Bennett, Colin J.

Working Paper

The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada should consider accession

CIGI Papers, No. 246

Provided in Cooperation with:
Centre for International Governance Innovation (CIGI), Waterloo, Ontario

Suggested Citation: Bennett, Colin J. (2020) : The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada should consider accession, CIGI Papers, No. 246, Centre for International Governance Innovation (CIGI), Waterloo, ON, Canada

This Version is available at:
https://hdl.handle.net/10419/299718

Centre for International
Governance Innovation

CIGI Papers No. 246 — November 2020

The Council of Europe's Modernized Convention on Personal Data Protection

Why Canada Should Consider Accession

Colin J. Bennett

Centre for International
Governance Innovation

CIGI Papers No. 246 — November 2020

The Council of Europe's Modernized Convention on Personal Data Protection

Why Canada Should Consider Accession

Colin J. Bennett

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Director, Digital Economy Research Robert Fay
Program Manager Heather McNorgan
Publications Editor Susan Bubak
Senior Publications Editor Jennifer Goyder
Graphic Designer Brooklynn Schwartz

For publications enquiries, please contact publications@cigionline.org.

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Author

Colin J. Bennett is a professor in the Department of Political Science at the University of Victoria. He has enjoyed visiting professorships at the Harvard Kennedy School at Harvard University; the Center for the Study of Law and Society at the University of California, Berkeley; the School of Law at the University of New South Wales; the Law, Science, Technology & Society Research Group at the Vrije Universiteit in Brussels; and the Faculty of Information at the University of Toronto. His research has focused on the comparative analysis of surveillance technologies and privacy governance at the domestic and international levels. In addition to numerous scholarly and newspaper articles, he has published seven books on these subjects. He is currently researching the capture and use of personal data for political campaigning in Western democracies.

Acronyms and Abbreviations

APEC	Asia-Pacific Economic Cooperation
CBPR	Cross-Border Privacy Rules
CETS	Council of Europe Treaty Series
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CUSMA	Canada-United States-Mexico Agreement
DPA	data protection authority
G7	Group of Seven
GDPR	General Data Protection Regulation
ISED	Innovation, Science and Economic Development Canada
OECD	Organisation for Economic Co-operation and Development
PIPEDA	Personal Information Protection and Electronic Documents Act

Executive Summary

The Council of Europe's (CoE's) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was originally passed in 1980, and has recently been reformed to be more relevant to contemporary global digital communications. This paper contends that Canada should seriously consider accession to this important convention. Accession would reinforce Canada's reputation as a trusted jurisdiction for personal data processing and thereby assist the development of the Canadian digital economy; help Canada's application to the European Union for continued "adequacy" status under the General Data Protection Regulation (GDPR); facilitate the import and export of personal data to and from other signatories to the convention; potentially reinforce data export restrictions in recently signed international trade treaties; make a powerful statement about Canada's commitment to international privacy rights; and also enhance the credibility of the convention as the only binding and multilateral standard for the protection of personal information at a critical time in the development of the global digital economy.

Introduction

The CoE's Convention 108 was originally passed in 1980 and opened for ratification a year later.[1] It was, and remains, the only binding international convention within the international privacy and data protection policy space. It has recently been updated and modernized. This modernized "Convention 108+" is open for accession from both member states of the CoE and non-member states.[2]

Since the late 1990s, however, Convention 108 has stood in the shadows of the European Union's 1995 Data Protection Directive[3] and its successor, the GDPR.[4] Both EU instruments have operated to promote data protection policies around the world and have had an extraordinary extraterritorial effect (Bennett and Raab 2006; Newman 2008; Kuner 2013). Graham Greenleaf and Bertil Cottier (2020) have counted more than 140 countries with data protection or information laws as of the end of 2019. There is perhaps no greater evidence of the externalization of the European Union's regulatory power and of the trading up of standards through what has been called the "Brussels effect" (Bradford 2020; Bygrave 2020).

The GDPR promotes external data protection standards through the relatively coercive mechanism of the adequacy standard, decided on a case-by-case basis by the EU Commission as a result of detailed analysis of the data protection legislation of "third countries." Organizations in countries with adequate levels of protection are then able to import personal data from the European Union without having to negotiate or apply further safeguards; Canada has enjoyed this status since 2002. This is not the only mechanism through which personal data can be legally transferred from the European Union: codes of conduct, standard contractual clauses, binding corporate rules and certification mechanisms can all offer possible legal guarantees. The terms for data transfers in each case are imposed by the European Union to protect the fundamental rights of EU citizens.[5]

By contrast, Convention 108+ is explicitly drafted with a view to its possible role as a global instrument that offers reciprocal rights and obligations. As explained below, it is motivated by, and framed in, clear human rights language. Unlike the GDPR, it is not driven by an overriding need to balance privacy with commercial interests. Its language is also more accessible than the highly legalistic GDPR. It is designed to "travel" (Bygrave 2020).

This paper contends that it is in Canada's interests to accede to Convention 108+ and that the federal government should now seriously consider the question. Canadian accession would:

1 The author uses the term "data protection" throughout to describe the category of law that regulates the processing of personal data by public and private sector organizations in order to protect the broader value of personal privacy.

2 See https://rm.coe.int/16808ade9d.

3 See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

4 See GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

5 Ibid., article 46.

- assist in extending Canada's adequacy status with the European Union;
- establish voluntary and mutual obligations for personal data export and import with countries outside the European Union;
- facilitate international personal data processing for business (especially in light of the recent decision by the Court of Justice of the European Union [CJEU] known as Schrems II);
- potentially assist in the implementation of the data export provisions of recent international treaties;
- bolster Canada's international reputation as a trusted jurisdiction for personal data processing and thereby assist the development of the Canadian digital economy; and
- make a powerful statement to the rest of the global community about Canada's commitments to international privacy rights in the face of extraordinary levels of global surveillance.

Canadian accession would also significantly enhance the credibility of Convention 108+ as a global privacy protection standard. As the first Group of Seven (G7) economy outside the CoE, Canada would send a message about the importance of this treaty and potentially inspire similar considerations in other countries. Canada's accession could also send an important message to the Global South and would bolster the decisions of those countries in Africa, Asia and Latin America that have already acceded or made the decision to accede. Canadian accession could, therefore, give an important boost to the global reach of the convention at a critical time in the development of international privacy protection policy.

The question of Canadian accession to Convention 108 has rarely been raised in Canadian policy and legal circles. It is time for the federal government to seriously consider such a step.

Convention 108

The CoE is an intergovernmental organization of 47 member states, stretching far beyond the scope of the European Union. Canada was granted "observer status" in 1996 and has the right to send representatives to meetings of the Committee of Ministers and the Parliamentary Assembly.[6]

The CoE's interests in the right to privacy and new technology have their roots in article 8 of the right to privacy in the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights). More detailed work on the impact of new technologies on the emerging right to data protection dates back to the 1960s (Bennett 1992, 133). A series of studies and recommendations culminated in the original Convention 108, adopted and opened for ratification on January 28, 1981, the anniversary of which is now celebrated annually with Data Privacy Day. The convention formally came into effect on October 1, 1985.[7]

At the time, many countries lacked comprehensive data protection rules for the collection, storage and use of personal information. Convention 108 propelled a greater harmonization in data protection standards and had a significant influence on the first generation of data protection laws, including the first UK Data Protection Act in 1984. The original Convention 108 was signed and ratified by all 47 members of the CoE. It was also ratified by eight non-CoE countries in Africa and Latin America: Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia and Uruguay.[8]

The convention requires signatory states to apply its principles within its domestic information privacy or data protection legislation. An additional protocol to the convention was added in 2001, requiring the appointment of a data protection authority (DPA) and imposing certain data export restrictions for transfers to non-parties to the convention. Over the years, the CoE has also adopted a series of recommendations on specific technologies and sectors, such as health-related data, police information, profiling and social media services, as well as guidelines on artificial intelligence, big data and other issues.[9] The CoE is currently considering the application of the

6 See www.coe.int/en/web/portal/canada.

7 See www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

8 See www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.

9 For the full details of CoE legal instruments, see www.coe.int/en/web/data-protection/legal-instruments; for reports, studies and opinions, see www.coe.int/en/web/data-protection/reports-studies-and-opinions#.

new convention to personal data processing within election campaigns (Bennett 2020a).

Convention 108 has remained central to the development and implementation of global data protection standards for four interrelated reasons, according to Paul de Hert and Vagelis Papakonstantinou (2014). First, there exists no other international instrument of similar status as a binding international legal instrument; ratification obliges states to incorporate the convention's provisions into their domestic legislation. Second, its text is relatively uncomplicated and flexible, especially compared with the formalistic complexity of the EU Data Protection Directive and the GDPR. Third, the convention remains the only mandatory and multilateral data protection instrument that contains specific provisions about the use of personal data by law enforcement agencies. Fourth, it has a solid basis in human rights law and, in particular, in the right to privacy guaranteed in article 8 of the European Convention on Human Rights: "Everyone has the right to respect for his private and family life, his home and his correspondence." Over the years, the European Court of Human Rights has handed down a series of judgments on data protection that are particularly impactful in areas where EU law is excluded, namely national security.

That said, by 2010, it was generally agreed that Convention 108 was dated and needed modernization in response to developments in global digital services and new technologies. The Consultative Committee on Convention 108 then embarked on a process of amendment and updating, maintaining a close eye on the parallel development of the GDPR within the European Union, and on the updating of the 1981 guidelines from the Organisation for Economic Co-operation and Development (OECD). Several outside countries (including Canada and the United States) and international organizations had observer status, participated in the public consultation process and were present at the plenary meetings (de Hert and Papakonstantinou 2014, 641). The modernized convention (Convention 108+) was finalized on May 18, 2018, in an "amending protocol" (Council of Europe Treaty Series [CETS] No. 223) and was opened for signature later that year.[10] As of October 2020, 42 countries have signed the new convention (including four non-CoE members) and eight have ratified it.[11]

The Modernized Convention 108+

The aim of modernization was both to address privacy challenges from new technologies and to strengthen enforcement. The amending process was based on three general assumptions: that it must be general and technologically neutral; that it must be compatible with emerging legal frameworks; and that it must continue to be an open, and potentially universal, standard.[12]

Convention 108+ is also explicitly rooted in a broad aim "to secure the human dignity and protection of the human rights and fundamental freedoms of every individual." It speaks of "personal autonomy based on a person's right to control of his or her personal data and the processing of such data." It recognizes that the "right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression."[13]

The consolidated convention contains eight interrelated chapters: general provisions, basic principles, transborder data flows, supervisory authorities, cooperation and mutual assistance, the duties of the Convention Committee, the amending procedure and final clauses.[14] The basic data protection principles mirror those in other international instruments and are driven by the essential precept (article 5) that "data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake." Convention 108+ therefore

10 See https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e.

11 See www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures. The four non-CoE members are Argentina, Mauritius, Tunisia and Uruguay.

12 See https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

13 See Convention 108+, Preamble: https://rm.coe.int/16808ade9d.

14 See https://rm.coe.int/16808ade9d.

covers all sectors, including national security and law enforcement. It strictly limits the processing of sensitive forms of data on a person's race, politics, ethnic origin, trade-union membership, health, religion, sexual life and criminal record, in the absence of proper legal or technical safeguards.

Convention 108+ differs from the original convention in a number of important respects. The main "novelties" include:

- a stronger affirmation of the relationship between data protection and other fundamental rights and freedoms;
- changes to the scope of application (and, in particular, the mandatory inclusion of manual files);
- stronger requirements for the demonstration that legal measures are effective (a "follow-up" mechanism);
- clarification on the principle of proportionality;
- strengthening of the consent requirements;
- an extension of the categories of sensitive forms of data;
- data breach notification requirements;
- enhanced transparency requirements;
- new rights of the data subject, especially with respect to automated processing; and
- improved accountability measures, together with obligations concerning impact assessments and privacy by design and privacy by default.[15]

For many countries outside the CoE, the rules concerning international data flows are going to be a compelling reason to consider accession. Convention 108+ requires an "appropriate" protection of individuals when data flows away from the jurisdiction of a party to the convention. It establishes two main means to ensure that the level of data protection is indeed appropriate: either by law, or by ad hoc or approved standardized safeguards that are legally binding and enforceable (notably contractual clauses or binding corporate rules). The protection afforded "has to be of such quality as to ensure that human rights are not affected by globalisation and transborder data flows."[16] Data can flow freely, however, between parties to the convention. There is no lengthy and legalistic determination of an "adequate level of protection" as there is under the GDPR: data flows cannot be prohibited or subjected to special authorization "for the sole purpose of the protection of personal data."[17]

It is recognized in the GDPR that a country's accession to Convention 108+ will be an important factor in the judgment of a country's adequacy. Recital 105 states: "The Commission should take account of obligations arising from the third country's or international organization's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention [108]...and its Additional Protocol should be taken into account." Accession is obviously not a guarantee of a positive adequacy assessment, but it would clearly assist the case and perhaps facilitate a speedier process of evaluation.

Greenleaf (2020) has concluded that Convention 108+ includes most of the important provisions of the GDPR, even if they are in a less prescriptive form. The main gaps appear to be the following: no right of "data portability," no specific right to delinking (the "right to be forgotten"),[18] and weaker requirements for enforcement and fines. He goes on to argue, however, that the process of evaluating whether countries meet the standards of Convention 108+, while more rigorous than those under its predecessor, also offers some flexibility. Evaluation will also require each party to demonstrate sufficient evidence of the convention's provisions in practice. These evaluations, going forward, will depend on the way that the Convention Committee ensures that its decisions are based on a "fair, transparent

15 See https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8.

16 Explanatory Report to the Protocol, clause 103: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

17 Ibid., clause 105: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

18 It should be noted that a right to "erasure" exists in article 9(e) of the modernized text, and that the combination of other provisions in the convention arguably provides the same result as the "right to be forgotten" in the GDPR.

and public procedure."[19] Greenleaf has also argued that national privacy non-governmental organizations have a critical role to play as engaged observers of the Convention 108+ accession process going forward (2020, 28–30).

Thus, adherence to Convention 108+, including proper enforcement, may well be sufficient to satisfy the standard of adequacy under the GDPR (Greenleaf 2018a; Article 29 Data Protection Working Party 2017).[20] For many outside countries, therefore, Convention 108+ could provide a far more attractive and "importable" standard.

The Globalization of Convention 108+

Convention 108 has always been viewed as an instrument whose principles can be exported; globalization is within its DNA (Kwasny 2017). It was not until 2008, however, that the CoE began to actively promote the convention through accessions by non-European states. The modernized convention was more explicitly developed with an eye to its global impact, since its open character gives it a "unique potential as a universal standard."[21] This vision is shared by UN Special Rapporteur Joseph Cannataci, who, in his 2018 annual report, recommended that UN member states "be encouraged to ratify data protection Convention 108+ using CETS223 and implement the principles contained there through domestic law without undue delay, paying particular attention to immediately implementing those provisions requiring safeguards for personal data collected for surveillance and other national security purposes."[22] The idea has also occasionally been pitched by privacy advocacy organizations, such as the Electronic Privacy Information Center in the United States,[23] the Australian Privacy Foundation and Privacy International, based in London, which are accredited as official observers to the Convention 108 Consultative Committee.[24]

International privacy law expert Lee Bygrave has contended that there is significant potential for a "Strasbourg effect," perhaps overriding the dominant "Brussels effect." The European Union can leverage the GDPR's adequacy mechanism to help advance the global diffusion of Convention 108+. Indeed, it is the only conceivable way that a multilateral treaty can be advanced based on European privacy principles. Further, the EU data protection regime has become "byzantine," characterized by massive rulemaking, huge officialdom, procedural intricacy and high-profile judicial support. It has become, according to Bygrave, imperious and increasingly self-referential. EU data protection is a "Kafkaesque castle full of semantic mazes, winding procedural alleys, subterranean cross-passages, conceptual echo chambers and an immense bureaucratic apparatus" (Bygrave 2020, 18–19).

By contrast, Bygrave (2020, 21) argues, Convention 108+ is a "breath of fresh air." It is a "relatively slim, neatly packaged and uncomplicated code." It offers a "cleaner and more understandable data protection template than the GDPR." It is more in line with the very roots of data protection law — the essential data protection principles that form the core of the legal regime and around which the early data protection statutes converged (Bennett 1992, chapter 3). Of course, the superficial simplicity of Convention 108+ does mask some considerable legal and procedural complexity, inevitable given the close alignment with the EU model. In fairness, EU institutions, interpreting the more detailed EU instruments, have been far more influential in promulgating the more refined interpretations of data protection norms and their application in different contexts, and that inevitably, over time, produces intricacy (de Hert and Papakonstantinou 2014, 641).

How do non-member countries accede, therefore? The CoE Directorate of Legal Advice and Public International Law has outlined the process,

19 See Explanatory Report to the Protocol, clause 163: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

20 It should also be noted that the EU Commission contemplates specific guidance on assessing adequacy in countries that have ratified Convention 108.

21 See Explanatory Report to the Protocol, clause 2: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

22 See https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/324/47/PDF/G1832447.pdf?OpenElement.

23 See https://epic.org/privacy/intl/coeconvention/.

24 For a list of observers, see https://rm.coe.int/list-of-observers-nov-2018-en/1680938538.

which is typically initiated by the minister of foreign affairs or equivalent.[25] Any decision to invite accession to the convention has to be unanimously agreed by those members that have ratified the convention. The state invited has to ensure that it takes the necessary measures to ensure that its domestic law is consistent with the convention. It is up to the Committee of Ministers to decide, based on the Consultative Committee's opinion, whether a country's laws are sufficiently similar to the convention, or whether they require changes. If there are no objections, the convention shall enter into force three months after the instrument of accession is deposited at the seat of the CoE in Strasbourg.

To accede, states must be democratic, but there is no clear indication about what that means. States must have laws that cover both public and private sectors, although the convention does not require a single "omnibus" statute on the European model. The laws must embody the principles of the original convention, as well as those in the amending protocol (CETS No. 223) — the fully modernized convention, in other words. Accession to the additional protocol is also now mandatory, whereas under the original convention it was more discretionary. In practice, therefore, countries will need laws overseen by a DPA, or at least an equivalent independent supervisory authority. They will also have to provide for enforceable data export restrictions (Greenleaf 2016). Beyond these basic requirements, the exact process of evaluation and the operation of the new follow-up mechanism is still being determined.

Why Canada Should Accede to Convention 108+

Greenleaf (2016) has listed a number of interrelated benefits to Convention 108+ accession for countries outside Europe. It provides a minimum standard, and countries may enact higher standards if they wish. Unlike the GDPR, which seeks to impose privacy standards through the adequacy mechanism, Convention 108+ is based on a voluntary acceptance of mutual and reciprocal obligations. The convention's other benefits include the following:

- → It signals a recognition of best practices.
- → It can serve as an alternative to the specification of "whitelists" for data exports.
- → It assists in the determination of adequacy under the GDPR.
- → It may assist certain international organizations in areas such as policing, financial surveillance and humanitarian assistance that must develop procedures for international transfers of personal data.
- → It facilitates assistance between DPAs.
- → It provides certain benefits for businesses, both exporters and importers, and data controllers and data processors, where there are reciprocal obligations.
- → It provides benefits for individual data subjects, because enforceable privacy laws apply wherever their data is exported, and DPAs are required to aid these individuals (ibid.).

Greenleaf therefore believes that the convention has some realistic prospects of globalization, as it is really the only binding and multilateral global privacy agreement in existence.

When he prioritizes the various countries with data protection laws that might accede to Convention 108+, Canada is near the top of his list. It is one of only six countries[26] that meet all the criteria and have already been declared adequate under EU rules (Greenleaf 2018a). In light of this position, what extra benefits could accrue from Convention 108+ accession for Canada?

First, accession to Convention 108+ could certainly enhance Canada's likelihood of extending its adequacy status with the European Union under the GDPR. The Canadian government has been providing regular updates to the EU Commission on developments in Canadian privacy law (Innovation, Science and Economic Development Canada [ISED] 2019), but it is by no means certain that Canada's

25 See https://rm.coe.int/16809028a4.

26 Including Argentina, Israel, New Zealand, Uruguay and, most recently, Japan.

adequacy status will continue. The standard has shifted to that of "essential equivalence" to EU data protection (after the first Schrems decision by the CJEU in 2015), and the relevant starting point is the new GDPR rather than the 1995 Directive; the GDPR contains several provisions that do not appear in Canadian law. Furthermore, the commission's intense focus on potential access to personal data by law enforcement and intelligence agencies — the issue that has now invalided both the US-EU Safe Harbor and Privacy Shield mechanisms — was not part of the original evaluation of Canadian law back in 2002, when Canada's adequacy status was first granted. Adequacy evaluations are, therefore, now more comprehensive. Accession to Convention 108+ will not be determinative, but it is a fact that the commission is bound to consider (as required by Recital 105 of the GDPR quoted above).

Second, a further benefit could accrue from Canada's relations with members of the CoE that are non-EU countries and that are, or could be, parties to the treaty. This includes an additional 20 or so countries and some quite big economies, including Norway, the Russian Federation, Switzerland, Turkey and, of course, a post-Brexit United Kingdom. Essentially, Convention 108+ establishes a safe harbour for the free flow of personal data based on mutual and reciprocal agreement.

Third, there may be benefits in relation to countries outside the European Union and the CoE, including Mexico, one of Canada's largest trading partners. Many such countries have data protection laws, and some of them establish a whitelist of countries to which personal data might be legally exported. The new Japanese Act on the Protection of Personal Information is a recent example. Mutual accession to Convention 108+ would serve to substitute for the tricky and politically sensitive compilation of whitelists in different countries. Accession saves individual countries from having to conduct their own adequacy judgments on the legal systems of the multiple jurisdictions to which their companies might transfer personal data for processing. It should also be noted that these data export restrictions not only appear in national laws but also in some subnational jurisdictions. Quebec's new Bill 64, for instance, establishes new requirements for enterprises to conduct a privacy impact assessment to evaluate whether exported information will receive the level of protection equivalent to that provided by Quebec law.[27]

Fourth, and relatedly, accession could help resolve some of the inconsistencies within the privacy protection rules in Canada. Only Alberta, British Columbia and Quebec have passed data protection laws covering their provincially regulated private sectors.[28] The federal Personal Information Protection and Electronic Documents Act (PIPEDA) only regulates a portion of Canada's commercial sector, and it is only that portion that is covered by the EU Commission's 2002 Canadian adequacy finding. Sub-jurisdictional adequacy assessments are contemplated within the adequacy mechanism of the GDPR, but they are unlikely to be conducted in the near future. Accession for the entire federation, including public and private sectors, would produce a larger jurisdictional safe harbour than the partial one currently provided through Canada's "partial" adequacy assessment of data transferred to organizations covered by PIPEDA.

There may be some concern in governmental circles that the federal/provincial division of powers might preclude the ability of the federal government to argue on behalf of all jurisdictions that the complex array of federal and provincial, public and private sector laws might not provide the seamless coverage required of Convention 108+. An assessment of Canadian equivalence to the Convention 108+ principles would no doubt involve some careful legal analysis, but Canada's federal structure should not be seen as a barrier to accession. The principle-based framework of Convention 108+ permits an assessment of jurisdictional protection, even if that protection is afforded across a number of different statutory provisions.[29]

Fifth, advantages might accrue from consideration of provisions in recent trade agreements to which Canada is a party. Article 19.8 in the section on digital trade in the new Canada-United States-Mexico Agreement (CUSMA), for instance, recognizes the importance of the protection of

27 See Act Respecting the Protection of Personal Information in the Private Sector, section 107: http://legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1.

28 Ontario is currently considering its own privacy law for the private sector and has initiated a consultative process. See www.ontariocanada.com/registry/view.do?language=en&postingId=33967.

29 See https://rm.coe.int/consultative-committee-of-the-convention-for-the-protection-of-individ/16806945cc.

privacy, and the principles enshrined in cross-border agreements such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules System — the more self-regulatory mechanisms that the United States has endorsed. It does not mention Convention 108+, although it should be noted that Mexico is one of the non-CoE members that ratified the original convention.

Could accession to the convention allow a party to CUSMA to resist a challenge under article 19.11 on "Cross-Border Transfer of Information by Electronic Means"? This article states: "No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person." It goes on, however, "this Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective."[30] Greenleaf (2018b) contemplates a four-part test: a legitimate purpose, non-discrimination, no disguised restriction and necessity. Adherence to Convention 108+ could bolster the case that protecting Canadians' personal data is a legitimate and necessary purpose, and that international data flow restrictions are applied in a non-discriminatory manner. Critically, however, this test does not apply to data localization measures imposed outside the public sector, leaving Canada open to challenge for any attempts to restrict personal data storage for commercial purposes to servers within Canada (Geist 2018).

There is more flexibility under the new Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). This same test is applied to both the restrictions to the free cross-border flow of information (article 14.11) *and* any data localization measures (article 14.13). Further, article 14.8 explicitly addresses "Personal Information Protection" and recognizes the "economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence." It goes on: "Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks."[31] Presumably, Convention 108+ would be such a framework. Chapter 14 only contemplates a challenge to data localization requirements imposed for commercial reasons; it explicitly excludes government procurement.[32]

Sixth, accession would also remedy some of the obvious weaknesses in the APEC Privacy Framework and its system of Cross-Border Privacy Rules (CBPR) (APEC 2015). Canada is a signatory to this framework and was instrumental in its development in the early 2000s. Its practical implementation across the Asia-Pacific region, however, has been disappointing. The CBPR system is a self-certification system designed to harmonize regulatory differences and facilitate the sharing of personal data in participating economies. To date, only Australia, Canada, Japan, Mexico, Singapore, South Korea, Taiwan and the United States have agreed to participate in the system. Critical to the operation of this system is the designation of "accountability agents" to which a company is subject to oversight and consumers can complain. To date, the only accountability agents approved by their respective governments are in Japan, Singapore, South Korea and the United States. Canada has been receiving applications, but no appointment has yet been made. In a context where an increasing number of countries in the Asia-Pacific region have developed enforceable data protection laws, the potential impact of the APEC framework has receded.

Finally, Canada is also a party (since 2015) to the CoE Budapest Convention on the fight against cybercrime. This international treaty harmonizes domestic criminal substantive law provisions

30 See www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/cusma-19.pdf.

31 See CPTPP, article 14.8: www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng.

32 Ibid., article 14.2.

in the area of cybercrime, provides for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences, and seeks to set up a fast and effective regime of international cooperation. It relates to crimes committed over the internet or other computer networks, in particular computer-related fraud, child pornography, violations of network security and infringements of copyright. The negotiation of a second international protocol to this treaty is currently under way and is designed, broadly, to simplify the regime for mutual legal assistance and international production orders. The protocol will also include data protection safeguards.[33] Canada is currently negotiating this second additional protocol. There are strong merits to Canada affirming its commitment to data protection standards, through its accession to Convention 108+, to strengthen its commitment to these additional standards on cybercrime.

Accession to Convention 108+ could never operate as an alternative to the continuation of adequacy status under the GDPR; there is no getting around the inherent advantages of this status for Canadian companies, nor the continued extraterritorial impact of European data protection law. However, accession would potentially make it easier for an adequacy determination to be achieved and could operate as a complementary protection for Canadian consumer and business interests. Convention 108+ offers more legal certainty than the self-regulatory arrangements inherent in the APEC Privacy Framework. Canadian companies would have fewer restrictions with data exports to, and imports from, other parties to the convention. Accession would offer a further opportunity to promote Canada as a jurisdiction with strong privacy and security standards and thereby promote its domestic digital and cloud-computing services.

Conclusion

In the wake of the CJEU decision in the Schrems II case, there is considerable uncertainty about how businesses can transfer personal data internationally and, at the same time, abide by the GDPR and not violate EU citizens' fundamental rights.[34] The court has invalidated the EU-US Privacy Shield and confirmed that standard contractual clauses may only be used as a legitimate transfer mechanism if the transfer does not violate the GDPR and the fundamental rights of Europeans. Since Schrems II, the state of international personal data protection is in some disarray. The decision has global implications for any company that wishes to import data from the European Union, including Canadian companies (Bennett 2020b). Furthermore, uncertainty has also increased as a result of the CJEU's decision on the general or indiscriminate capture and retention of telecommunications traffic data for the purposes of combatting crime or safeguarding national security (CJEU 2020).

Different international instruments, with differing levels of legal compulsion, now occupy the landscape. The OECD guidelines and the APEC framework are voluntary. The GDPR is compulsory, and its extraterritorial effect is felt through the regulation of any controller or processor outside the European Union offering goods or services within the European Union, or monitoring behaviour within the European Union.[35] In an environment where the globalization of personal data flows requires a true globalization of consistent rules, Convention 108+ is the only candidate, absent the negotiation of a separate international treaty, for a set of truly international and legally binding rules.

Thus, paradoxically, the true value of Convention 108+ does not accrue significantly to EU countries. Its added value lies more broadly, and in particular to countries that are outside both the European Union and the CoE. As de Hert and Papakonstantinou (2014, 642) conclude, it represents a balanced approach: "a text that is broad enough for all countries in the world to accept and still has binding power for everybody to actually implement." Greenleaf wrote in 2013 that the modernized convention needs to meet the "Goldilocks test" — not too strong to scare away potential signatories, and not too weak to be seen to be undermining the stronger EU standards (Greenleaf 2013).

33 See www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

34 See http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404.

35 See GDPR, article 3(2): https://gdpr-info.eu/art-3-gdpr/.

For Canada, there is no inherent reason why the GDPR should be seen as the only viable international standard to guide domestic privacy law reform at the federal and provincial levels. Even if accession is not pursued, federal and provincial privacy law reform would benefit from close attention to the principles enshrined in Convention 108+. For Canada, a country that has prided itself over the years for offering pragmatic solutions to domestic and international privacy protection, Convention 108+ offers more viable, practical and importable language than that found in the GDPR.

However, Canada should also consider more formal accession to Convention 108+ as an appropriate complement to continued EU adequacy status under the GDPR. There are few, if any, costs to accession for Canada — especially as the government has already introduced Bill C11, reforming PIPEDA, and begun a formal consultation on the revision of the Privacy Act as part of its Digital Charter agenda (ISED 2020). Canadian accession would also significantly enhance the credibility of Convention 108+ as a global privacy protection treaty. As the first G7 economy outside the CoE, Canadian accession could give an important boost to the treaty and potentially inspire similar considerations in other countries. Canada's accession could also send an important message to those countries in Africa, Asia and Latin America that have already acceded or made the decision to accede, and thus take a stand in support of global privacy protection standards.

For Canadian officials and experts, Convention 108+ might be regarded as marginal and incremental, but there is the potential (as argued above) for some significant legal, economic and political benefits for both Canada and for the entire international data protection regime. Convention 108+ requires a boost. If Canada were to signal its willingness to accede, that might just be the action to propel Convention 108+ from its current status as a "useful add-on" to the stricter and more well-known GDPR, to its envisaged role as the basis of a global privacy treaty. The more countries take it seriously, the more likely it is that it will be taken seriously.

Acknowledgments

The author is very grateful to Sophie Kwasny, Graham Greenleaf, Lee Bygrave, Greg Smolynec, Chris Prince, Bill Hearn, Bob Fay and to the two anonymous reviewers for their helpful comments on an earlier draft of this paper.

Works Cited

APEC. 2015. *APEC Privacy Framework*. Singapore: APEC Secretariat. www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

Article 29 Data Protection Working Party. 2017. "Adequacy Referential." WP 254 rev.01. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

Bennett, Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press.

———. 2020a. "Personal Data Processing by and for Political Campaigns: The Application of the Council of Europe's Modernised Convention 108." Draft paper prepared for the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Strasbourg, June 11.

———. 2020b. "The Schrems II decision: Implications and challenges for Canada." *Colin J. Bennett* (blog), July 16. www.colinbennett.ca/data-protection/the-schrems-ii-decision-implications-and-challenges-for-canada/.

Bennett, Colin J. and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective.* Cambridge, MA: MIT Press.

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World.* Oxford, UK: Oxford University Press.

Bygrave, Lee A. 2020. "The 'Strasbourg Effect' on Data Protection in Light of the 'Brussels Effect': Logic, Mechanics and Prospects." University of Oslo Faculty of Law Research Paper No. 2020-14. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3617871.

CJEU. 2020. "Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Order des barreaux francophones et germanophone and Others." CJEU press release No. 123/20, October 6. https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf.

de Hert, Paul and Vagelis Papakonstantinou. 2014. "The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition." *Computer Law & Security Review* 30 (6): 633–42.

Geist, Michael. 2018. "How Canada Surrendered Policy Flexibility for Data Localization Rules in the USMCA." *Michael Geist* (blog), October 10. www.michaelgeist.ca/2018/10/how-canada-surrendered-policy-flexibility-for-data-localization-rules-in-the-usmca/.

Greenleaf, Graham. 2013. "'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?" *Computer Law & Security Review* 29 (4) 430–36.

———. 2016. "Balancing Globalisation's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe." University of New South Wales Law Research Paper No. 16-52. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2801054.

———. 2018a. "Convention 108+ and the Data Protection Framework of the EU." University of New South Wales Law Research Series. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3202606.

———. 2018b. "Asia-Pacific Free Trade Deals Clash with GDPR and Convention 108." *Privacy Laws & Business International Report* 156: 22–24.

———. 2020. "Implementing Convention 108+ — observer and NGO contributions." *Privacy Laws & Business International Report* 166: 28–30.

Greenleaf, Graham and Bertil Cottier. 2020. "2020 Ends a Decade of 62 New Data Privacy Laws." *Privacy Laws & Business International Report* 163: 24–26. https://ssrn.com/abstract=3572611.

ISED. 2019. *Fifth Update Report on Developments in Data Protection Law in Canada: Report to the European Commission.* Ottawa, ON: ISED. www.ic.gc.ca/eic/site/113.nsf/eng/h_07666.html.

ISED. 2020. "New proposed law to better protect Canadians' privacy and increase their control over their data and personal information." ISED news release, November 17. www.canada.ca/en/innovation-science-economic-development/news/2020/11/new-proposed-law-to-better-protect-canadians-privacy-and-increase-their-control-over-their-data-and-personal-information.html.

Kuner, Christopher. 2013. *Transborder Data Flows and Data Privacy Law.* Oxford, UK: Oxford University Press.

Kwasny, Sophie. 2017. "Convention 108, a Trans-Atlantic DNA?" In *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*, edited by Dan Jerker B. Svantesson and Dariusz Kloza, 533–42. Cambridge, UK: Intersentia.

Newman, Abraham L. 2008. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Ithaca, NY: Cornell University Press.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline