Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic
University of Ottawa – Faculty of Law, Common Law Section
57 Louis Pasteur Street
Ottawa|ON|K1N 6N5
cippic@uottawa.ca
https://cippic.ca

LEGISLATIVE ASSEMBLY OF BRITISH COLUMBIA

Special Committee to Review the *Freedom of Information and Protection of Privacy Act*

Oral Testimony of the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)

ON

Trade Agreements: Recent and Upcoming Implications for BC FIPPA section 30.1

November 18, 2015

Tamir Israel, Staff Lawyer

INTRODUCTION

1. Thank you. Good morning Mr. Chairman and members of the Committee. My name is Tamir Israel and I am Staff Lawyer with CIPPIC, the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa's Faculty of Law. I am also a member in good standing of the Law Society of Upper Canada. CIPPIC is grateful for the opportunity to provide our input into this committee's review of the BC *Freedom of Information & Protection of Privacy Act*.

2. CIPPIC is a law and technology clinic that works to advance the public interest in policy debates at the intersection of law and technology, which is our core mandate. We additionally provide pro bono legal assistance to under-represented organizations and individuals on law and technology issues, and provide legal and public education on related matters. CIPPIC's expertise in this field has evolved through its myriad public advocacy activities on this front, which include interventions at various levels of court, involvement in Internet governance related matters before various quasi-judicial tribunals and international fora, the publication of academic and research reports on Internet law related issues, and expert testimony before parliamentary committees such as this one.

3. While CIPPIC has wide-ranging interest in issues related to privacy, data protection and freedom of information, I have been asked today to provide an overview of potential implications arising from trade agreements for BC FIPPA's data localization mechanism, encoded in section 30.1. My comments today will therefore present a change of pace from testimony heard so far by this committee as they'll be restricted to that topic. We do, however, reserve the option of providing a more comprehensive written submission within your comment period.

4. In my comments today I will first provide an overview of section 30.1 and the foreign intelligence context, followed by an overview of recent developments in trade agreements. I will close with some details on specific implications or potential implications of trade agreements for section 30.1 of BC *FIPPA*.

Section 30.1 & Foreign Intelligence Concerns: An Overview

5. At the outset, I'll address section 30.1 by way of background, however the core of my presentation will relate to trade implications. As the committee is aware, section 30.1 was enacted out of concern that outsourcing of storage of Canadian data – and particularly of health information – to the United States would subject this data to an excessive investigative context that places few

limits state data-gathering activities. The passing of the USA PATRIOT Act was, at the time, pointed to as an example of the expansive powers granted to United States agencies. However, a less notorious yet far more serious United States law – the FISA Amendment Act of 2008 – is the true source of concern for Canadian data hosted in the United States. It provides United States intelligence agencies, primarily the National Security Agency (NSA), near limitless powers to access the information of foreigners.[1] While these powers are so broad they incidentally capture significant amounts of US data, they at least provide some minimal protection for non-foreigners in the nature of restrictions on its use, further disclosure and identity suppression.

6. The NSA has not hesitated to make full use of its expansive powers, and documents released by former NSA contractor Edwards Snowden demonstrate that the agency obtains an average of 100 million pieces of data from United States-based computer network in an average day.[2] A detailed qualitative analysis of NSA-stored data obtained by the Washington Post demonstrates the expansive nature of the resulting data collection programs. This analysis found that only 10% of the 11,000 individuals whose data was present in the sample were actual NSA targets, the rest being individuals whose data was collaterally captured in getting to those 10%. Given the minimal technical and legal constraints on the NSA, no effort is made to discard files openly acknowledged by the NSA itself to be irrelevant. Regarding the quality of this collateral impact, the Washington Post analysis describes it as such:

> Many other files, described as useless by the analysts but nonetheless retained, have a startlingly intimate, even voyeuristic quality. They tell stories of love and heartbreak, illicit sexual liaisons, mental-health crises, political and religious conversions, financial anxieties and disappointed hopes.[3]

The individual profiles themselves specifically included medical records, resumes, childrens' academic transcripts and sensitive pictures described by the Washington Post as "risqué".

---

[1] Tamir Israel, "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation", in Michael Geist, *Ed*., *Law, Privacy & Surveillance in Canada in the Post-Snowden Era*, (Ottawa: University of Ottawa Press, 2015), <http://www.ruor.uottawa.ca/bitstream/10393/32424/1/9780776621838_WEB.pdf>.

[2] Glenn Greenwald & Ewan MacAskill, "Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data", *The Guardian* (11 June 2013), <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>.

[3] Barton Gellman, Julie Tata & Ashkan Soltani, "In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are", *The Washington Post* (5 July 2014), <https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html>.

7. The foreign intelligence framework put in place by FAA2008 – which grants the NSA carte blanche regarding the privacy of foreigners – is starkly at odds with the interconnected nature of our modern digital activities. Canada, it should be noted, is not immune from this paradigm as our own foreign intelligence agency, the Communications Security Establishment (CSE), is granted similar leeway when gathering information of non-Canadians, as are other foreign intelligence agencies around the world. Collectively, this entire paradigm creates significant cross-border challenges for those governments hoping to provide some measure of privacy for their citizens while still finding ways to participate in the global communications infrastructure. Data localization restrictions such as that encoded in BC FIPPA's section 130.1, Nova Scotia's *Personal Information International Disclosure Protection Act*, and Australia's *Personally Controlled Electronic Health Records* Act.

8. Territorial restrictions of this nature are not a 'silver bullet'. They fail to directly address the underlying problem which is the disregard for privacy of foreigners that is at the heart of many foreign intelligence frameworks. Even with data localization measures, foreign intelligence agencies can – and do – reach into foreign territories and compromise data centres remotely. Gaining this type of remote access requires greater practical effort, has accompanying exposure risks and lacks the ease associated with compelling a domestically present company to comply with access orders. Nonetheless, remote access is pervasively employed by foreign intelligence agencies. Moreover, these agencies situate themselves at key points in the global communications network and capture significant amounts of data in transit.

9. On the other hand, territorial restrictions can lead to greater privacy by increasing the difficulty by which foreign intelligence agencies can gain access to such data.[4] Moreover, they can lead to the adoption of stronger privacy protections more generally. For example, concern over foreign intelligence agencies such as the NSA has pushed companies such as Microsoft to develop clouds based in local data centres in several jurisdictions including Canada,[5] India,[6]

[4] See: Heidi Bohaker, Lisa Austin, Andrew Clement & Stephanie Perrin, "Seeing Through the Cloud", (Toronto: CC-BY-NC-CA 2.5, 2015), <http://ecommoutsourcing.ischool.utoronto.ca/final-report/>.
[5] Shane Dingman, "Microsoft to Build Two Data Centres in Canada as it Expands Clound Services", *The Globe and Mail* (2 June 2015), <http://www.theglobeandmail.com/technology/microsoft-to-build-two-data-centres-in-canada-as-it-expands-cloud-services/article24756853/>.
[6] John Ribeiro, "Microsoft Will Offer Locally Hosted Cloud Services in India", *IDG News Service* (30 September 2014), <http://www.pcworld.com/article/2689572/microsoft-will-offer-locally-hosted-cloud-services-in-india.html>.

Germany[7] and Ireland, as well as to seek legal recognition of this data segmentation scheme in United States courts.[8] It has provided the BC government with the incentive and impetus to negotiate enhanced protections such as tokenization schemes with foreign-based cloud computing companies.[9] Notably, it has provided the basis for negotiations between the European Union and the United States with the object of securing better protection of EU citizens within the United States' foreign intelligence framework.[10] These negotiations arose in response to a decision of the Court of Justice of the European Union invalidating the ability of private companies to transfer data to the United States because such companies cannot provide protection against the NSA's excessive foreign intelligence regime.[11] These bilateral EU-US negotiations regarding the need to adopt protections for EU citizen data within the United States foreign intelligence regime only arose out of the EU's data transfer restriction regime.[12]

10. With this general discussion of the potential and limits of data localization as a means of safeguarding domestic data against foreign state agencies in mind, I now turn to a discussion of recent developments in trade frameworks and their potential implications for this data localization regime.

Trade Agreements: Some General Background

11. While earlier waves of trade agreements have had as their primary object the reduction of tariffs as a means of trade liberalization, more recent trade initiatives have begun to address significant elements of domestic regulation in an attempt to harmonize and set specific

[7] Glyn Moody, "Microsoft Building Data Centers in Germany that US Government Can't Touch", *Ars Technica* (12 November 2015), <http://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/>.

[8] *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*, Docket No 14-2985, United States Second Circuit, decision pending.

[9] British Columbia, Information & Privacy Commissioner, Tokenized Data as Personal Information, OIPC File No F13-55076, April 4, 2014. Acknowledging that, as with most obfuscation techniques, much will depend on proper implementation: BC Freedom of Information and Privacy Association, Submission to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*, October 16, 2015, <https://www.leg.bc.ca/content/CommitteeDocuments/40th-parliament/4th-session/foi/presentations/20151016/Presentation-FOI-40-4-BCFIPA.pdf>.

[10] European Commission, "Commission Issues Guidance on Transatlantic Data Transfers and Urges the Swift Establishment of a New Framework Following the Ruling in the Schrems Case", *European Commission – Press Release* (6 November 2015), <http://europa.eu/rapid/press-release_IP-15-6015_en.htm>; and Article 29 Working Party, "Statement of the Article 29 Working Party", (16 October 2015), <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf>.

[11] *Schrems v Facebook Inc*, Case C-362/14 (Court of Justice of the European Union, 2015).

[12] European Commission, "On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU", COM(2013) 847 final, (27 November 2013), <http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf>, Section 7.1 and Recommendations 12-13.

standards.[13] The result of this shift is that impact of trade agreements is no longer primarily economic in nature, and the potential of such agreements to undermine the ability of states to protect their citizens is high. The trend in question has taken hold in earnest with respect to domestic intellectual property laws, and is beginning to encompass a growing range of the digital ecosystem that fall primarily to provincial control under Canada's constitutional scheme. This includes privacy protection, e-commerce transactional protections and neutrality obligations. The trend poses significant issues for democratic legitimacy, as the autonomy granted to the executive branch of the federal government to enter into foreign policy commitments in secret and without meaningful consultation with the public is broad.

12. Where this autonomy was historically limited to negotiating trade quotas and tariffs, the impact of these processes on domestic regulatory policy was more limited. However, trade agreements today include significant and detailed obligations regarding domestic regulatory regimes and this trend is only likely to intensify in the future, meaning that the impact on domestic regulatory regimes such as BC *FIPPA* may be an ongoing process.

13. The shortcomings of the trade process as an instrument of legitimate democratic policy-making are significant. The instruments are negotiated in highly secretive contexts, with substantive texts outside the reach of not only the public and of freedom of information laws, but even of parliamentarians. This creates difficulties in attempts to ensure that the policy outcomes which are ultimately encoded in trade agreements reflect the public interest, as the public is effectively locked out of the policy development stage.

14. Once a trade agreement is completed, it is presented to the public as a *fait accompli*. Increasingly, the obligations undertaken in trade agreements are detailed and specific, allowing for minimal latitude in how these are ultimately encoded in domestic legislation or action. This leaves any *ex post* democratic protections an inadequate safeguard for ensuring balanced public policy. Even without legislative action, trade commitments can have direct impact on domestic policy. Our courts will interpret ambiguities in domestic legislation in a manner that presumes compliance with international commitments such as trade agreements.

[13] See for example: Lawrence Summers, "Rescuing the Free-Trade Deals", *The Washington Post*, June 14, 2015, <https://www.washingtonpost.com/opinions/rescuing-the-free-trade-deals/2015/06/14/f10d82c2-1119-11e5-9726-49d6fa26a8c6_story.html>, Michael J. Trebilcock & Robert Howse, "The Regulation of International Trade", 3rd Edition, (New York: Routledge, 2005), Chapter 12, generally.

15. Even where commitments undertaken in a trade agreement do not make their way into domestic legislation directly, the ability to enforce trade commitments can impose heavy consequences for domestic governments operating regulatory regimes that do not comply with these. There are in essence two types of enforcement mechanisms that have taken root in trade agreements in recent years.

16. The first and more insidious of these is the inclusion of Investor-State Dispute Resolution (ISDS) rights that grant foreign investors the right to sue domestic governments in international tribunals as a means of challenging regulatory actions of those governments. This is a powerful instrument placed in the hands of one set of stakeholders – foreign investors – while ignoring all others. A second, and only somewhat less concerning means of enforcing trade obligations is through the inclusion of bi-lateral Dispute Resolution measures, which allow one state government to sue another over perceived violations of rights.

17. The ambiguous nature of trade language has meant that these dispute resolution mechanisms can sometimes lead to surprising and unpredictable outcomes. For example, in 2005, a World Trade Organization Appellate Body upheld an Antigua and Barbuda lawsuit that emerged from a series of United States laws designed to prevent online gambling. This lawsuit succeeded even though the United States had not intended to make any trade commitments relating to the regulation of gambling at all. The remedy granted to Antigua was the right to violate US Intellectual Property laws in order to recover its annual losses (estimated at $21 million a year) until United States legislatures took steps to address the repudiated gambling regulation.[14]

18. These dispute resolution mechanisms can even be used by foreign governments or investors, as the case may be, to challenge the results of domestic judicial decisions interpreting laws previously thought to be compliant with trade obligations in a manner that negatively impacts the party in question. For example, pharmaceutical company Eli Lilly recently filed a $500 million lawsuit under NAFTA's ISDS regime against the federal government. The lawsuit arose out

[14] Annie Lowrey, "Caribbean Nation Gets an International Go-Ahead to Break US Copyright Laws", *New York Times* (28 January 2013), <http://www.nytimes.com/2013/01/29/business/global/dispute-with-antigua-and-barbuda-threatens-us-copyrights.html>.

of a Supreme Court of Canada decision that evolved patent obligations in a manner designed to prevent patent holders from claiming patent protection over outcomes that are never realized.[15]

19. It is notable that the public interest is not only locked out of the trade commitment development process, but also of the *ex post* judicial development of these commitments. In democracies, lawsuits, class actions and constitutional challenges can be launched by individuals and companies alike. Under the trade regime, it is only companies or states that can initiate such processes. Moreover, whereas in most democracies constitutional restraints exist as an ultimate limit on the impact of regulator action, the highest consideration in the application of trade commitments becomes the overriding need to limit barriers to trade. Collectively, this creates an atmosphere where it is difficult for any 'gold standard' to emerge or prevail. There have already been documented instances in Canada, for example, where the spectre of trade enforcement was used to chill certain public policy initiatives that would have set higher protection standards.[16] In this regard, Eli Lilly's stated justification for challenging Canadian patent law under NAFTA is telling – "... and we're afraid it can lead to other countries attempting to undermine intellectual property."[17] In addition, a country that first adopts a higher standard may have a harder time justifying such a restriction in the manner required by many trade agreement prohibitions.

Recent Trade Commitments & Section 30.1

20. Against this backdrop, data localization rules such as those in British Columbia, Nova Scotia, Australia and India have all been explicitly and increasingly targeted primarily by United States-based information technology industry groups and, as a result, by the United States Trade Representative. This has made data localization a live issue in three major regional agreements. These include the recently concluded Trans-Pacific Partnership Agreement (TPP), its east-coast counterpart, the Transatlantic Trade and Investment Partnership (TTIP), and the global Trade in Services Agreement (TiSA). Each of these agreements includes similar sets of commitments, modified for the particular regional contexts and negotiated outcomes. The

[15] Department of Foreign Affairs, Trade and Development Canada, "NAFTA – Chapter 11 – Investment: Cases Filed Against the Government of Canada", *International.gc.ca*, last modified February 9, 2015 (accessed November 18, 2015), <http://www.international.gc.ca/trade-agreements-accords-commerciaux/topics-domaines/disp-diff/eli.aspx>.
[16] Scott Sinclair, "NAFTA Chapter 11 Investor-State Disputes to January 1, 2015", *Canadian Centre for Policy Alternatives* (14 January 2015), <https://www.policyalternatives.ca/publications/reports/nafta-chapter-11-investor-state-disputes-january-1-2015>.
[17] Ed Silverman, "Eli Lilly vs Canada: The Patent War Moves to Washington", *Wall Street Journal* (14 April 2014), <http://blogs.wsj.com/corporate-intelligence/2014/04/14/eli-lilly-vs-canada-the-patent-war-moves-to-washington/>.

commitments adopted in these agreements are co-extensive, meaning that Canada will be subject to all of these, in addition to its existing commitments under NAFTA, GATT and GATS.

21. The most salient feature of these new agreements is the electronic commerce chapter. This chapter directly addresses privacy generally, as well as data localization laws specifically. The Trans-Pacific Partnership Agreement's (TPP, for short) e-commerce chapter includes explicit data localization restrictions, as does a leaked draft of the Trade in Services Agreement (TiSA or short).

22. While the TPP e-commerce chapter was initially reported as imposing limitations on private and public sector alike, the final version as adopted excludes government procurement and data collection from its scope. This effectively immunizes BC *FIPPA*'s section 30.1. However, the finalized TPP provision is nonetheless instructive, as it may be applied to state action in future agreements. The provision adopts a general prohibition on state attempts to prevent cross-border transfer of information (Article 14.11) and from requiring the local presence of computing facilities (Article 14.13). States can depart from these prohibitions, but only if a rigid justification test is met. This test includes the need to prove that that the restriction in question does not extend further than strictly necessary to achieve a legitimate public policy objective (sub-paragraph 3 (b) of Articles 14.11 and 14.13, respectively).[18] In the context of section 30.1, if the public policy objective is established to be placing barriers on the ability of foreign intelligence agencies to access personal information of Canadians, then the onus will be on the government to demonstrate that the provision does, in fact, achieve this objective. The data localization restriction in TiSA's most recently leaked e-commerce chapter is more restrictive. To begin with, it applies to private and public sector action alike.[19] Moreover, it adopts a categorical prohibition to data localization that brooks no limitation.

23. Both TiSA and the TPP's e-commerce chapters are subject to enforcement through state to state Dispute Resolution. The TPP also includes an Investor-State Dispute Resolution (ISDS) chapter which, in its final iteration, does not apply to the rights granted in its e-commerce chapter. As a result even if an E-commerce chapter's explicit data localization obligations were

[18] Burcu Kilic & Tamir Israel, "Trans-Pacific Partnership E-Commerce Chapter: The Highlights", *Public Citizen & Canadian Internet Policy & Public Interest Clinic (CIPPIC)* (5 November 2015), <https://www.citizen.org/documents/tpp-ecommerce-chapter-analysis.pdf>.
[19] Tamir Israel, "TiSA Annex on Electronic Commerce: A Preliminary Analysis", *Wikileaks.org* (3 June 2015), <https://wikileaks.org/tisa/ecommerce/analysis/Analysis-TiSA-Electronic-Commerce-Annex.pdf>.

applied to the public sector, the Canadian government would not be subject to direct company-initiated lawsuits over section 30.1. However, TPP's ISDS regime does grant foreign investors the right to sue governments over any treatment of domestic investors or to investors of another country that is more favourable, in like circumstances, than that accorded to it. The viability of section 30.1 under this regime will largely turn on what is considered 'like circumstances'. As the TPP ISDS chapter expressly affirms that legitimate public welfare objectives are a factor in determining whether 'like circumstances' exist or not, the government's ability to demonstrate that the distinction drawn by the provision between Canadian-based and foreign data storage is based on real differences between the two will be integral.[20]

24. I will close today with a brief overview of a trade context challenge to a data localization requirement that was decided in the United States, as an illustration of what might be expected if section 30.1 were ever challenged in this way in the future.

25. The United States Government Accountability Office (GAO) has found that data localization restrictions can, under certain conditions be justified in the face of more generalized market access commitments. The decision in question involved a challenge to the United States General Services Administration (GSA) decision to limit its procurement request for a custom cloud service to a specific list of countries, excluding others. GSA explained its justification for this need as such:

> ... GSA has argued that the government has a need to know where its data resides and transits, because when U.S. government data crosses national borders, the governing legal, privacy, and regulatory regimes become ambiguous and raise a variety of concerns including the potential of foreign jurisdictions to assert access rights to U.S. Government data. ... Later, in response to specific questions from our Office, GSA argued that the data center location requirements were not unduly restrictive or unreasonable because ... "[t]o state that data centers can be located anywhere in the world would be irresponsible, given the many factors that must be addressed when considering risk inherent in any IT system."[21]

GSA noted that in order to meet this objective, procurement should be limited to US-based companies alone. However, in response to pressure from the office of the United States Trade Representative, GSA had compromised its security needs in order to permit vendors from a list

[20] Trans-Pacific Partnership Agreement, Chapter 9 – Investment, footnote 14.
[21] *In the Matter of Technosource Information Systems, LLC et al*, B-405296, B-405296.2 & B-405296.3, (United States Government Accountability Office, 2011), <http://www.gao.gov/decisions/bidpro/405296.pdf>.

of 'designated countries' which had entered into trade agreements with the United States. The decision to exclude vendors on this basis was challenged by protest to the GAO. In assessing the protest, the US GAO acknowledged that the GSA had raised legitimate security needs associated with data location. However, it further found that the GSA's delineation between 'designated' and non-designated countries to be arbitrary, noting that "the legal ambiguities and hazards associated with locating data outside the jurisdiction of the United States exist without regard to whether a country is a 'designated country'".[22] GSA was therefore asked to re-issue its procurement document with a clearer explanation for why some non-US locations were permitted while others were denied.

26. The US GAO protest, while arising in a different context, is instructive for how a trade agreement-based challenge to section 30.1 may ultimately unfold. The justification framework under applied by the GAO in its assessment of GSA's localization obligation is less stringent than that found in some current trade proposals – it need only determine whether restrictions placed on procurement are justified as necessary for a legitimate objective. However, it is nonetheless notable that the GAO accepted GSA's justification for localizing procurement to the United States alone. What it did not accept was the arbitrary acceptance of some countries and rejection of others without any factual basis for why concerns are more salient when data is located in some excluded states as opposed to other not excluded states. Along these lines, the importance of a detailed and accurate factual record justifying the localization restriction and its connection to privacy protection will be integral to any defence of section 30.1 in the context of a hypothetical trade dispute in the future.

27. I would just like to close by thanking the committee once again for inviting CIPPIC to testify on this topic. I welcome any questions you may have.

***** END OF DOCUMENT *****

[22] *In the Matter of Technosource Information Systems, LLC et al*, B-405296, B-405296.2 & B-405296.3, (United States Government Accountability Office, 2011), <http://www.gao.gov/decisions/bidpro/405296.pdf>.

USEFUL REFERENCES

Heidi Bohaker, Lisa Austin, Andrew Clement & Stephanie Perrin, "Seeing Through the Cloud", (Toronto: CC-BY-NC-CA 2.5, 2015): <http://ecommoutsourcing.ischool.utoronto.ca/final-report/>

In the Matter of Technosource Information Systems, LLC et al, B-405296, B-405296.2 & B-405296.3, (United States Government Accountability Office, 2011): <http://www.gao.gov/decisions/bidpro/405296.pdf>

Tamir Israel, "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation", in Michael Geist, *Ed*., *Law, Privacy & Surveillance in Canada in the Post-Snowden Era*, (Ottawa: University of Ottawa Press, 2015):
<http://www.ruor.uottawa.ca/bitstream/10393/32424/1/9780776621838_WEB.pdf>

Tamir Israel, "TiSA Annex on Electronic Commerce: A Preliminary Analysis", *Wikileaks.org* (3 June 2015):
<https://wikileaks.org/tisa/ecommerce/analysis/Analysis-TiSA-Electronic-Commerce-Annex.pdf>

Burcu Kilic & Tamir Israel, "Trans-Pacific Partnership E-Commerce Chapter: The Highlights", *Public Citizen & Canadian Internet Policy & Public Interest Clinic (CIPPIC)* (5 November 2015):
<https://www.citizen.org/documents/tpp-ecommerce-chapter-analysis.pdf>.

Scott Sinclair, "NAFTA Chapter 11 Investor-State Disputes to January 1, 2015", *Canadian Centre for Policy Alternatives* (14 January 2015): <https://www.policyalternatives.ca/publications/reports/nafta-chapter-11-investor-state-disputes-january-1-2015>.

Schrems v Facebook Inc, Case C-362/14 (Court of Justice of the European Union, 2015)

Michael J. Trebilcock & Robert Howse, "The Regulation of International Trade", 3rd Edition, (New York: Routledge, 2005)