Fostering Trust and Confidence in Electronic Commerce

Will the EU-Canada Comprehensive Economic and Trade Agreement Really Effect Change?

Nicolas Vermeys*

* Professeur agrégé, Faculté de droit de l'Université de Montréal, Directeur adjoint du Laboratoire de cyberjustice, Codirecteur de la Maîtrise en commerce électronique (UdeM), Chercheur régulier du Centre de rechercherche en droit public et du Regroupement droit, changements et gouvernance, Membre du Comité Réforma sur les modes alternatifs de résolution des conflits.

Fostering Trust and Confidence in Electronic Commerce

Will the EU-Canada Comprehensive Economic and Trade Agreement Really Effect Change?

Nicolas Vermeys

INTRODUCTION

Ever since it was announced, back in October of 2008, that "EU and Canadian Leaders agreed to work together to "define the scope of a deepened economic agreement and to establish the critical points for its successful conclusion, particularly the involvement of Canada's provinces and territories and the EU Member States in areas under their competencies""[1], speculation has run rampant as to what would be enclosed in the eventual document that is today referred to as the Comprehensive Economic and Trade Agreement (or "CETA") and, more importantly, how it could and would affect our rights and liberties. From the privatization of drinking water, to loss of dominion, many nightmarish scenarios were imagined as possible outcomes of the agreement[2], a situation that was reinforced by the relative opacity of ongoing discussions. Even serious commentators who wished to study the actual implications stemming from what were seen by many Canadians as the most important trade negotiations since NAFTA (although they have since been somewhat overshadowed by the Trans-Pacific Partnership[3]), had no other recourse than to

1. See: *Canada-European Union Joint Report: Towards a Comprehensive Economic Agreement*, available at: <http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/eu-ue/can-eu-report-can-ue-rapport.aspx?view=d>
2. See: *Canada-EU Trade Agreement: Opening New Markets in Europe*,, available at: <http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/eu-ue/can-eu.aspx-?view=d> (the page was taken down prior to the publication of this paper).
3. Information on the TPP can be obtained from the *Foreign Affairs, Trade and Development Canada* website, available at: <http://www.international.gc.ca/trade-agreements-accords-commerci-

partly build their arguments around whispers, gossip, and speculation deriving from leaked versions of working copies of the Agreement[4]. That being said, and although it is still too early to know exactly how the CETA will ultimately impact our lives, now that the draft *CETA Consolidated text* (hereinafter: the "*Consolidated text*") has been made public[5], we do know that the agreement does cover a broad array of trade questions, including the one that is to be the focus of this paper: electronic commerce.

Like is the case in other fields covered by the CETA, and even with the *Consolidated text* in hand, it is still too soon to establish how electronic commerce will actually be impacted if and when the final draft of the agreement is eventually ratified by both parties. However, as we explained elsewhere[6], electronic commerce specialists remain in a far better position than those in other fields to predict the CETA's true impact with regards to their topic of interest. This claim is not due to an uncanny gift of foresight, but rather to the fact that electronic commerce negotiations between Canada and the European Union have been ongoing since 1999[7], and have consistently focused on three main issues: Privacy, information security, and consumer protection[8]. Furthermore, positions on how these issues should be addressed have been the product of consensus between those involved since the very beginning[9]. Therefore, logic dictates that since the CETA chapter regarding electronic commerce (which is said to have been agreed upon back in March of 2011[10]) has not strayed far from these and other positions that have been universally held for over twelve years, the CETA's influence on the field should be minimal.

aux/agr-acc/tpp-ptp/index.aspx?lang=eng>

4. The last leaked version, which is similar to the official *Consolidated text*, is available on the Tagesschau website: <http://www.tagesschau.de/wirtschaft/ceta-dokument-101.pdf>
5. See: <http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/toc-tdm.aspx?lang=eng>
6. Nanette Neuwhal, and Nicolas Vermeys, "The EU-Canada Comprehensive Economic and Trade Agreement and E-Commerce", in Finn Laursen (ed.), *The EU and the Political Economy of Transatlantic Relations*, Bruxelles, P.I.E. Peter Lang, 2012, p. 147.
7. See *European Union - Canada Joint Statement: Electronic Commerce in the Global Information Society*, available at: <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00386.html> (hereinafter: the "1999 Joint Statement").
8. *Id.* See also: *Electronic Commerce in the Global Information Society – EU-Canada Work Plan 2000/2001: Privacy, Security and Consumer Protection*, available at: <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/er/09549en-communiqu%C3%A9.htm#_Toc486671336> (hereinafter: the "2000-2001 Work Plan").
9. *Id.*
10. Canadian Conference of the Arts, "An alliterated update: CRTC, C-470 and CETA", (2001) 10/11 *CCA Bulletin*, available at: <http://ccarts.ca/resources/federal-policies-investments/an-alliterated-update-crtc-c-470-and-ceta/>

For example, as indicated in the *Consolidated text*, the main reason for incorporating electronic commerce within the CETA is to promote its development between Canada and the EU[11], a goal that is closely linked to the parties' ability to foster "trust and confidence in electronic commerce"[12]. This goal seems coherent with previous discussions such as those that led to the 1999 European Union – Canada joint statement titled *Electronic Commerce in the Global Information Society*[13] in which both parties agreed to "actively work in concert with the private sector, civil society and international organisations to […] [p]romote trust and confidence in the global marketplace"[14].

Within this context, how will the CETA effect change or, rather, how will it be able to reach its goal to further promote electronic commerce when it seems to simply reiterate previous bilateral agreements and promises? In order to eventually answer these questions, one first needs to study why EU and Canadian authorities deem it necessary to foster trust and confidence in electronic commerce (I), and what measures they have – and hope to – put into place to effectively do so (II). It should be specified that, while the CETA aims to address both business-to-business (B2B) and business-to-consumer (B2C) electronic commerce, our focus will mostly be put on B2C online transactions.

1. Identified risks stemming from electronic commerce

Section 1 of article X-05 of the *Consolidated text*'s chapter on electronic commerce states that the parties "agree to maintain a dialogue on issues raised by electronic commerce, which will *inter alia* address […] the protection of personal information and the protection of consumers and businesses from fraudulent and deceptive commercial practices in the sphere of electronic commerce". This seems like an obvious focal point for any agreement as these two issues were raised before in a 2008 joint study[15], and have been pointed to by numerous authors[16] as the two

11. Article X-01, paragraph 1, of the chapter on electronic commerce.
12. Article X-03 of the chapter on electronic commerce.
13. Available at: <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00386.html>
14. *Id.*
15. European Commission and Government of Canada, "Assessing the costs and benefits of a closer EU – Canada economic partnership, A Joint Study by the European Commission and the Government of Canada", (2008), p. 71, available at: <http://trade.ec.europa.eu/doclib/docs/2008/october/tradoc_141032.pdf> (hereinafter: the "2008 Joint Study").
16. See, for example, Cynthia Chassigneux, "La confiance, instrument de régulation des environ-

major hurdles to fostering consumer confidence in electronic commerce. However, as we will now demonstrate, these same issues have been the focus of many legislative efforts on both national and international levels. It therefore becomes a question of envisioning how the CETA will be applied in order to reinforce current legislation and agreements to improve their effectiveness.

1.1. Privacy issues

The *Consolidated text* submits that "[e]ach Party should adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce and, when doing so, shall take into due consideration international standards for data protection of relevant international organisations of which both Parties are a member"[17]. If left unchanged, this undertaking would simply serve as a restatement of the position held in the 1999 Joint Statement where it was agreed that "EU and Canada consider that legislative frameworks for the protection of privacy and personal information are a vital component of electronic commerce strategy and beneficial to the evolution of an information society"[18].

Of course, much has happened between 1999 and 2015, and both parties have since honoured their commitment. Europe acted first, as its *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* actually predates the Joint Statement (as well as the rise of the Internet). Although already evident to most observers[19], the fact that said Directive was applicable to electronic commerce was officially confirmed in 2002 with the adoption of *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*.

Meanwhile, Canada enacted its own privacy legislation in 2001 with the ascension into law of *An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments*

nements électroniques", (2007) 37 *R.D.U.S.* 441.

17. Article X-03 of the chapter on electronic commerce.

18. 1999 Joint Statement, prec., note 7.

19. See, for example, Cynthia Chassigneux, *Vie privée et commerce électronique*, Montreal, Themis, 2004, p. 120.

Act and the Statute Revision Act[20], (better know under its short title, the *Personal Information Protection and Electronic Documents Act* or PIPEDA). As is common knowledge in the privacy community, the Commission of the European Communities has judged that PIPEDA offers an "adequate level of protection for personal data"[21], meaning that it recognises that Canadian privacy regulation offers acceptable protection for personal information, therefore implying that Europe considers that Canada has upheld its obligations under the 1999 Joint Statement.

As for the second part of the quoted section of the *Consolidated text*, the notion that parties should "take into due consideration international standards for data protection of relevant international organisations of which both Parties are a member" [22], it too is nothing but a reassertion of the 1999 Joint Statement's mention that "[i]nternationally, EU and Canada will support a standards-based approach to complement national frameworks"[23], as well as the 2000-2001 work plan's agreement to promote "a compatible standards-based approach to complement national frameworks"[24]. Furthermore, since the 2008 Study revealed that "[t]he EU and Canada also continue to address electronic commerce in multilateral fora (i.e. OECD, WIPO, WTO)"[25], the pertinence of reasserting the need to consider international standards is somewhat debatable since it will mainly serve to ensure that the parties continue their current practices and keep taking part in OECD, WIPO and WTO negotiations.

This last statement could, in our opinion, be applied to the CETA's overall suggestion that the parties "adopt or maintain laws, regulations or administrative measures for the protection of personal information of users engaged in electronic commerce"[26], as adopting laws is no longer an issue. Admittedly, maintaining laws into place remains relevant, but since local consumer protection groups and organisations have as much stake in a legislative *status quo* as do international partners, we doubt that repealing such laws would be an option even without international

20. SC 2000, c 5 (hereinafter: "PIPEDA").
21. *Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act*, C(2001) 4539. It should be noted, however, that a recent decision (*Schrems* v *Data Protection Commissioner*, Case C362/14 of the European Court of Justice) could bring said recognition into question for any member country where a complaint is registered (see paragraph 66 of the decision).
22. Article X-03 of the chapter on electronic commerce.
23. 1999 Joint Statement, prec., note 7.
24. 2000-2001 Work Plan, prec., note 8.
25. 2008 Joint Study, p. 171, prec., note 15.
26. Article X-03 of the chapter on electronic commerce.

involvement. In fact, both the EU and Canada have since adopted more aggressive privacy protection rules[27]. Furthermore, to use the "dog's bark is worse than his bite" analogy, one could say that the CETA, like previous agreements and laws, is concentrating on bark while offering very little bite. In Canada, consumer privacy is very well protected by both federal and provincial legislation. On top of PIPEDA, provincial legislators are free to implement "substantially similar" laws[28] to govern private data circulating inside the province. This has been done by British Columbia[29], Alberta[30], Quebec[31] and, to a lesser extent, Ontario[32], New Brunswick[33], and Newfoundland and Labrador[34] (only with regards to health information). Quebec, for example, has adopted its *Act respecting the Protection of personal information in the private sector*, as well as dispositions protecting privacy both online and offline in the *Civil Code*[35], the *Act to Establish a Legal Framework for Information Technology*[36] and, of course, the Quebec Charter[3738]. This only goes to reinforce our position that the current legislative framework governing private data with regards to electronic commerce is more than sufficient. Some authors and commentators have even suggested that said framework has become too complex and difficult to navigate through when it relates to e-commerce, notably for most small businesses, making its effectiveness debatable[39]. As one analyst puts it, such a risk does exist:

27. On June 18th, 2015, *An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act* (2015, c. 32) received royal assent in Canada, while the 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/2012/011 is expected to come into force in 2016.
28. PIPEDA, prec., note 20, Section 26.
29. *Personal Information Protection Act*, SBC 2003, c 63.
30. *Personal Information Protection Act Regulation*, Alta Reg 366/2003.
31. *An Act respecting the Protection of personal information in the private sector*, CQLR c P-39.1.
32. *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A.
33. *Personal Health Information Privacy and Access Act*, S.N.B. 2009, c. P-7.05.
34. *Personal Health Information Act*, SNL 2008, c P-7.01.
35. LRQ, c C-1991.
36. CQLR c C-1.1.
37. *Charter of human rights and freedoms*, CQLR c C-12.
38. It should be noted, however, that these laws were drafted before PIPEDA came into force, and not as a reaction to it or to the 1995 European Directive. In fact, both the *Act respecting the Protection of personal information in the private sector* and the *Civil Code* came into force in 1994, while the *Act to Establish a Legal Framework for Information Technology* came into effect in 2001, as an answer to electric commerce legislation in the US and Europe as well as the UNCITRAL 1996 *Model Law on Electronic Commerce*.
39. On this general issue, see Pierre Trudel, «La protection de la vie privée dans les réseaux : des paradigmes alarmistes aux garanties effectives», (2006) 61 *Annales des télécommunications* 950.

> "an overly burdensome and prohibitive set of privacy laws would almost surely prove too cumbersome for effective e-commerce, and "would lessen or even remove the convenience aspect from Web-based transactions." […] "[t]he ability to collect PII from e-consumers allows this ever expanding economic sector to operate efficiently; serious restrictions on the ability to collect this information is akin to removing a plant from sunlight—e-commerce, as it exists today, would inevitably wither and die.""[40]

This being said, and while we agree with the basic claim that too much legislation may become detrimental to commerce, an overprotective legislature should not have a negative impact on consumers' confidence, although it does seem incompatible with the CETA's goal of "facilitating the use of electronic commerce by small and medium sized enterprises"[41]. A problem that is more germane to fostering trust on the consumer's side in an electronic commerce context is not the overabundance of laws, but rather the lack of enforcement of applicable privacy legislation. As explained by Canada's former Privacy Commissioner:

> "Unlike most other major jurisdictions now, Canada has no major sanctions for those who don't follow its commercial privacy law. I hope that when the second five-year review of PIPEDA will be undertaken by Parliament this issue could be discussed. I believe companies take notice—and I'm talking about very large international companies that operate on a very large scale—when they are subject to major fines or some kind of enforcement action. We have very limited power in that regard, and I believe that more respect would be shown to Canada's laws if we did have that power."[42]

Furthermore, this problem has been made worse by the fact that federal and provincial privacy watchdogs have effectively been neutered by lack of proper funding[43].

As for consumers' direct recourse against those who would misuse their private data online, the relatively low value associated to personal information by Canadian courts does not serve as a strong deterrent to corporations[44]. In fact, court costs

40. Jake Spratt, "An Economic Argument for Electronic Privacy", (2011) 7 *Journal of Law and Policy for the Information Society*, available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1831905> (References omitted).

41. Article X-04 (c) of the chapter on electronic commerce.

42. Jennifer Stoddart, Presentation to the Standing Committee on Access to Information, Privacy and Ethics, Tuesday, May 29, 2012, available at: <http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&Parl=41&Ses=1&DocId=5616948&File=0>

43. See France Houle and Lorne Sussin, "Powers and Functions of the Ombudsman in the Personal Information Protection and Electronic Documents Act: An Effectiveness Study", Research commissioned by the Office of the Privacy Commissioner of Canada, 2010, p. 165.

44. Fines are usually limited to a few thousand dollars. See Karl Delwaide and Antoine Aylwin, *Leçons tirées de dix ans d'expérience : la Loi sur la protection des renseignements personnels dans le secteur privé du Québec*, Ottawa, Commissaire à la protection de la vie privée du Canada, 2005,

and lawyer fees are often superior to possible claims[45], making legislative efforts to comply with international agreements, including the CETA, somewhat theoretical.

1.2. Fraudulent and deceptive commercial practices

As with privacy issues, "the protection of consumers and businesses from fraudulent and deceptive commercial practices in the sphere of electronic commerce"[46] is also mentioned in the *Consolidated text* as an issue that the parties need to address. This raises an important question regarding what qualifies as a fraudulent and deceptive commercial practice in the sphere of electronic commerce, and how said sphere is different than the more general area of commerce (electronic or otherwise). In other words, what makes fraudulent and deceptive commercial practices in the sphere of electronic commerce so unique as to necessitate specific dispositions in international documents such as the CETA? If one accepts that electronic commerce is, first and foremost, commerce, then fraudulent and deceptive commercial practices in the field of electronic commerce should obey the same rules and regulations as other commercial trade practices. In this sense, a broader statement similar to the opening paragraph of the preamble to the OECD's *Guidelines for Consumer Protection in the Context of Electronic Commerce*[47] seems more appropriate:

> "Consumer laws, policies and practices limit fraudulent, misleading and unfair commercial conduct. Such protections are indispensable in building consumer confidence and establishing a more balanced relationship between businesses and consumers in commercial transactions".

In Canada, it is important to mention that, following section 92 of the Constitution[48], drafting consumer legislation falls under the provincial government's authority and, in such, legislation varies from one province to the next. Therefore, although all provinces and territories do have a Consumer Protection Act or equivalent piece of legislation[49] that indeed limits fraudulent and deceptive commer-

p. 165. It must however be noted that there are important exceptions to this rule, as in *Veilleux* v. *Compagnie d'assurance-vie Penncorp*, 2008 QCCA 257, where the Quebec Court of Appeal awarded $125 000 in damages for privacy violations.

45. See Pierre-Claude Lafond, *L'accès à la justice civile au Québec – Portrait général*, Cowansville, Yvon Blais, 2012, p. 50 and ss.

46. Article X-05 (1) (d) of the chapter on electronic commerce.

47. Said paragraph reads: "Consumer laws, policies and practices limit fraudulent, misleading and unfair commercial conduct. Such protections are indispensable in building consumer confidence and establishing a more balanced relationship between businesses and consumers in commercial transactions".

48. *The Constitution Act*, 1867, 30 & 31 Vict, c 3.

49. Alberta: *Fair Trading Act*, RSA 2000, c F-2; British Columbia: *Business Practices and Consumer Protection Act*, SBC 2004, c 2; Manitoba: *Consumer Protection Act*, CCSM c C200 ; Newfoundland and Labrador: *Consumer Protection and Business Practices Act*, SNL 2009, c C-31.1; Northwest Territories: *Consumer Protection Act*, RSNWT 1988, c C-17 ; Nova Scotia: *Consumer Pro-*

cial practices both on and offline, these pieces of legislation do not always address the problem in the same manner. As we shall see, this problem has however been somewhat lessened by efforts to harmonize current legislation. That being said, and getting back to our initial statement that fraudulent and deceptive commercial practices in the field of electronic commerce should obey the same rules and regulations as other commercial trade practices, we do acknowledge that the cross-border nature of the online environment makes it more difficult to control said practices and, therefore, that laws should be adapted to better reflect this reality.

This is why the *Consumer Measures Committee*, a committee of officials established under article 809 of the *Agreement on Internal Trade*[50] that "provides a federal-provincial-territorial (FPT) forum for national cooperation to improve the marketplace for Canadian consumers, through harmonization of laws, regulations and practices and through actions to raise public awareness"[51], took upon itself to draft best practices for B2C e-commerce. This document, titled *Internet Sales Contract Harmonization Template*[52], offers strict guidelines that online merchants should follow regarding consumer information, cancellation policies, and chargeback possibilities. Some provinces have already chosen to incorporate sections of the Template into their existing consumer legislation[53]. This is the case, for example, in Ontario, where the Template has inspired the drafting of sections 37 through 40 of the *Consumer Protection Act*, a chapter aimed at regulating "electronic conventions". Quebec has also chosen to adapt the Template to its needs, and to incorporate its principles into its *Consumer Protection Act*[54]. However, unlike his Ontarian counterpart, the Quebec legislator opted to extend the Template's reach to all "distance contracts", not only those concluded online, giving credence to our initial point that fraudulent and

tection Act, RSNS 1989, c 92; Nunavut: *Consumer Protection Act*, RSNWT (Nu) 1988, c C-17 ; Ontario : *Consumer Protection Act*, 2002, SO 2002, c 30, Sch A ; Prince Edward Island: *Consumer Protection Act*, RSPEI 1988, c C-19; Quebec: *Consumer Protection Act*, CQLR c P-40.1; Saskatchewan: *The Consumer Protection Act*, SS 1996, c C-30.1 ; Yukon: *Consumers Protection Act*, RSY 2002, c 40.

50. *Agreement on Internal Trade*, Consolidated Version, 2012, available at: <http://www.ait-aci.ca/en/ait/ait_en.pdf>

51. Consumer Measures Committee, "About the CMC", (2011) available at: <http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/h_fe00013.html>

52. Consumer Measures Committee, *Internet Sales Contract Harmonization Template*, May 29th, 2001, available at: <http://cmcweb.ca/eic/site/cmc-cmc.nsf/vwapj/Sales_Template.pdf/$file/Sales_Template.pdf>

53. Alberta, for example, has adopted the *Internet Sales Contract Regulation*, Alta Reg 81/2001, which is a restatement of the Template.

54. Nicole L'Heureux and Marc Lacoursière, *Droit de la* consommation, 6th ed., Cowansville, Yvon Blais, 2011, p. 139 and ss.

deceptive commercial practices in the field of electronic commerce should obey the same rules and regulations as other commercial trade practices[55].

Two important principles reside at the centre of the Quebec Act as modified to reflect the *Internet Contract Harmonization Template*. The first is the merchant's obligation to disclose a series of information about his business (name, address, telephone number, etc.), as well as information about the transaction (exact amount to be paid, delivery method and costs, etc.)[56]. Such transparency makes it more difficult to defraud the buyer. Furthermore, should this information be lacking or false, the consumer can always cancel the contract and demand a refund[57]. If the merchant refuses to refund the consumer, the second principle residing at the core of the new sections comes into play: the chargeback option[58]. This allows the consumer to request a refund from his or her credit card company should he or she be the victim of a fraudulent merchant. This mechanism also exists in other provinces, making it relatively easy for victims of deceptive or fraudulent merchants to get redress. It should also be pointed out that private online escrow services such as Paypal offer similar chargeback options to their customers, therefore enhancing the safety of online purchases made through such intermediaries.

Canadian legislation thus already protects consumers against fraudulent and deceptive commercial practices[59]. Furthermore, as we just saw, most provinces have adapted their consumer protection laws to incorporate some if not all of the changes suggested by the *Internet Sales Contract Harmonization Template*, making them better adapted to curtail these practices in an online environment.

As for European consumers, they too benefit from legislative solutions to fraudulent and deceptive commercial practices. Said solutions are the result of *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain*

55. It should be noted, however, that the current phrasing of sections 54.1 and ss. of the Act makes it difficult to apply said sections to telephone or mail-order contracts. See: Vincent Gautrais and Adriane Porcin, "Les 7 péchés de la L.p.c. : actions et omissions applicables au commerce électronique", (2009) 43 *R.J.T.* 559, 567 and ss. In this sense, British-Columbia, which has also adapted the Template to cover all distance sales contracts, has taken a more pragmatic approach since it does make a distinction between distance sales contracts in electronic forms and other distance sales contracts. See section 47 of the British-Columbia *Business Practices and Consumer Protection Act*.
56. Section 54.1 of the Act.
57. Section 54.8 of the Act.
58. Section 54.14 of the Act.
59. It should be added that, on top of provincial statutes, the federal *Competition Act* (RSC 1985, c C-34) also offers safeguards for consumers.

legal aspects of information society services, in particular electronic commerce, in the Internal Market ("*Directive on electronic commerce*"), and *Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts*, the later of which was recently replaced by *Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council*.

These directives offer consumers similar protective measures as those outlined in the *Internet Sales Contract Harmonization Template* such as consumer information[60], and right of withdrawal[61]. As is the case in Quebec, *Directive 2011/83/EU* has a wide scope that covers consumer rights with regards to all contracts, not making any distinction between online and offline transactions, except for the moment when certain information is to be made available to a given consumer:

> "If a distance contract to be concluded by electronic means places the consumer under an obligation to pay, the trader shall make the consumer aware in a clear and prominent manner, and directly before the consumer places his order, of the information provided for in points (a), (e), (o) and (p) of Article 6(1)." [62]

The information referred to relates to the identification of the goods, the total cost of the transaction, as well as the duration of the contract. Therefore, e-consumers dealing with European online merchants should have enough information to make informed decisions and, should they have issues with getting their goods or with the quality of said goods, they will have the opportunity to withdraw from the contract. All this points to European member state legislation offering sufficient protection to consumers[63].

This goes to show that legislative measures have already been taken on both sides of the Atlantic to ensure that consumers are properly protected from fraudulent and deceptive commercial practices in the sphere of electronic commerce (as in other spheres) and that, although legislators need to stay vigilant to adapt to changing practices and technologies, the CETA should have little impact on the current legis-

60. *Directive 2011/83/EU*, article 8 (2.).

61. *Id.*, article 9.

62. *Id.*, article 8 (2.).

63. It should be pointed out that, according to article 28 of *Directive 2011/83/EU*, member states had until December 13th, 2013 to adopt "the laws, regulations and administrative provisions necessary to comply with this Directive".

lative framework. This implies that the parties agreeing "to maintain a dialogue on issues raised by electronic commerce, which will *inter alia* address […] the protection of personal information and the protection of consumers and businesses from fraudulent and deceptive commercial practices in the sphere of electronic commerce"[64] does not modify current practices, but it does ensure that Canadian and European legislators will indeed continue to monitor how changes in e-commerce affect consumers and will cooperate in addressing these changes. In this sense, although the CETA doesn't create any new obligations, it does strengthen a continued partnership.

* * *

Although privacy and fraudulent and deceptive commercial practices are presented as two distinct concerns stemming from electronic commerce, these issues can come to be intertwined in certain areas. For example, unsolicited electronic commercial communications (spam), another issue raised and addressed by the *Consolidated text* as well as previous joint studies[65] and statements[66] is considered a fraudulent and deceptive commercial practice under both Canadian law[67] and European Conventions[68]. However, since this practice uses private or professional email addresses, which can be considered to be personal information[69], they also raise questions regarding privacy. That being said, as both Canada and the EU have already adopted spam legislation[70], this serves as another example of an area where the CETA's guidelines will have little impact on current practices.

Therefore, to summarize part I of this paper, we believe that the CETA's framework, since it follows long-standing trends in EU-Canada negotiations, will have a limited impact on legislative efforts regarding privacy issues as well as fraudulent and deceptive commercial practices.

64. Article X-05 (1) of the chapter on electronic commerce.

65. See, for example, the 2008 Joint Study, prec., note 15.

66. *Id.*, p. 103.

67. *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23.

68. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on privacy and electronic communications).

69. Regarding private email addresses, see for example *Job Seeker Not Adequately Informed about Purpose of Personal Information Collection*, 2012 CanLII 31194 (PCC), par. 5. Regarding commercial email addresses, see Office of the Privacy Commissioner of Canada, "Legal information related to PIPEDA", (2011), available at: <http://www.priv.gc.ca/leg_c/interpretations_02_e.asp#_ftn3>

70. See footnotes 67 and 68.

2. Proposed solutions to foster "trust and confidence in electronic commerce" under the CETA

Stating that parties need to work towards "the protection of personal information and the protection of consumers […] from fraudulent and deceptive commercial practices in the sphere of electronic commerce"[71] is one thing, but implementing pragmatic solutions, whether legal or otherwise, to better encompass said practices is quite another. As alluded to in the first section of this paper, good intentions, even when made into law, can only be successfully implemented when supported by an appropriate framework of safeguards and corrective measures. In this sense, the CETA's scope – as it relates to electronic commerce – is somewhat underwhelming since it only offers draft guidelines regarding illegal practices. For these guidelines to be effective, they need to be followed by the adoption of pre-emptive (A) and corrective (B) measures that can ensure a more secure online environment.

2.1. Pre-emptive solutions

According to the *Consolidated text*, parties agree to work together to promote "the recognition of certificates of electronic signatures issued to the public and the facilitation of cross-border certification services"[72]. The first part of the statement, recognising electronic signature certificates, seems to be a valid undertaking since "[a] large problem encountered by electronic signature technology is the lack of international, and even domestic, uniformity in legislative standards required to give legal effect to electronic signatures"[73]. Furthermore, as with other areas of the CETA electronic commerce chapter, this goal is a reiteration of previous joint efforts[74].

According to the Canadian legislator, electronic signature "means a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document"[75], while in Europe an electronic signature "means data in electronic form which are attached to or logically associated with other electronic data and which serve as a

71. Article X-05 (1) (d) of the chapter on electronic commerce.
72. Article X-05 (1) (a) of the chapter on electronic commerce.
73. Andra Leigh Nenstiel, "Online Dispute Resolution: A Canada-United States Initiative", (2006) 32 *Can.-U.S. L.J.* 313, 318, quoting William Krause, "Do You Want to Step Outside? An Overview of Online Alternative Dispute Resolution", 19 *J. Marshall J. Computer & Info. L.* 457, 496-471.
74. See the 1999 Joint Statement and the 2008 Joint Study, which both state that "The EU and Canada agreed on the need to develop policies to facilitate the use of authentification [sic] technologies and to implement secure electronic commerce activities".
75. PIPEDA, prec., note 20, section 31.

method of authentication"[76]. Stating that the parties will work together towards "the recognition of certificates of electronic signatures issued to the public and the facilitation of cross-border certification services"[77], therefore seems like a worthwhile endeavour since these two definitions of "electronic signature" are not identical and, since an effort will eventually need to be made to unify them. This could be done by one party agreeing to the other's definition, but could also involve the adoption of a new definition such as the one proposed in the 2001 *UNCITRAL Model Law on Electronic Signatures*, wherein an electronic signature "means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message"[78]. Of course, since neither Canada nor any EU member state has chosen to enact said model law as of these writings, this seems to be a somewhat improbable choice.

As for the definition of a certificate, as Canada's PIPEDA doesn't offer one[79], the EU's definition, i.e. "an electronic attestation which links signature-verification data to a person and confirms the identity of that person"[80], could serve as a starting point for negotiations. Again, the parties could also choose to adopt a new definition based on the UNCITRAL's Model Law: "a data message or other record confirming the link between a signatory and signature creation data"[81].

That being said, if this is an area where one could submit that CETA negotiations are useful – prior agreements having yet to be acted upon – we submit that lack of recognition of certificates of electronic signature currently has little to no impact on the development of electronic commerce between Canada and the EU (or anywhere else in the world for that matter). Means of identifying a co-contractor and verifying his or her intent online have been sought since the birth of the Internet, hence the need to define what could be construed as an electronic signature[82]. However, although the definitions referred to above were made to cover a wide array of processes and acts, electronic signatures will, more often than not, be associated with digital signatures, i.e., "a means of verifying and authenticating a document by ha-

76. *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*, article 2.
77. Article X-05 (1) (a) of the chapter on electronic commerce.
78. Article 2 of the Model Law.
79. It should be noted, however, that Quebec's *Act to Establish a Legal Framework for Information Technology* offers certification guidelines. See sections 47 through 62 of the Act.
80. *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*, article 2.
81. Article 2 of the Model Law.
82. On this issue, see Jean-François Blanchette, "Burdens of Proof", Cambridge, MIT Press, 2012.

ving a computer create a unique identifier through the application of encryption or encoding"[83]. Therefore, while all digital signatures are electronic signatures, all electronic signatures are not necessarily digital signatures, notwithstanding the fact that both terms are often viewed as being interchangeable. The distinction is nevertheless an important one since, while electronic signatures are widespread and commonly used, digital signatures are not; that is to say that their use is often limited to official documents such as notarised papers[84]. Although digital signatures could be used to foster trust in electronic commerce, and although some legislators have favoured their use in this sector[85], the technology has yet to truly be implemented by those who buy and sell online. For consumers, digital signatures are seen as an unnecessary and somewhat complicated step that is not justified considering the low stakes of most online purchases. While it arguably offers stronger security, a digital signature also implies a process that is longer than using a username and password, meaning that it might repel consumers instead of drawing them in. In other words, true digital signatures are currently ill adapted for B2C electronic commerce.

Since the *Consolidated text* refers to electronic and not digital signatures, and since we made it clear that electronic signatures are not limited to digital signatures, one might ask why we would then claim that "the recognition of certificates of electronic signatures issued to the public and the facilitation of cross-border certification services"[86] will not help develop Canada-EU electronic commerce while only using arguments linked to digital signatures. The reason is simple. Third party generated certificates of electronic signature, while not necessarily linked to digital signatures, are rarely used in other contexts. When they are, they stem from already trusted third parties such as credit card companies that do not need government recognition to generate trust and confidence. In other words, if certificates are linked to digital signatures, it is our belief that their recognition will have little impact on B2C electronic commerce since online merchants are not using this technology in such a context; if they are linked to other types of electronic signatures, state recognition will have much less impact than brand recognition. Consumers do not eat at McDonald's or Burger King because their beef is USDA inspected, but rather because of their track record and advertising campaigns.

83. Mark Lewis, "Digital Signatures: Meeting the Traditional Requirements Electronically", (2002) 2 *Asper Rev. Int'l Bus. & Trade L.* 63, 69. For further definitions, see Barry Sookman, *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions*, Toronto, Carswell, 2005, pp. 117-120.

84. See, for example, <https://www.notarius.com/home/index.dot?com.dotmarketing.htmlpage.language=1>

85. See, for example, *Utah Digital Signature Act*, *Utah Code* §§ 46-3-101 to 46-3-504. Enacted by L. 1995, ch. 61.

86. Article X-05 (1) (a) of the chapter on electronic commerce.

Although not directly referred to in the *Consolidated text*, a commonly invoked tool to foster trust and confidence in electronic commerce is the use of trustmarks. As one author explains:

> "Trustmarks are roughly equivalent to a seal of approval, created by independent organizations and displayed on the webpage of online businesses for the purposes of creating trust and confidence in the business, thereby encouraging online transactions. In order to display the trustmark, businesses must agree to commit to certain codes of conduct for the prevention and resolution of disputes, as created by the trustmark organization. Guidelines often require businesses to adhere to best marketing practices and provide easy access to information including cancellation and refund policies, privacy practices, and complaint and dispute resolution procedures. Some trustmarks require businesses to participate in ODR for the resolution of any disputes through the use of specified private providers. It is then up to the trustmark organization to police and regulate the member businesses to ensure compliance with the guidelines. By ensuring potential business partners easy access to dispute resolution services and installing trust and confidence in a particular online business through established dispute prevention procedures, a trustmark encourages the use of internet transactions."[87]

Trustmarks have been around since the very beginning of the Internet[88] and, while they have their detractors[89], established SSL (secure socket layer) seals such as "Norton Secured" or trust seals such as "McAfee Secure" or "TRUSTe Certified Privacy" do seem to generate trust among consumers[90]. As Ethan Katsh and Janet Rifkin explain:

> "Building trust online involves providing information to customers that tells them something about the party they are dealing with. The value of a seal or trustmark […] is that a third party is providing information about the website owner […] Trust comes, therefore, from information on the third party's site and the reputation of the third party"[91].

87. A. L. Nenstiel, prec., note 73, 317.
88. For more on the subject, see Bernard Brun, "Nature et impacts juridiques de la certification dans le commerce électronique sur Internet", (2001) 7-1 *Lex electronica*, available at: <http://www.lex-electronica.org/fr/resumes_complets/147.html>
89. See, for example, Tom Fox-Brewster, "TRUSTe fined $200,000 for misleading web security seal", (2014) *The Guardian*, available at: <http://www.theguardian.com/technology/2014/nov/18/truste-fine-web-security-seals>
90. See Christian Holst, "Which Site Seal do People Trust the Most? (2013 Survey Results)", (2013) *Baymark Institute*, available at: <http://baymard.com/blog/site-seal-trust>
91. Ethan Katsh and Janet Rifkin, *Online Dispute Resolution: Resolving Conflicts in Cyberspace*, San Francisco, Jossey-Bass, 2001, p. 87.

This suggests, as with certificates, that government recognition of a given seal or trustmark will not have as much impact on its perceived value as brand recognition or the overall reputation of the organisation granting a seal. As demonstrated by a recent survey, the most trusted seals also happen to be those with the most recognized logos, themselves belonging to the most established companies[92]. In the same sense, well-established websites such as Amazon garner more trust than arguably more secure sites, mostly because of brand recognition[93]. If the CETA, in its goal to "facilitat[e] the use of electronic commerce by small and medium sized enterprises"[94], cannot affect the spread of private seals or brand recognition of said enterprises' wares among consumers, a CETA trustmark, i.e. a trustmark stating that a given website obeys the laws of Canada and of EU countries, could be a viable option to foster trust and confidence in these websites.

2.2. Corrective solutions

Notwithstanding what we exposed in the first half of this paper, fostering trust and confidence in electronic commerce will ultimately come down to whether or not those who take part in online transaction feel that they can get redress should their co-contractor not fulfill their obligations. This is not to say that privacy and fraudulent and deceptive commercial practices bare no impact on whether consumers will chose to purchase goods and services from an online merchant, but rather that said impact is not necessarily as important as those in the legal community might expect.

Studies show that consumers often undervalue their privacy and will seldom give a second thought to sharing personal information if this allows them to save on the purchase price of a given item[95]. Furthermore, since the nature and reach of the security measures put into place by a corporation to protect said data are rarely shared or discussed, consumers don't really know if company A exposes their personal information to higher risks than company B[96]. Finally, since consumers share their personal information with numerous third parties (webmail services,

92. C. Holst, prec., note 90.

93. See <http://marketresearchexpert.co.uk/2012/02/16/top-10-most-trusted-websites-in-the-uk/> (the page was taken down prior to the publication of this paper).

94. Article X-04 (c) of the chapter on electronic commerce.

95. See, for example, Raj Samani, "How Much do you Value your Personal Data?", (2012) *The Telegraph*, available at: <http://www.telegraph.co.uk/technology/internet-security/9605078/How-much-do-you-value-your-personal-data.html>

96. On the means companies need to adopt to secure information, See Nicolas W. Vermeys, *Responsabilité civile et sécurité informationnelle*, Cowansville, Yvon Blais, 2010.

social networks, Internet service providers, financial institutions, online merchants, etc.), it becomes difficult, if not simply unfeasible, to establish which organisation's possible security breach could be responsible for our private data being accessed and used by a malevolent third party. To help resolve this issue, certain states have enacted security breach notification laws under which corporations that have been the victim of computer attacks or other types of events resulting in the loss of personal information have a duty to inform their costumers[97] and/or the authorities. For example, section 34.1 of Alberta's *Personal Information Protection Act*[98] states that:

> An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

Although Alberta is the only Canadian province to have adopted such a disposition, it has been argued, most notably by the former privacy commissioner of Canada[99], that these types of laws should be adopted across the country. On the federal level, dispositions were recently added to PIPEDA to make notification mandatory[100]. However, said dispositions have yet to come into effect as of these writings. On the European side of the Atlantic, while some countries have their own data breach notification laws[101], their reach and focus differ. For example, German companies who fall victim to data breaches are obligated to notify both the DPA (data protection authority) and the data subjects[102], while in other countries, such as France[103], this obligation is limited to electronic communication service providers, as per the

97. See Benoît Dupont and Benoît Gagnon, *La sécurité précaire des données personnelles en Amérique du Nord, Une analyse des statistiques disponibles*, Chaire de recherche du Canada en sécurité, identité et technologie, 2008, p. 4, available at: <http://www.cicc.umontreal.ca/recherche/chercheurs_reguliers/benoit_dupont/chaire_note_recherche1.pdf>

98. SA 2003, c P-6.5.

99. See Jennifer Stoddart, "Preventing Data Breaches with Good Privacy – Remarks for the 6th Annual e-Crime Congress", (2008), available at: <http://www.priv.gc.ca/media/sp-d/2008/sp-d_080305_e.asp>

100. See *An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act*, 2015, c. 32, s. 10, which added sections 10.1 through 10.3 (Breaches of Security Safeguards) to PIPEDA.

101. Andreas Rockelmann, Joshua Budd, and Michael Vorisek, *Data breach notifications in the EU*, Crete, ENISA, 2011, p. 12.

102. *Id.*

103. See section 34 bis of the *Informatique et Libertés* act (Loi no 78-17 du 6 janvier 1978). Furthermore, under section 226-17-1 of the French Penal Code, an electronic communication service provider who fails to comply with this obligation risks spending 5 years in jail and having to pay a fine of €300 000.

e-Privacy Directive[104]. To fix this discrepancy, the EU is currently working on draft regulation that would impose similar data breach notification rules on all European businesses, therefore making it easier for companies to know the extent of their obligations[105]. According to privacy watchdogs, these types of laws can go a long way in fostering trust and confidence in electronic commerce, since consumers will be kept abreast of any security breach affecting their data[106]. However, many in the private sector have pointed to the fact that they create an unfair burden on businesses while not really addressing the issue of information provenance – i.e., just because a corporation is hacked doesn't mean that it is the source of a consumer's data being used by a third party. In other words, these laws create a presumption of provenance in the consumer's mind that is not necessarily factual. This is not to say that notification laws do not serve a purpose – it is important for consumers to know their information is at risk to allow them to cancel credit cards or change passwords – but that purpose is not necessarily linked to a consumer getting restitution for damages suffered. Moreover, security experts point to the existence of negative externalities associated with this type of legislation – such as breach notification fatigue – that could make the cure worse than the disease.

104. *Directive 2002/58/EC on Privacy and Electronic Communications, as modified by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Article 4, paragraph 3 of the amended 2002 Directive* reads: "In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay. Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it".

105. See "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)", (2012), available at: <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>. Article 31, paragraph 1 of the proposed regulation states that: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours".

106. See, for example, J. Stoddart, prec., note 99.

Breach notification fatigue results from the simple fact that breach notification laws have the adverse effect of flooding consumers' mailboxes and inboxes with notices, therefore desensitising them to the impact of said notices. As the Information and Privacy Commissioner of Ontario puts it:

> In the beginning, when they were novel, breach notification letters had a significant effect on raising awareness and stimulating corrective behaviour on the part of both organizations and individuals. Over time, however, while the number of notification letters has continued to grow […], the marginal utility and value of notification letters has levelled off and perhaps diminished as people become inured to receiving them and less concerned.[107]

Furthermore, a recent survey suggests that consumers will most likely lose their trust and confidence in the organization reporting the data breach[108], therefore statistically demonstrating that data breach notification laws would have the opposite effect of what CETA drafters are hoping to achieve. Granted, statistics rarely tell the whole story[109], and the loss of trust and confidence would be in one website, not the Internet as a whole, but when these statistics are read in conjunction with others that claim consumers often cannot differentiate between websites[110], one is entitled to question whether such legislation is a proper measure to reach the goals set by the CETA.

As for fraudulent and deceptive commercial practices, although they remain an issue that needs to be dealt with, they will only affect a consumer's trust and confidence in electronic commerce if said consumer knows that a given practice is fraudulent or deceptive, or rather that he actually cares. As Vincent Gautrais points out, very few online consumer contracts would actually survive a legal audit[111]. Yet, Canadian consumers spend billions of dollars online annually[112]. Therefore, as we see it, the practice itself is not what will push consumers away from electronic com-

107. Ann Cavoukian, "A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight", (2009), available at: <http://www.ipc.on.ca/images/Resources/privacy_externalities.pdf>, p. 9.

108. "2012 Consumer Study on Data Breach Notification", p. 9, available at: <http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf>. According to this study, 62% of consumers claim that they would lose trust and confidence in a company from which they receive a data breach notification.

109. As Benjamin Disraeli is claimed to have said: "There are three kinds of lies: lies, damned lies, and statistics".

110. See Liz Bales, "Digital content: copycat websites represent threat to creative industries", (2013) *The Guardian*, available at: <http://www.theguardian.com/media-network/media-network-blog/2013/jul/10/digital-content-copycat-websites-creative>

111. Vincent Gautrais, "Les contrats de cyberconsommation sont presque tous illégaux !", (2005) *Revue du Notariat* 617.

112. David Sweet (chair), "E-commerce in Canada: Pursuing the Promise - Report of the Standing Committee on Industry, Science and Technology", 2012, 41st Parliament, 1st session, p. 4.

merce, but rather whether or not they can get redress after such a practice is discovered. As one author puts it: "[t]he major obstacles to increasing transnational online business transactions include a lack of confidence in online transactions and the lack of predictable internet commercial laws for the resolution of online disputes"[113] (emphasis added).

That being said, the question of redress seems to have been left out of CETA electronic commerce negotiations or, rather, it is not addressed in the *Consolidated text*. Legal purists will point to the fact that this is irrelevant since private international law has long since established which court or courts are competent to hear a case involving foreign entities. Furthermore, the courts have already dealt with how to approach the specificities of e-contracts on numerous occasions, making any lingering issues of conflict of laws regarding e-commerce mostly theoretical[114]. However, given that the average online purchase is in the one hundred to two hundred dollar range (depending on the device used)[115], Court costs will usually be prohibitive for cyberconsumers[116]. Even if that wasn't the case, execution of a decision in such a small amount against a foreign entity seems highly unlikely. This is why it is believed by many that "[online] cross-border disputes [require] tailored mechanisms that [do] not impose costs, delays and burdens that [are] disproportionate to the economic value at stake"[117]. Furthermore, as others have put it, since "[e]very component of electronic commerce occurs online (meetings, information exchanges, negotiation and final signature)" [118], it could be argued that "[i]n order to provide effective resolution of the disputes that result from this kind of interaction, it is absolutely imperative that the methods used to manage the process are tailored specifically to the electronic environment"[119].

The aforementioned chargeback option could be presented as such a method. However, while useful in certain cases, this device has proven to have its flaws since it implies shorter delays than those afforded by the courts. For example, in Quebec, while a dissatisfied consumer has three years to seize the courts[120], he or she has to initiate the chargeback procedure within sixty days following the merchant's

113. A. L. Nenstiel, prec., note 73, 313.

114. See, for example, Sylvette Guillemard, *Le droit international privé face au contrat de vente cyberspatial*, Cowansville, Yvon Blais, 2006.

115. See Statista, "Average value of global online shopping orders in 2nd quarter 2015, by device (in U.S. dollars)", (2015), available at: <http://www.statista.com/statistics/239247/us-online-shopping-order-values-by-device/>

116. See P.-C. Lafond, prec., note 45, p. 50 and ss.

117. UNCITRAL, "Report of the United Nations Commission on International Trade Law", Forty-third session (21 June-9 July 2010), par. 254.

118. Karim Benyekhlef and Fabien Gélinas, "Online Dispute Resolution", (2005) 10-2 *Lex Electronica*: <http://www.lex-electronica.org/docs/articles_87.pdf>

119. *Id.*

120. *Civil Code of Québec*, section 2925.

refusal to reimburse him or her[121]. Furthermore, the chargeback option leaves the consumer with no other recourse than to cancel a purchase where seizing the courts will allow him or her to "force specific performance of the obligation" or "take any other measure provided by law to enforce his right to the performance of the obligation"[122].

Since the chargeback option is not sufficient to remedy all grievances stemming from online transactions, and since courts are not adapted to hear high-volume, low-value cross-border disputes, what solutions remain for settling electronic commerce disputes? As has been pointed out by numerous actors and observers, it is a commonly shared view that since "traditional judicial mechanisms for legal recourse [do] not offer an adequate solution for cross-border e-commerce disputes, […] the solution — providing a quick resolution and enforcement of disputes across borders — might reside in a global online dispute-resolution system for small-value, high-volume business-to-business and business-to-consumer disputes"[123].

Online dispute resolution (or ODR) can be defined as: "a means of dispute settlement which may or may not involve a binding decision being made by a third party, implying the use of online technologies to facilitate the resolution of disputes between parties" [124]. In short, ODR, in its widest acceptance, encompasses all methods and mechanisms that allow parties to settle their disputes using the Internet[125]. Such methods and mechanisms can be "incorporated directly into the electronic marketplace [which] not only make it possible to resolve disputes at the source, when they arise, but also to reassure the parties and create trust conducive to commercial transactions"[126]. Since fostering trust and confidence in electronic commerce is at the very core of the CETA's chapter on electronic commerce, drafters

121. *Consumer Protection Act*, section 54.14.

122. *Civil Code of Québec*, section 1590.

123. UNCITRAL, "Report of the United Nations Commission on International Trade Law", Forty-third session (21 June-9 July 2010), par. 254.

124. UNCITRAL Working Group III (Online Dispute Resolution), "Online dispute resolution for cross-border electronic commerce transactions – Note by the Secretariat", Twenty-second session (13-17 December 2010) par. 3. In this sense, ODR "has similarities with offline conciliation and arbitration" (commonly referred to as "alternative dispute resolution" or "ADR"). For a more thorough analysis of ODR, see E. Katsh and J. Rifkin, *prec.*, note 91; and Colin RULE, *Online dispute resolution for business: B2B, e-commerce, consumer, employment, insurance, and other commercial conflicts*, San Francisco, Jossey-Bass, 2002.

125. Arthur M. Monty Ahalt, "What You Should Know About Online Dispute Resolution", (2009) *The Practical Litigator* 21, at 21. See also A. L. Nenstiel, *prec.*, note 73, 313, quoting Ethan Katsh, "Cyber Law: Issues Affecting the Internet and Its Governance", (2001) 28 *N. Ky. L. Rev.* 810, 813.

126. K. Benyekhlef and F. Gélinas, prec., note 118. On this same issue, see Haitham A. Haloush & Bashar H. Malkawi, "Internet Characteristics and Online Alternative Dispute Resolution", (2008) 13 *Harv. Negot. L. Rev.* 327; and A. L. Nenstiel, prec., note 73, 313.

should therefore logically have done all that they could to facilitate the deployment of ODR solutions[127].

This is not to say that ODR guidelines should necessarily have been incorporated into the CETA, but a reference to the parties agreeing to work together to promote the use of ODR and to establish a legal framework to better regulate ODR providers should, in our opinion, have been envisioned. That being said, as with the current content of the *Consolidated text*'s chapter on electronic commerce, an ODR provision would probably have little real-world effect on actual efforts and collaborations to help promote ODR since Canada and the EU have already begun collaborating to this end.

For example, in 2010, the UNCITRAL "established a working group to undertake work in the field of online dispute resolution relating to cross-border electronic commerce transactions, including business-to-business (B2B) and business-to-consumer (B2C) transactions"[128]. Canada and the EU both have delegations taking part in these negotiations, as do many EU member states[129]. Since its inception, "Working Group III: Online Dispute Resolution", as it has been christened, has met twice yearly to draft procedural rules for "Online dispute resolution for cross-border electronic commerce transactions"[130]. Unfortunately, the Working Group has yet to be able to produce B2C guidelines since many delegations acknowledged the impossibility for a consensus to be reached[131]. Furthermore, as UNCITRAL has given the Working Group a 2016 deadline to produce said guidelines[132], their eventual adoption seems less and less likely. However, since Canada and the EU have had similar argu-

127. On the link between ODR and fostering trust on the Internet, see E. Katsh and J. Rifkin, prec., note 91, p. 85 and ss.

128. UNCITRAL Working Group III (Online Dispute Resolution), "Online dispute resolution for cross-border electronic commerce transactions – Note by the Secretariat", Twenty-second session (13-17 December 2010) par. 2.

129. A list of participants to each session is available in the session reports. Said reports are published on the UNCITRAL website: <http://www.uncitral.org/uncitral/commission/working_groups/3Online_Dispute_Resolution.html>

130. See *id.* for the evolution of said rules.

131. See <http://www.uncitral.org/uncitral/audio/meetings.jsp> for the audio files to the Working Group's 31st session.

132. A letter sent to Working Group participants in September 2015 states that: "Under the terms of reference established by the Commission at its forty-third session and pursuant to the Working Group's progress report to the Commission at its forty-eighth (A/69/17, under preparation), the Working Group is instructed to continue its work towards elaborating a non-binding descriptive document reflecting elements of an ODR process, on which elements the Working Group had previously reached consensus, excluding the question of the nature of the final stage of the ODR process (arbitration/non-arbitration). Delegations and observers may also wish to take note that the Working Group was given a time limit of one year or no more than two Working Group sessions to undertake this work, after which the work of the Working Group will come to an end, whether or not a result has been achieved."

ments all through the negotiations[133], pursuing talks on a bilateral basis should not be too problematic.

Moreover, since corporations linked to online merchants or other interested parties have been known to offer ODR (or ADR) services[134], we would submit that fostering trust and confidence in ODR, which would have a direct impact on fostering trust and confidence in electronic commerce as a whole, passes through state-run or state-sanctioned ODR[135]. This emerging trend seems to be spreading across the globe as a valid alternative to for-profit ODR. In fact, in November of 2011, the European Commission published a "Proposal for a Regulation of the European Parliament and of the Council on online dispute resolution for consumer disputes" (Regulation on consumer ODR), which aims to provide "a European ODR platform ('ODR platform') facilitating the independent, impartial, transparent, effective, fast and fair out-of-court resolution of disputes between consumers and traders online" in 2016[136]. Similarly, courts[137] and recognised professional orders such as bailiffs[138] are also experimenting with providing ODR services.

Therefore, bringing this notion one step further, a Canada-EU sponsored ODR system could go a long way in improving trust and confidence in electronic commerce, and, therefore, augmenting online transactions. As one author observed while proposing a similar platform for Canada-USA electronic commerce:

> "The resources expended through the public creation of an ODR system would likely be recovered through the savings of judicial resources, by providing alternative solutions to formal adjudication, and the increase in the wealth of the economy created by improving relationships and confidence in engaging in bilateral trade, allowing businesses to prosper through international online transactions."[139]

* * *

133. See, prec., note 131.

134. See, for example, Robert Berner, "Big Arbitration Firm Pulls Out of Credit Card Business", (2009) *Bloomberg Business*, available at: <http://www.businessweek.com/investing/wall_street_news_blog/archives/2009/07/big_arbitration.html>

135. See Karim Benyekhlef and Nicolas Vermeys, "A Plea for Court-Sanctioned ODR", (2012) *Slaw*, available at: <http://www.slaw.ca/2012/08/01/a-plea-for-court-sanctioned-odr/>

136. *Regulation (EU) no 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC* (Regulation on consumer ODR), article 1. According to article 22 of the Regulation, it "shall apply from 9 January 2016".

137. See Nicolas W. Vermeys and Karim Benyekhlef, "ODR and the Courts", in Mohamed S. Abdel Wahab *et al.*, *Online Dispute Resolution: Theory and Practice*, The Hague, Eleven, 2012, p. 295.

138. See, for example, <https://www.cmhj.fr/>

139. A. L. Nenstiel, prec., note 73, 320.

Combining pre-emptive solutions such as trustmarks and corrective solutions such as ODR would give online consumers a comfort-level that is equivalent – some might say superior – to that offered by brick-and-mortar businesses, therefore ensuring a rise in trust and confidence in electronic commerce[140]. A trustmark stating that a given electronic commerce website accepts to take part in any mediation or arbitration session submitted through the aforementioned Canada-EU sponsored ODR system (or systems) would guarantee online consumers that they'll have access to an adapted and efficient dispute resolution mechanism since "[w]ithout a prior agreement to engage in ADR proceedings, it has been shown that there is a decreased chance that businesses will use alternative dispute resolution"[141]. Furthermore, the threat, for businesses, of losing a trustmark should they neglect or refuse to conform to an agreement or decision, would make it more likely for consumers get redress.

This type of proposal is not new. In fact, it stems from a similar project put forth by the European Commission almost 15 years ago. In 2001, the EC launched the ECODIR platform, an ODR platform developed by the Centre de Recherche en Droit Public (CRDP) to settle online consumer disputes (ECODIR stands for Electronic Consumer Dispute Resolution). This platform was supposed to be the centerpiece of a greater EU-wide effort to foster trust and confidence in electronic commerce. The Commission was expected to follow ECODIR's launch with an outreach to online merchants, advertising campaigns, and an ECODIR trustmark[142]. Unfortunately, lack of funding forced the project to be halted, and the ECODIR platform, its only accomplishment, remains lost in the catacombs of cyberspace[143]. For the CETA to have a chance at truly effecting change, we believe that the parties need to revisit the ECODIR model and invest in creating a similar platform (and associated trustmark system) for Canada-EU consumer disputes.

140. E. Katsh and J. Rifkin, prec., note 91, p. 86-87.

141. A. L. Nenstiel, prec., note 73, 324.

142. See Karim Benyekhlef, "La résolution en ligne des différends de consommation : un récit autour (et un exemple) du droit postmoderne", in Pierre-Claude Lafond (dir.), *L'accès des consommateurs à la justice*, Cowansville, Yvon Blais, 2010, p. 89, at pages 103 and ss.

143. The website (www.ecodir.org) is no longer active. See *id.*

CONCLUSION

How a person chooses to predict whether the CETA will positively affect electronic commerce really depends on whether that individual views the glass as being half empty or half full. The most cynical among us will claim that the CETA's dispositions on electronic commerce are a waste of ink and paper (or bytes) since all the necessary tools for its promotion are already in place or being created in other *fora*. On the other hand, optimists will point to previous agreements and joint statements as the building blocks for a robust and effective CETA. Only time will tell if either (or both) of these positions is and will be correct. Until then, however, we can all find comfort in the fact that the CETA will most likely have very little discernable impact on our rights and obligations when contracting for the sale of goods and services in cyberspace. At best, it will make transactions safer and less costly, at worse, it will do nothing at all… Either way, unless important investments are made in the field of ODR, legislative changes will be for naught since stronger legislation will not resolve the issue of court costs being more important than possible awards for breach of contract and/or damages[144].

144. K. Benyekhlef and F. Gélinas, prec., note 118.