

Council of Europe Cybercrime Convention Committee (T-CY)
c/o consultation email : t-cy@coe.int
Cybercrime Division
Council of Europe
Strasbourg, France

Re: Preparing a 2nd Additional Protocol to the Budapest Convention on Cybercrime

Members,

Thank you for making the commitment and taking the time to consult with data protection experts on privacy requirements for cooperation between law enforcement in one state and service providers in another. For convenience and ease of reference, we append a copy of the OPC's previous feedback (see **Annex A**) in response to your Committee's November 2019 consultation round. For the sake of brevity, we will focus our remarks and observations specifically to the latest draft text¹ of the proposed Second Protocol:

Article 7: while provision 2.b. (page 9) provides signatories with the discretion to make such requests (for subscriber information) subject to independent oversight, it would be preferable from a legal and data protection vantage to make this a positive requirement. Independent judicial authorization should be the ideal standard, as widely as possible among cooperating authorities, given the fundamental rights that are implicated.²

Article 13: following on the point above, the direct linkage made in this article (p. 13) of the draft Protocol, between the privacy and human rights concerns at play, and a requirement for full assurance, implementation and application by all signatories, is welcome.³ As the explanatory notes remark (p. 44), necessity and proportionality (as well as non-discrimination) must be built into the internal processes for making data requests for the very reason alluded to; namely, that privacy is a globally protected human right, where risks are heightened in the context of international investigations by police.

.../2

¹ Draft text of the second additional Protocol to the Budapest Convention was approved on 12 April by the T-CY Protocol Drafting Plenary - <https://rm.coe.int/2nd-additional-protocol-budapest-convention-en/1680a2219c>.

² See also OPC *Submission on review of the state of federal laws on broadcasting and telecommunications* (January 11, 2019), sections 6-8 - URL: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ised_190111/

³ See also ICDPPC *International Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising Other Fundamental Rights* (October 2019) - <http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf>

Article 14: the data protection principles listed here (pp. 19-22) appear to draw upon feedback provided previously by EU data protection authorities, and aim to codify key principles such as limits upon secondary use, the importance of accuracy, prohibitions on discrimination, limits upon retention and onward transfer, and transparency. From a rights protection standpoint, these are all critically important, but also require the necessary support to apply actively in the criminal investigation context. We encourage the Committee to give a full hearing to concerns expressed by our colleagues in EU data protection offices as to the hurdles and resource constraints they have in the domain of overseeing ongoing law enforcement activities.⁴

In addition, we have the following discrete comments to make about specific paragraphs under article 14:

Paragraph 6 provides for protections in relation to “automated decisions.” We applaud these measures; however, the wording of the current text describes the scope of application of the protections in what looks to be very broad. In particular, it unclear whether these protections apply solely to the law enforcement context or beyond. To avoid confusion in either case, or data protection authorities having to interpret this provision, we recommend clarifying its extent in some manner.

Paragraph 7.b provides a risk-based incident response protocol. We agree with this approach; however, the current text does not explicitly require the *containment* of the security incident, only the mitigation of its effects. To address this, we recommend rewording the initial clause to state that, “the receiving Party ... shall promptly *contain the incident and* take appropriate action to mitigate such harm.” There is also some ambiguity to the use of ‘promptly’; ‘immediately’ might be better suited, given the potential sensitivities.⁵

Paragraph 11.a describes notice modalities. In particular, it provides that “Each Party shall provide notice through the publication of general notices or through personal notice to the individual whose personal data has been collected” We agree that these are the two

.../3

⁴ International Working Group on Data Protection in Telecommunications, “Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes” (April 2018) – URL: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2018/2018-IWGDPT_Working_Paper_Cross-border_data_requests.pdf

⁵ E.g, Section 3 of Government of Canada’s TBS *Guidelines for Privacy Breaches* (May 2014) - <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154>

appropriate modalities. However, the description of general notices lacks implementation detail. To address this, we recommend adding that, “Each Party shall provide notice through the publication of general notices *on its organizational website or other publicly accessible media*”

Paragraph 11 is entitled “Transparency and notice.” However, we note that it does not contain a requirement for receiving Parties to implement formal public reporting of aggregate statistics about requests. We recommend that the paragraph be modified to contain such a requirement, as transparency reports are a key measure towards providing the public with adequate information regarding the domestic activities of foreign law enforcement authorities.

Thank you again for seeking consultation with the data protection community as you continue your ongoing work. Should you have any follow-up questions or need additional input, please feel free to contact Chris Prince (Christopher.Prince@priv.gc.ca) in the Policy, Research and Parliamentary Affairs Directorate of my Office for any needed clarifications.

Sincerely,

Gregory Smolynec
Deputy Commissioner
Policy and Promotion Sector

Enclosure

JAN 14 2019

Council of Europe Cybercrime Convention Committee (T-CY)
c/o Nina Lichtner
Cybercrime Division
Council of Europe
Strasbourg, France

Re: Preparing a 2nd Additional Protocol to the Budapest Convention on Cybercrime

Members,

Thank you for taking the time to consult with data protection experts on privacy requirements for cooperation between law enforcement in one state and service providers in another. You are in particular examining interactions between the Budapest Convention and the requirements of Convention 108 I believe. Consequently, you are consulting Members of the European Data Protection Board as well as the European Data Protection Supervisor. I believe that to be an important step in your development process. However, given that Canada itself is not a party to Treaty 108¹, I will confine my input to the privacy implications stemming from the two specific legal procedures that your Committee is considering. These proposals are:

- 1) *An order or similar request for subscriber information (and possibly other data) from a competent authority in one Party to a service provider in another Party, and the direct transmission of such information (or data) by a service provider to the requesting Party in return, and,*
- 2) *A request for the expedited preservation of stored computer data from a competent authority in one Party directly to a service provider in another Party and the actual preservation [without disclosure] of such data by the service provider.²*

Legal context around collection of digital evidence

As noted in your meeting backgrounder, in recent years, high-level courts in multiple jurisdictions have annulled warrantless police powers for searches and seizures of subscriber

.../2

¹ Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – Status as of 13/11/2018* – URL: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?desktop=true>

² Cybercrime Convention Committee (T-CY), *Consultation with data protection experts* – URL: <https://rm.coe.int/t-cy-2018-31-pdp-consult-dataprotection-outline/16808e4e28>

information, citing constitutional protections and privacy law.³ Since the 2001 Convention was first signed, decisions of the German Constitutional Court, Supreme Court of Canada, EU Court of Justice and European Court of Human Rights have all disallowed the practice of police authorities collecting subscriber data or metadata without court authorization. In many jurisdictions, these questions are “settled law”.

While I appreciate this can create delays for government investigators and justice officials, the overall direction from the courts seems to me relatively clear. Independent judicial oversight may take time, but it is indispensable in the specific context of law enforcement investigations.

Relevant input on data protection requirements

That said, as a regulator with an investigative function, I also understand the need to develop clear legal process for obtaining relevant data held in other jurisdictions. Data protection authorities are aware this can create some delay. Given your specific focus, I would refer your Committee specifically to an April 2018 paper by the International Working Group on Data Protection in Telecommunications entitled *Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes*.⁴

This group is comprised of technical specialists from data protection offices examining privacy in the context of new technologies like cloud computing. My Office contributed directly to the development of standards to ensure data protection safeguards for any new procedure for “law enforcement cross-border data transfer” when personal information is at issue.

For ease of reference, those necessary safeguards are:

1. **Accountability.** *The transfer mechanisms should ensure that all actors in the process are appropriately accountable for their actions;*
2. **Procedural Fairness (Due Process).** *The transfer mechanisms should ensure that data subjects are guaranteed their rights of procedural fairness (due process) including both clear and transparent legal standards and procedures for requests;*
3. **Efficacy.** *Efficacy of strong transfer mechanisms should be prioritized to facilitate prompt and regular processing of requests, including through the establishment of*

.../3

³ Cybercrime Convention Committee (T-CY) Preparation of 2nd Additional Protocol to the Budapest Convention on Cybercrime, *Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments - Discussion paper* - <https://rm.coe.int/t-cy-2018-26-ip-addresses-v6/16808ea472>

⁴ International Working Group on Data Protection in Telecommunications, “Working paper on Standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes” (April 2018) – URL: https://www.datenschutz-berlin.de/fileadmin/user_upload/publikationen/working-paper/2018/2018-IWGDPT_Working_Paper_Cross-border_data_requests.pdf

mutually understood interpretations of any legal standards and procedures for requests and robust resourcing of transfer mechanisms;

4. **Notice and Opportunity to Challenge.** *Data subjects should have a right to notice and an opportunity to challenge a foreign state's request for access to their personal data;*
5. **Necessary and Proportionate Determination.** *No one should be subject to a lesser standard of legal process than permitted in applicable international human rights law and data protection and privacy frameworks, including necessity and the proportionality to legitimate aims;*
6. **Judicial Authorization.** *The requests should be subject to judicial authorization and review;*
7. **Oversight.** *There should be appropriate independent oversight of transfer mechanisms;*
8. **Transparency mechanism.** *Formal public reporting of aggregate statistics about requests should be required.*⁵

Direct requests for subscriber information and other data

On access to subscriber data specifically, I would offer that here in Canada federal officials and law enforcement consulted the privacy community last summer on expediting access. That discussion followed the unanimous Supreme Court of Canada decision in *R. v. Spencer*, referenced in your Committee background paper.⁶ We noted in response to that decision that government authorities seem preoccupied with:

*... distinguishing certain data elements (for example, IP addresses or IMEI numbers) from individuals' subscriber data, in an attempt to classify one or the other as less sensitive. Since Spencer, however, this seems to us a distinction without a difference. The elements at issue... constitute metadata of one type or another, and can be used to identify individuals ... metadata can be highly revealing and sensitive.*⁷

All that to say, I do not believe lowered thresholds for access to subscriber data, metadata, transmission data - or however else one redefines personal information in this context - will bear legal scrutiny. The collective input which Canadian privacy officials provided also stressed the pivotal roles of independent court authorization for data access "consistent with the rule of law" because the "courts are best placed to balance the law enforcement interests of the

.../4

⁵ Ibid, page 6.

⁶ Cybercrime Convention Committee (T-CY), *Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments - Discussion paper*, pp. 10-11 - <https://rm.coe.int/t-cy-2018-26-ip-addresses-v6/16808ea472>

⁷ Letter from Canadian Privacy Commissioners to the Cybercrime Working Group of the Committee of Senior Officials on Criminal Justice (CCSO), June 2017, p. 2

police and the privacy interests of individuals” prior to collection.⁸ I would simply take this occasion to reiterate that bedrock safeguard as a prerequisite for any new proposal.

Direct requests for data preservation

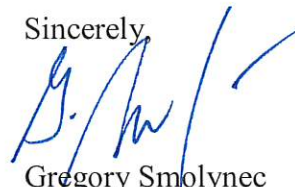
Finally, on the issue of data preservation, in a separate consultation by public safety officials in Canada, our office noted the importance of developing a tailored approach that does not cast requests for retention that are overly broad. I noted that:

... law must reflect the fact that metadata can reveal personal information that is more sensitive than the data for which warrants have traditionally been required in the pre-digital world ... It must also ensure that modern investigative tools do not violate the privacy of law-abiding citizens ... collection of metadata could be limited to cases where all other investigative methods have been exhausted and for violent crimes where public safety may outweigh privacy risks ... there should be conditions aimed at protecting the privacy of people incidentally targeted by a warrant, but not suspected of involvement in a crime. For example, use of the data could be restricted to the crime being investigated, and metadata not related to criminal activity destroyed without delay.⁹

I also noted, in many jurisdictions, “preservation orders are a current tool available by law enforcement to ensure that a communications company’s customer data is not deleted during an investigation.” Therefore, I have generally advised government against broad requirements for companies to retain customers’ data without a court order. Data minimization remains a key data protection safeguard - so unless preservation demands comport to legal requirements of duration and particularity - they are inconsistent with this privacy principle.¹⁰

Thank you again for seeking consultation with the data protection community as you continue your ongoing work. If you should have any follow-up questions or need additional input, please feel free to contact my Office.

Sincerely,



Gregory Smolynec
Deputy Commissioner
Policy and Promotion Sector

⁸ Ibid, p. 5

⁹ OPC, Backgrounder – Metadata in a criminal law context (December 2016) – URL: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/bg_161206/

¹⁰ OPC, Submission to the National Security Policy Directorate of Public Safety Canada – Section II: Retention (December 2016) – URL: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_psc_161205/