperability" between the European and American rules on data protection. This basically means a mutual recognition of the respective rules on both sides of the Atlantic, maybe with some legal tricks to make the arrangement appear solid.

The catch: in the United States, there are currently no comprehensive data protection laws. The Safe Harbor decision of 2000, [8] under which US companies can voluntarily submit to European standards so as to be allowed to process personal data from Europe, is largely ineffective. The European Parliament criticized it when it was developed in 2000, and in the final report of the NSA special inquiry of 12 March 2014 even demanded its suspension. [9] So there is nothing to be interoperable with from a European perspective, except for voluntary self-regulation measures and the usual non-enforceable commitments to transparency in order to allow "consumer choice", which are buried under long and unreadable terms of service. [10]

"Interoperability" is an attempt to undermine European data protection standards. The requirements in EU data protection law set a much higher threshold than just "interoperability". The Data Protection Directive of 1995 in Article 25 requires that:

> *"the* ***transfer to a third country of personal data*** *which are undergoing processing or are intended for processing after transfer* ***may take place only if*** *(…) the third country in question ensures an* ***adequate level of protection****."* (emphasis added)

In short, the European foundation for the transfer of personal data to third countries is the "adequacy" of their data protection situation. The US side is trying to replace this with mere "interoperability".

Some European data protection experts are already part of this “interoperability” manoeuvre. At the end of April 2014, Massachusetts Institute of Technology and the University of Amsterdam launched a series of roundtables called “privacy bridges”

> *“to develop a framework of **practical interoperability** options to bridge the gaps between the European and United States legal systems of data privacy. (…) Over the next 18 months, the group will prepare a consensus white paper outlining a path forward between the United States and Europe. The efforts are aimed at providing a framework of practical options that advance strong, globally accepted privacy values in a manner **that produces interoperability and respects the substantive and procedural differences between the two jurisdictions**.”* [11] (emphasis added)

Participants include some well-known data privacy defenders such as former German commissioner Peter Schaar, but others have strong industry links, which are disguised behind a university affiliation. [12] Anything developed in this context might end up in the TTIP text later. The scope of the privacy bridges project excludes legal changes in US law. Ironically, even the White House “big data” report, which was published about the same time as the project was started, explicitly states a need for better legal protections for non-US-persons under American data protection law. [13]

Some heavy-weight industry players go even further than “interoperability”. The Business Coalition for Transatlantic Trade, founded by the US Chamber of Commerce, calls for “a framework that allows for flexibility on privacy and continuing cooperative work on security matters” [14] – as if the NSA leaks had never happened and Europe had no fundamental right to data protection.

Are “Schengen routing” and an “EU cloud” barriers to trade?

The US side has been playing a semantic trick for a few months now. It began in the context of European responses to the Snowden surveillance affair. From several sides, there were suggestions to introduce changes to the routing of Internet data packets, so that they take a certain path and remain within the EU or even within Germany in cases where the sender and receiver are both located there. Such suggestions were made - with different motives - by privacy experts such as Ian Brown from Oxford University, [15] but also by Deutsche Telekom. [16] What at first glance sounds like a sensible idea (why should an email from Brussels to Berlin be routed through New York or other shady jurisdictions?) is technically not easy, and is also dangerous in its potential second-order effects. Technically it is not trivial because the Internet protocol with its IP addresses uses a logical address space that does not know from the underlying physical transport level where a given IP address is geographically located. While there are services to enable IP-level localisation, they only reach an approximation: my own IP address in the European Parliament in Brussels looks like I am located in Luxembourg, because of the three official seats of the Parliament in Brussels, Luxembourg and Strasbourg. Even if geo-routing was technically feasible, it cannot be our goal to re-shape the topology of the transnational and global Internet along national boundaries. This would quickly trigger undesirable consequences, such as calls for "immigration controls" for data packets, which would be equivalent to Internet censorship. [17]

The Greens in the European Parliament tabled an amendment to the final report of the NSA special inquiry to instead encrypt all Internet traffic from end to end, because then it would no longer matter where the data was flowing. This amendment was adopted as part of a compromise at the committee vote in February and confirmed by the Parliament’s plenary vote in March. [18] After the debate on national or European routing seemed dead by early 2014, German Chancellor Angela Merkel pushed for some kind of European routing in her weekly podcast, [19] which was taken up widely by the media. The debate simmers on.

From the US side, this debate is now being used to attack European rules and limitations for the transfer of personal data to third countries. They throw terms like “Schengen network”, “cloud computing” and the third country rules of the EU Data Protection Directive into the same category, and label it with the term “localization”. US Trade Representative Michael Froman did this on 4 April 2014 in the presentation [20] of his report on trade agreements for the telecommunications market. [21] He claimed that European “localization” rules that would require data transport or data processing in Europe constitute an illegal trade barrier. The “Business Coalition for Transatlantic Trade” argues along the same lines and calls for the TTIP agreement “to prohibit requirements that service suppliers use local servers or other infrastructure or establish a local presence.” [22]

It is however important to keep routing and data processing clearly distinct here. [23] While rules on data packet routing may be ill-advised, it is highly relevant where data is processed – especially if it is personal data. Even on the European side of this debate, many have not yet fully understood that EU data protection rules are *fundamentally* rules for localization. Because data protection in Europe is a binding fundamental right with constitutional status in the EU Charter of Fundamental Rights, personal data may in principle be processed only within Europe. Any rules for the transfer of such data to third countries constitute exceptions from this principle and must meet certain conditions - such as an adequate level of protection in the respective third country.

In the post-Snowden era, there is a wider debate now in Europe over stricter limits on transfers of personal data to the US and other third countries. The European Parliament has introduced a new Article 43a into its version of the upcoming General Data Protection Regulation, [24] which would prevent third countries’ authorities from demanding a transfer from a European data controller without regard to a mutual legal assistance treaty. The European Court of Justice will now have to decide if data transfers to the US under the Safe Harbor decision are still legal, after a preliminary ruling from the Dublin High Court based on a challenge by Austrian activist Max Schrems and his group “Europe vs Facebook”. [25]

The “Digital Trade Act” and TTIP

US Trade Representative Michael Froman is not alone. A draft “Digital Trade Act”, introduced in the US Senate in December 2013, [26] would give the United States Trade Representative a binding mandate for international negotiations in the area of e-commerce. Regulations for “localization” would have to be banned, and “interoperability” of data processing rules would be enshrined as a fundamental principle. This Act would of course also apply to negotiations over the corresponding chapter in the TTIP agreement. The bill is currently being discussed in the Committee on Finance. Similar provisions can also be found in the draft for a bipartisan “Trade Priorities Act”, introduced in the US Senate in January 2014. [27]

Drafts from US negotiators for the e-commerce section of TTIP already include these two crucial points: the principle of “interoperability” of European and US data protection rules, and a ban on “localization”. [28] It is clear that there is a strong push from US negotiators, backed by US industry, to keep this in the final agreement text.

The EU Commission is obliged to not meet the US side’s demands in any way. But trade negotiations always lead to compromise. It is therefore to be feared that TTIP will, at least in attenuated form, include regulations that undermine our European data protection standards, e.g. by limiting the room of interpretation for the GATS exception clause to extraordinary circumstances.

The Trade in Services Agreement (TiSA): TTIP on steroids

Parallel to TTIP, and largely un-noticed by the public for a year, negotiations for a plurilateral agreement on trade in services have been taking place since January 2013. [29] The so-called Trade in Services Agreement (TiSA) would succeed GATS for the countries involved – so far the US, the EU, and 21 others, all from the industrialised world. [30] US industry has woken up to the rise of public debate and criticism around TiSA in recent months, and like in the context of TTIP, has started a PR campaign in favor of loosening trade restrictions through TiSA. The "TiSA Business Coalition", also called "Team TiSA", was launched on 18 June 2014 in Washington in the presence of the US Trade Representative and the Japanese ambassador. [31]

An explicit goal of the TiSA negotiations is to overcome the exceptions in GATS that protect certain non-tariff trade barriers, inter alia data protection. [32] A first leak of a TiSA document illustrates this: the draft Financial Services Annex of TiSA, published by Wikileaks on 19 June 2014, would allow financial institutions, such as banks, the free transfer of data, including personal data, from one country to another. [33] This would constitute a radical carve-out from European data protection rules. The transfer and analysis of financial data from EU to US authorities for the US "Terrorist Finance Tracking Programme" (TFTP) has already shaken EU-US relations in the past and led the European Parliament to veto a first TFTP agreement in 2010. With the draft text of the TiSA leak, all floodgates would be opened.

The weakening of EU data protection rules through TiSA goes further than "only" the financial sector. According to sources close to the negotiations, a draft of the TiSA "Electronic Commerce and Telecommunications Services Annex" contains provisions that would ban any restrictions on cross-border information flows and localisation requirements for ICT service providers. A provision proposed by US negotiators would rule out any conditions for the transfer of personal data to third countries that are currently in place in EU data protection law. Another provision, again put on the table by US negotiators, would ban requirements to use computing facilities in the respective country.

Personal data localization as a fundamental right

In the context of Snowden revelations, it has become clear that Europe urgently needs to invest in re-building an independent IT industry, from the hardware level to the applications and services, if it wants to be protected from mass surveillance by the NSA. European public authorities and private companies increasingly insist on localisation provisions when buying computing services in order to ensure that their personal data or their sensitive business information does not end up in shady jurisdictions. This was even underlined by the European Court of Justice in its landmark ruling that repealed the data retention directive in April 2014, where the Court openly criticised the lack of localisation obligations:

> *"[The data retention] directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security (…) is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data."* [34]

In plain English: any trade agreement must not prohibit such a preferential treatment of European ICT companies. Or in even simpler English: "Eat this, US Trade Representative."

It remains to be seen if Europe can maintain and even improve its data protection rules in the face of massive pressure to reach agreement on TTIP and TiSA.

Endnotes

[1] Privacy International, the Center for Digital Democracy, the European consumer alliance BEUC and the U.S. Consumer Federation have been most active on this so far.
[2] Documentation: http://www.greens-efa.eu/transatlantic-data-flows-and-the-trade-and-investment-partnership-ttip-11815.html, a good summary is available at http://acta.ffii.org/?p=2050.
[3] Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner: 'Towards a more dynamic transatlantic area of growth and investment', speech at a Conference organised by the Peterson Institute, SAIS and the EU Delegation, Washington DC/USA, 29 October 2013, http://europa.eu/rapid/press-release_SPEECH-13-867_de.htm
[4] World Trade Organization: General Agreement on Trade in Services, 1995, http://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm
[5] Council of the European Union, 'Directives for the negotiation on the Transatlantic Trade and Investment Partnership between the European Union and the United States of America', 17 June 2013, http://www.s2bnetwork.org/fileadmin/dateien/downloads/EU-TTIP-Mandate-from-bfmtv-June17-2013.pdf
[6] See Article 64, http://keionline.org/sites/default/files/eu-kommission-position-in-den.pdf
[7] Among them are former EU ambassador to the US Hugo Paemen, former US Trade Representative Clayton Yeutter, and Daniel Weitzner, former Deputy Chief Technology Officer for Internet Policy in the White House, see http://www.hoganlovells.com/hogan-lovells-forms-coalition-for-privacy-and-free-trade-03-18-2013
[8] Commission Decision 2000/520/EC of 26 July 2000, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF
[9] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN
[10] See 'Terms of Service; Didn't Read', http://www.tosdr.org
[11] Press release by the MIT's CSAIL project and University of Amsterdam's Institute for Information Law, 'EU and US privacy experts in search of transatlantic privacy solutions' (including a participants list), http://www.ivir.nl/news/privacy_bridges_launch.pdf. See also: Sam Pfeifle, 'Will New Privacy Bridge Project Bring EU and U.S. Together?', https://www.privacyassociation.org/publications/will_new_privacy_bridge_project_bring_eu_and_u.s._together
[12] For example co-convenor Daniel Weitzner who is also involved in the above-mentioned industry 'Coalition for Privacy and Free Trade', or Christopher Kuner from Brussels-based law firm Wilson Sonsini Goodrich & Rosati, chairman of the Task Force on Privacy and the Protection of Personal Data of the International Chamber of Commerce. **Update, 26 September 2014: Christopher Kuner has asked for a clarification that he nowadays spends most of his time as an academic and is no longer chair of the ICC task force.**
[13] Executive Office of the President: 'Big Data: Seizing Opportunities, preserving values', 1 May 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014_1.pdf
[14] Business Coalition for Transatlantic Trade: Digital Trade, http://www.transatlantictrade.org/issues/digital-trade. European businesses at least seem to have accepted the existence of data protection rules. A May 2014 joint position paper from the Coalition of Services Industries and the European Services Forum explicitly refers to the GATS exceptions for the protection of privacy, see https://servicescoalition.org/images/CSI__ESF_Joint_Statement_on_TTIP_-_FINAL.pdf
[15] Ian Brown, 'Will NSA revelations lead to the Balkanisation of the internet?', *The Guardian*, 1 November 2013, http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet
[16] Jürgen Berke, ‚Telekom will innerdeutschen Internetverkehr übers Ausland stoppen', Wirtschaftswoche, 12 October 2013, http://www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html
[17] Under the Hungarian EU Council presidency, a proposal for a "virtual Schengen border" for the Internet was discussed in 2011, see: http://edri.org/virtual_schengen
[18] Ibid. at [9]

[19] Matthias Monroy, ‚Aus #Neuland wird #Schengenland: Merkel für Aufbau "europäischer Kommunikationsnetzwerke"', 16 Februuary 2014, http://netzpolitik.org/2014/aus-neuland-wird-schengenland-merkel-fuer-aufbau-europaeischer-kommunikationsnetzwerke
[20] Office of the US Trade Representative, 'USTR Targets Telecommunications Trade Barriers', press release, 4 April 2014, http://www.ustr.gov/about-us/press-office/press-releases/2014/March/USTR-Targets-Telecommunications-Trade-Barriers
[21] Office of the United States Trade Representative, '2014 Section 1377 Review On Compliance with Telecommunications Trade Agreements', http://www.ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf
[22] Business Coalition for Transatlantic Trade, 'Digital Trade', http://www.transatlantictrade.org/issues/digital-trade
[23] This is already established in "mere conduit" rules for telecommunications carriers, who cannot be held liable for the content they transport or for the data processing that takes place at the sender or receiver.
[24] European Parliament legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012, Amendment 140, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402
[25] Judgement of the Irish High Court, Judge Hogan, in Case 2013 No. 765JR, 18 June 2014, http://www.europe-v-facebook.org/hcj.pdf
[26] S.1788 – Digital Trade Act of 2013, introduced 12 December 2013 by Sen. John Thune (R-SD), https://beta.congress.gov/bill/113th-congress/senate-bill/1788
[27] S.1900 - Bipartisan Congressional Trade Priorities Act of 2014, introduced 9 January 2014 by Sen. Max Baucus (D-MT), https://beta.congress.gov/bill/113th-congress/senate-bill/1900
[28] EU Commission trade official Jan-Willem Verheijden at the hearing organised by Greens/EFA in the European Parliament, 5 March 2014. See: Ante Wessels, 'US wants to undermine privacy in TTIP negotiations', http://acta.ffii.org/?p=2050.
[29] The start of negotiations was announced by the USTR on 16 January 2013 in a blog post (see http://www.ustr.gov/about-us/press-office/blog/2013/january/wts-entering-negotiations-for-ista), but negotiations have taken place under utmost secrecy and in non-standard locations outside the WTO in Geneva, e.g. in the Australian embassy.
[30] Among them are Switzerland, Canada, Japan, Australia, South Korea, Turkey, and countries from Latin America and Asia.
[31] See http://www.teamtisa.org
[32] Andreas Zumach, ‚Geheimverhandlungen in Genf', *taz*, 27 April 2014, http://www.taz.de/!137455
[33] Trade in Services Agreement (TiSA): Financial Services Annex, Consolidation of text proposals as of 14 April 2014, available at https://wikileaks.org/tisa-financial/WikiLeaks-secret-tisa-financial-annex.pdf
[34] See paragraph 68:, Judgement of the Court (Grand Chamber) in Joined Cases C‑293/12 and C‑594/12, 8 April 2014, http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN