epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

Consultation on Transborder Data Flows

August 6, 2019

By notice published April 9, 2019, the Office of the Privacy Commissioner of Canada (OPC) opened a consultation on transfers for processing under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[1] The OPC seeks to effectively protect privacy when data is transferred across borders under PIPEDA, whether through OPC re-interpretation or amendment. The OPC's historical interpretation of the law required ongoing accountability for any personal transferred across borders, but in part the OPC proposes to enhance accountability by amending the law to provide for OPC inspection authority and to re-interpret PIPEDA to require individualized consent for data to travel across borders.

EPIC submits these comments to urge the Office of the Privacy Commissioner to (1) require that the level of personal data protection afforded individuals should be the same across borders, and (2) to require that any approach provide multiple grounds for transfer, coupled with strong accountability measures.

---

[1] Office of the Privacy Comm'r, *Consultation on transfers for processing - Reframed discussion document*, Privacy.gc.ca (June 11, 2019), https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.[2] EPIC frequently testifies before the U.S. Congress,[3] participates in the U.S. administrative agency rulemaking process,[4] and litigates landmark privacy cases.[5] EPIC has played a central role in the development of cross border data flows. EPIC President Marc Rotenberg testified to the shortcomings of EU-U.S. Safe Harbor protection before the European Parliament[6] and the U.S. Congress.[7] EPIC is also currently participating in *Data Protection Commissioner v. Facebook* before the Court of Justice for the European Union, a case assessing whether EU-U.S. data flows violate the EU Charter of Fundamental Rights.[8]

I. The level of protection afforded personal data must be the same when transferred across borders.

EPIC welcomes renewed attention to the impact of cross-border data flows on privacy protection. The level of personal data protection guaranteed to individuals under law should be

[2] EPIC, *About EPIC*, https://epic.org/epic/about.htm.
[3] EPIC, *EPIC Congressional Testimony and Statements,* EPIC.org, https://epic.org/testimony/congress/.
[4] EPIC, *EPIC Administrative Procedure Act (APA) Comments,* EPIC.org, https://epic.org/apa/comments/.
[5] EPIC, *Litigation Docket,* EPIC.org, https://epic.org/apa/comments/ https://epic.org/privacy/litigation/#cases.
[6] Testimony and Statement of Marc Rotenberg, EPIC President, The Reform of the EU Data Protection Framework— Building Trust in a Digital and Global World Before the Comm. of the European Parliament on Civil Liberties, Justice, & Home Affairs, European Parliament (Oct. 10, 2012), https://www.epic.org/privacy/Rotenberg_EP_Testimony_10_10_12.pdf.
[7] Testimony and Statement of Marc Rotenberg, EPIC President, Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows: J, Hearing Before H. Energy & Commerce Subcomm, on Commerce, Manufacturing, Trade, Comm'n & Tech. (Nov. 3, 2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf.
[8] EPIC, *Data Protection Commissioner v. Facebook & Max Schrems (CJEU)*, EPIC.org. https://epic.org/privacy/intl/dpc-v-facebook/cjeu/.

maintained regardless of the location of data. This is also efficient as there is little individuals can do if there personal data is transferred to a jurisdiction without essentially equivalent data protection. These transfers expose personal data to unanticipated processing, poor security practices, undue access by national security and law enforcement authorities, and disruptions in trade.

The guarantees of national law and international data protection instruments can be undermined if data is simply transferred to a third-country without considered safeguards and oversight to preserve protection. EPIC has argued as much before the U.S. Congress. Urging the U.S. to implement comprehensive privacy law to both protect American consumers and support trade:

> *We do not permit the import of drugs, foods, consumer products, or cars that are not safe for American consumers. It would not be fair to our companies to expect them to comply with our regulatory requirements while allowing non-US firms to ignore the same legal obligations. The same applies to European companies in Europe. It is not fair to expect them to comply with European privacy and data protection laws if the American companies do not have to comply with the same rules. Data transfers to the US are not safe for non-US individuals because the lack of adequate privacy safeguards.*[9]

Without a federal data protection law or data protection authority, the unbounded collection and storage of personal data in the United States has led to staggering increases in identity theft, security breaches, and financial fraud.[10] The 2015 Office of Personnel Management breach,

[9] Testimony and Statement of Marc Rotenberg, EPIC President, *supra* note 7, at 9.
[10] Federal Trade Comm'n, Privacy & Data Security Update (2017) https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overviewcommissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

comprising sensitive background investigation forms of federal employees,[11] and the Yahoo hack of all of the company's three billion consumer accounts are among today's many high-profile hacks.[12] Indeed, today large, unchecked troves of data are also the targets of state actors and criminals.[13] These same breaches and personal risks inevitably impact the data of foreign nationals whose data is transferred to the U.S. The 2017 Equifax data breach, which exposed the personal information of more than 145 million Americans,[14] affected close to twenty thousand Canadians.[15] The recent data breach at Capitol One impact around six million Canadians, and more than a million Social Insurance Numbers were compromised.[16]

At the same time, this is not to suggest this is simply an issue of data transfers to the U.S.; data transfer to all jurisdictions should be considered. The overall policy aim should be to preserve a high level of data protection regardless of where domestic data travels.

Any data transferred may also be subject to access by national security and law enforcement authorities, as indicated by the Court of Justice for the European Union judgment in *Schrems v. Data Protection Commissioner* (2015). In the landmark *Schrems* decision striking down the EU-U.S. Safe Harbor Arrangement, the CJEU recognized that for data to flow

---

[11] *Cybersecurity Resource Center*, OPM.gov, https://www.opm.gov/cybersecurity/cybersecurity-incidents/.
[12] *Yahoo 2013 Account Security Update FAQs*, Yahoo! Help, https://help.yahoo.com/kb/account/SLN28451.html?.
[13] Press Release, Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People (May 9, 2019), https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including.
[14] *Equifax Data Breach*, FTC.gov, https://www.ftc.gov/equifax-data-breach.
[15] Sara Merken, *Equifax Canada's Safeguards Found Lacking, Contributed to Breach*, Bloomberg Law (Apr. 9, 2019), https://news.bloomberglaw.com/privacy-and-data-security/equifax-canadas-safeguards-found-lacking-contributed-to-breach.
[16] Melissa Bennardo, *Everything Canadians need to know about the Capital One data breach*, CBC News (Jul. 30, 2019), https://www.cbc.ca/news/business/capital-one-data-breach-1.5230287.

legitimately, national security authorities, not merely consumer protections, must also comport with the fundamental rights of individuals whose data is transferred. National security authorities must be proportionate and limited to what is strictly necessary,[17] and judicial redress for any such violations of privacy and data protection rights must be available to citizens whose data is transferred.[18] The CJEU decision also indicates that data transfer policies should not simply account for consumer privacy risks, but also should give due consideration to data transfers to countries with poor relationships to the rule of law, records of persecuting dissidents, human rights defenders, and journalists, or lacking due process and strong procedural safeguards for law enforcement and national security surveillance.[19]

Finally, accountability measures must ensure data that flows across borders accords with the requisite safeguards. Without the backing of strong enforcement, companies have little incentive to abide by privacy rules. EPIC has long emphasized data transfer regimes which simply permit the self-certification to certain privacy policies without robust oversight are inadequate.[20] A data protection authority should be empowered to bring fines against companies that fail to provide safeguards and require a change in practices, and to inquire about compliance with data transfer safeguards.[21] As to the EU-U.S. data transfers the Trans Atlantic Consumer Dialogue (TACD), a coalition of consumer advocates, pushed for mandatory registration and systematic auditing of companies to check compliance and publicly posting results of the investigations to

[17] Case C-362/14, *Schrems v. Data Protection Commissioner* [2015] EU:C:2015:650, at para 93.
[18] Case C-362/14, *Schrems*, para. 95.
[19] *See e.g.,* U.S. Dep't of State, 2018 Country Reports on Human Rights Practices (2019), https://www.state.gov/reports/2018-country-reports-on-human-rights-practices/.
[20] Testimony and Statement of Marc Rotenberg, EPIC President, *supra* note 7.
[21] *Id*.

make consumers aware of how their personal information may be used.[22] TACD also urged that Data Protection Authorities be able to suspend a data flows where fundamental rights were violated.[23]

II. OPC Should Look to Strong, Tried and Tested Privacy Frameworks for Cross Border Policy

Just as facilitating data flows are important for a global technological landscape, so is protecting privacy. However, historical practice supports diverse means of achieving this aim. The OPC should look to other strong, tried and tested privacy frameworks in establishing its own modern data transfer policy under PIPEDA. Two good examples are the recently modernized Council of Europe Convention 108 ("Convention 108+") and the EU General Data Protection Regulation (GDPR). These legal authorities offer 1) multiple, sophisticated grounds on which data may be transferred, and 2) ongoing accountability for data transfers, including powers of inquiry for authorities. Compatibility with these regimes also communicates an important policy message: that a growing block of democratic nations supports free *and* rights protective flow of data.

A. Convention 108+

The Council of Europe Convention 108+, the "Modernized" Privacy Convention, is the only international privacy standard for transborder flows of personal data.[24] The Convention remains the only legally binding international instrument for The Modernized Convention, opened

[22] Trans Atlantic Consumer Dialogue, Safe Harbor, Doc No. Ecom-18-00 (2000), http://tacd.org/wp-content/uploads/2013/09/TACD-ECOM-18-00-Safe-Harbor.pdf
[23] Trans Atlantic Consumer Dialogue, Resolution on EU-U.S. Privacy Shield Proposal, Doc. No. Infosoc 54/16 (2016), http://tacd.org/wp-content/uploads/2016/04/TACD-Resolution_Privacy-Shield_April161.pdf
[24] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (CETS No. 223), Oct. 10, 2018, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223 [hereinafter Convention 108+].

for signature in October 2018, has been signed by thirty countries.[25] The Convention seeks to safeguard privacy in transborder data flows. It provides multiple grounds for legitimate data transfers, allowing for appropriate flexibility, and accountability mechanisms.

Chapter III, Article 14 lays out the rules for transborder data flows. As a general rule, where the will be data is subject to the jurisdiction of a Party to the Convention, a Party may not "for the sole purpose of the protection of personal data, prohibit or subject to special authorization the transfer of such data."[26] However, a Party may introduce special authorizations where there is either "real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention" or required by "harmonised rules of protection" within a regional international organization.[27]

Where there is sufficient protection for personal data, data may also flow freely from Party to a non-Party's jurisdiction. Specifically, the recipient of the data is subject to the jurisdiction of a non-Party, "the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured."[28] The necessary level of protection can be secured by the laws of that non-Party, or "ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing."[29]

Transfers can also always occur in other, narrow circumstances: where "the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of

---

[25] *Chart of signatures and ratifications of Treaty 223*, Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures.
[26] Convention 108+ art. 14(1).
[27] *Id*. art. 14(2).
[28] *Id*.
[29] *Id*. art. 14(3)(a-b).

appropriate safeguards"; "the specific interests of the data subject require it in the particular case;" "prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society;" or "it constitutes a necessary and proportionate measure in a democratic society for freedom of expression."[30]

Finally, Parties to the Convention must ensure entities' accountability for compliance with these cross-border standards. For those grounds transfer more susceptible to misuse, Parties must implement additional layers of oversight. Supervisory authorities must be provided proactively with all relevant information concerning the transfer of data according to standardized safeguards, and upon request, must be given information concerning data transferred based on the data subject's interests or prevailing legitimate interests.[31] Supervisory authorities must also be empowered to "request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests" and to "prohibit such transfers, suspend them or subject them to condition."[32]

Convention 108+ also addresses important emerging privacy issues such as data breach notification, biometric identifiers, and algorithmic transparency.[33] EPIC has repeatedly urged the United States to ratify the Council of Europe Privacy Convention.[34] We would recommend also that the OPC support ratification of the Convention by Canada.

B. EU General Data Protection Regulation (GDPR)

[30] *Id*. art. 4(4)(a-d).
[31] *Id*. art. 14(5).
[32] *Id*. art. 14(6).
[33] *Id*. arts. 6(1), 7(2), 9(1)(a).
[34] Letter from EPIC to Senate Comm. on Foreign Relations (Mar. 26, 2019), https://epic.org/testimony/congress/EPIC-SFR-KeithKrach-Mar2019.pdf.

The EU GPDR is a second privacy framework that models a modern data transfer regime. Like the COE 108+, the GDPR includes multiple grounds to transfer data and requires ongoing accountability for compliance with data protections safeguards.[35] Rules for transfers of personal data to third countries and to international organizations for processing are found in Chapter 5 of the GPDR. Importantly privacy protections continue to apply even when that data is later transferred from a third country or international organization to a second third country or international organization.[36]

Transfers can occur under a diverse range of privacy tools: "adequacy decisions," approved safeguards, or in strictly defined exceptional circumstances. The primary, mechanism for transferring data is an adequacy decision by the European Commission, reflecting that a country affords an "essentially equivalent" level of privacy protection as the EU.[37] Once adequacy is determined, data may flow freely between the two regions. The recent Japan-EU agreement indicated for the first time that adequacy reviews can also be mutual, with each party reviewing the other's standards.[38] Transfers can also occur under a range of approved safeguards so long as accompanied by "enforceable data subject rights and effective legal remedies for data subjects."[39] Some of these available safeguards still require prior approval by a supervisory authority for transfers. Enforceable legal instruments negotiated between public authorities, binding corporate rules approved by supervisory authorities, and standard data protection clauses approved by the

[35] Commission Regulation 2016/679, 2016 O.J. (L 119) 64.
[36] GDPR art. 44.
[37] *Id*. art. 45.
[38] Press release, European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows (Jan. 23, 2019), https://europa.eu/rapid/press-release_IP-19-421_en.htm.
[39] GDPR art. 46(1)

European Commission do not.[40] On the other hand, transfers based on contractual clauses between distinct corporate, organizational, or public entities do require approval by supervisory authorities.[41] Finally, in strictly defined circumstances transfers can occur where neither an adequacy decision nor appropriate safeguards are available: with the express and informed consent of the data subject is secured, based on a contract that is in the interest of the individual, in cases of the protection from serious bodily harm, and certain additional narrow circumstances.[42]

Each of these mechanisms is also accompanied by accountability and redress - even as implementation of these guarantees by enforcement authorities has had room for improvement in practice.[43] For example, in the case of the recent Japanese adequacy decision, Japan's data protection authority can investigate processing and issue binding decisions, EU persons are able to complaint to the Japanese authorities for redress and to file civil actions in Japanese court, and EU persons have rights to request information, access, and correction of their data.[44] As a general matter DPAs are empowered investigate compliance with data protection rules, request information, order the suspension of data flows, and more.[45] Indeed, DPAs have a responsibility to independently investigative complaints that data protection rights are not being respected, including under an adequacy decision.[46]

---

[40] *Id*. art. 46(2)
[41] *Id*. art. 46(3).
[42] *Id*. art. 49.
[43] *See, e.g.*, Comments of EPIC to the FTC "In the Matter of ReadyTech" (Aug. 1, 2018), https://epic.org/apa/comments/EPIC-FTC-ReadyTech-Settlement.pdf.
[44] European Comm'n, EU Japan Adequacy Decision (2019), https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en_2019_1.pdf.
[45] GDPR arts. 51-59, 44-50.
[46] Case C-362/14, *Schrems v. Data Protection Commissioner* [2015] EU:C:2015:650, at paras 38-66.

III. Conclusion

EPIC welcomes the decision by the OPC to review its position on cross-border data transfers. National and international privacy protections can be circumvented without sufficient guarantees that the level of protection preserved even when transferred across borders. Data protection authorities should give due weight to these privacy concerns. EPIC encourages the OPC to align a new approach to data transfers with modernized privacy frameworks like Convention 108+ and the GDPR. These frameworks seek to preserve levels of privacy protection while providing appropriate flexibility via multiple grounds for transfer. And the texts aim to provide strong accountability, backed by powers of inquiry and enforcement for DPAs.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC International Counsel