Consultations on the 2nd Additional Protocol to the Convention on Cybercrime

Towards the 2nd Additional Protocol to the Budapest Convention on Cybercrime:

6th round of consultations with stakeholders

Online, 6 May 2021, and written submissions

Agenda

Part 1: Overview and review of Chapter II	Part 2: Safeguards
• Opening remarks and overview of the Protocol • Chapter II: Summary of comments received • Discussion	• Overview of the safeguards of the Protocol • Summary of comments received • Discussion

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

1

6th round of consultations: submissions received

- Access Now
- Asociacion por los Derechos Civiles (ADC)
- Council of Bars and Law Societies of Europe (CCBE)
- Council of European National Top-Level Domain Registries (CENTR)
- European Association of Trade Mark Owners (MARQUES)
- European Data Protection Board (EDPB)
- European Digital Rights et al (EDRI)
- EuroISPA
- EU Fundamental Rights Agency (FRA)
- ICANN
- Joint Civil Society
- Kaspersky
- Privacy Commissioner of Canada
- Privacy Commissioner of New Zealand

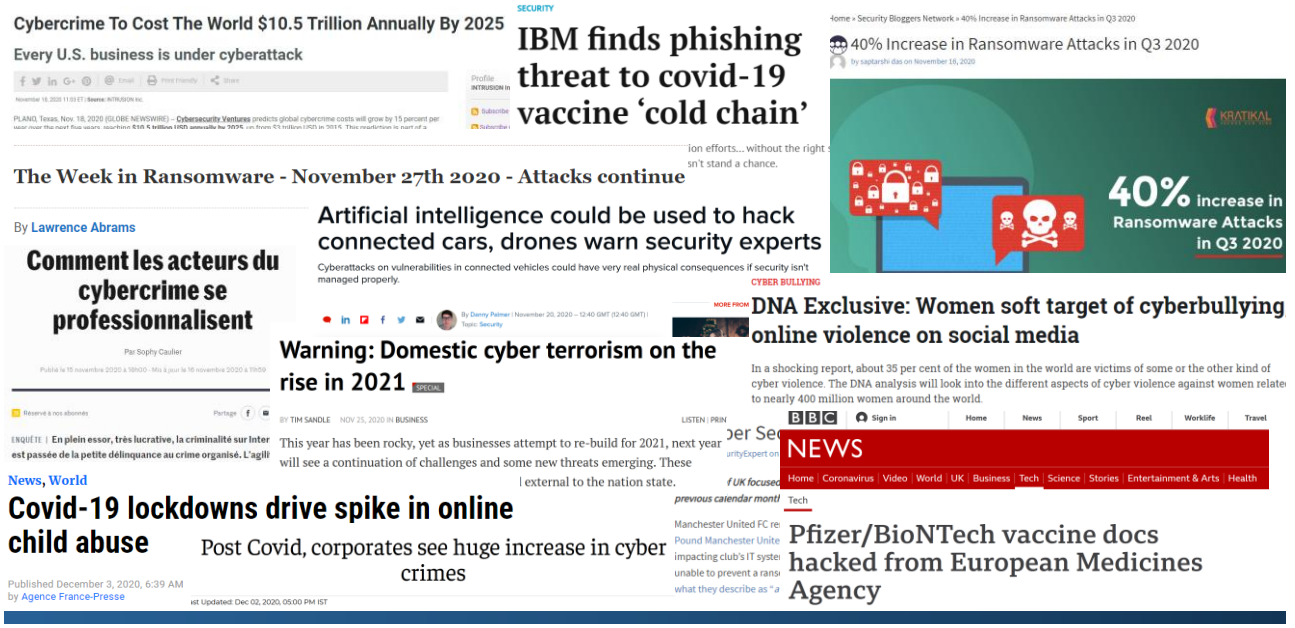
2

6th round of consultations: preliminary observations on submissions

- Contributions helped test the validity of the tools of the Protocol. Some answers already in the text but some may need to be explained further.
- The tools of the Protocol will not work in isolation but will need to be implemented and will be embedded in the domestic legal systems of a Party. The criminal justice systems of Parties include safeguards and systems of supervision.
- The Protocol is supplementing but not amending the Budapest Convention.
- The Protocol, like the Convention, is a criminal law treaty and applies to specific criminal investigations and proceedings (see Article 2 – Scope of application)
- Article 14 on the protection of personal data is the most detailed provision of the Protocol (covering some 20% of the text), required more meetings than any other provision, and delegations comprised data protection experts.
- The Budapest Convention is a treaty with currently 66 Parties (including 21 that are not member States of the COE and 40 that are not members of the European Union). The Protocol needs to work for all of them and more. Flexibility needed to permit adaptation to different legal systems.
- Victims.

3

Rationale: Why a 2nd Additional Protocol to the Budapest Convention?



4

Rationale: Why a 2nd Additional Protocol to the Budapest Convention?

- ► 1% of cybercrime reported to criminal justice?
- ► 1% of cases reported resulting in convictions?

- Problem of rule of law in cyberspace?
- No/limited expectation of justice for victims?
- Do governments meet their obligation to protect individuals against crime?
- Primary response by national security bodies; residual response by criminal justice system?

5

Rationale: Why a 2nd Additional Protocol to the Budapest Convention?

Why a new Protocol?

- The scale and quantity of cybercrime, devices, users and victims
- Cloud computing, territoriality and jurisdiction
  - Where is the crime?
  - Where is the data, where is the evidence?
  - Who has the evidence?
  - What legal regime applies to order / disclose data?
- The challenge of mutual legal assistance
- The 0.1% problem

- ► **How to obtain subscriber information efficiently?**
- ► **How to cooperate directly with a service provider in another Party?**
- ► **How to obtain WHOIS data (domain name registration information) from registrars?**
- ► **How to obtain stored data, including content, in an emergency situation?**
- ► **How to make mutual assistance more effective?**
- ► **How to reconcile efficient and effective measures with rule of law and data protection requirements?**

www.coe.int/cybercrime

6

Background to the 2nd Additional Protocol to the Budapest Convention on Cybercrime

- Preparatory work of the Cybercrime Convention Committee (T-CY):
  - Transborder Group (2012-2014)
  - Assessment of MLA provisions (2014)
  - Cloud Evidence Group (2014- 2017)
  - Need for Protocol identified
- T-CY 17 (June 2017): Terms of reference adopted
- T-CY 23 (Nov 2020): TOR extended to May 2021
- 9 Drafting Plenaries + 16 Drafting Group meeting + 60 virtual subgroup meetings + 6 rounds of consultations + numerous bi/trilateral meetings + domestic meetings

7

Inventory of meetings to prepare the draft Protocol

- 1st Meeting of the T-CY Protocol Drafting Group (Strasbourg, 19-20 September 2017)
- 1st Meeting of the T-CY Protocol Drafting Plenary (Strasbourg, 28-29 November 2017)
- 2nd Meeting of the T-CY Protocol Drafting Group (Strasbour, 1-2 February 2018)
- 3rd Meeting of the T-CY Protocol Drafting Group (Vienna, 11-13 May 2018)
- 2nd Meeting of the T-CY Protocol Drafting Plenary (Strasbourg, 10-11 July 2018)
- 4th Meeting of the T-CY Protocol Drafting Group (Strasbourg, 17 – 19 September 2018)
- 3rd Meeting of the T-CY Protocol Drafting Plenary (Strasbourg, 28 – 29 November 2018)
- 5th meeting of the Protocol Drafting Group (Strasbourg, 11-13 February 2019)
- 6th meeting of the Protocol Drafting Group (Vienna, 25 – 26 March 2019)
- 7th meeting of the Protocol Drafting Group (Strasbourg, 13 – 15 May 2019)
- 4th meeting of the Protocol Drafting Plenary (Strasbourg, 9 – 11 July 2019)
- 8th meeting of the Protocol Drafting Group (Paris, 16 – 18 September 2019)
- 9th meeting of the Protocol Drafting Group (Strasbourg, 15 – 18 October 2019)
- 5th meeting of the Protocol Drafting Plenary (Strasbourg, 19 – 20 November 2019)
- 10th meeting of the Protocol Drafting Group (Strasbourg, 21 – 24 January 2020)
- 11th meeting of the Protocol Drafting Group (virtual meeting, 2, 4 and 9 June 2020)
- 12th meeting of the Protocol Drafting Group (virtual meeting, 30 June – 2 July 2020)
- 13th meeting of the Protocol Drafting Group (virtual meeting, 3, 4, 8 and 9 September 2020)
- 6th meeting of the Protocol Drafting Plenary (virtual meeting, 22 – 25 September 2020)
- 14th meeting of the Protocol Drafting Group (22 – 28 October 2020)
- 15th meeting of the PDG (16 November 2020)
- 7th meeting of the Protocol Drafting Plenary (1 – 3 December 2020)
- 16th meeting of the PDG (22-24 February 2021)
- 8th meeting of the Protocol Drafting Plenary (26 February 2021)
- 9th meeting of the Protocol Drafting Plenary (12 April 2021)

Stakeholder consultations

1. July 2018
2. Nov 2018
3. Feb 2019
4. Nov 2019
5. Dec 2020
6. Apr/May 2021

9 Dec 20	27. Data protection
17 Dec 20	28. Structure
18 Dec 20	29. Structure
8 Jan 21	30. Data protection
11 Jan 21	31. Structure
13 Jan 21	32. Data protection
19 Jan 21	33. Structure
22 Jan 21	34. Structure
26 Jan 21	35. Data protection
27 Jan 21	36. Structure
29 Jan 21	37. Structure
4 Feb 21	38. Data protection
5 Feb 21	39. Structure
11 Feb 21	40. Data protection
12 Feb 21	41. Structure
18 Feb 21	42. Data protection
19 Feb 21	43. Structure
4 Mar 21	44. Data protection
5 Mar 21	45. Structure
11 Mar 21	46. Data protection
12 Mar 21	47. Structure
18 Mar	48. Data protection
19 Mar	49. Structure
25 Mar	50. Structure/DP
26 Mar	51. Structure/DP
29 Mar	52. Structure/DP
30 Mar	53. Structure/DP
16 Apr	54. Data protection
20 Apr	55. Data protection
22 Apr	56. Structure/DP
23 Apr	57. Structure/DP
27 Apr	58. Structure/DP
30 Apr	59. Structure/DP
5 May	60. Structure/DP

8

2nd Additional Protocol to the Convention on Cybercrime: content

Preamble

Chapter I: Common provisions

Article [1] Purpose
Article [2] Scope of application
Article [3] Definitions
Article [4] Language

Chapter II: Measures for enhanced cooperation

Section 1 – General principles applicable to Chapter II

Article [5] General principles applicable to Chapter II

Section 2 – Procedures enhancing direct cooperation with providers and entities in other Parties

Article [6] Request for domain name registration information
Article [7] Disclosure of subscriber information

Section [3] – Procedures enhancing international cooperation between authorities for the disclosure of stored computer data

Article [8] Giving effect to orders from another party for expedited production of subscriber information and traffic data
Article [9] Expedited disclosure of stored computer data in an emergency

Section [4] – Procedures pertaining to emergency mutual assistance

Article [10] Emergency mutual assistance

Section [5] – Procedures pertaining to international cooperation in the absence of applicable international agreements

Article [11] Video conferencing
Article [12] Joint investigation teams and joint investigations

Chapter III – Conditions and safeguards

Article [13] Conditions and safeguards
Article [14] Protection of personal data

Chapter IV: Final provisions

Article [15] Effects of this Protocol
Article [16] Signature and entry into force
Article [17] Federal clause
Article [18] Territorial application
Article [19] Reservations and declarations
Article [20] Status and withdrawal of reservations
Article [21] Amendments
Article [22] Settlement of disputes
Article [23] Consultations of the Parties and assessment of implementation
Article [24] Denunciation
Article [25] Notification

9

2nd Additional Protocol to the Convention on Cybercrime: benefits

Benefits of the Protocol

Operational value:

- Basis for direct cooperation with service providers for subscriber information ("direct disclosure")
- Effective means to obtain subscriber information and traffic data ("giving effect")
- Legal basis for disclosure of WHOIS information
- Cooperation in emergencies ("expedited disclosure" + "emergency MLA")
- Mutual assistance tools ("video-conferencing", "JITs")
- Data protection safeguards to permit the flow of personal data under the Protocol

Policy value:

- Convention on Cybercrime will remain relevant and effective
- Efficient cooperation with rule of law and data protection safeguards is feasible
- Respect for free Internet with limited restrictions in case of criminal misuse (specific criminal investigations, specified data)

10

Chapter II: Measures for enhanced cooperation

Section 1 – General principles applicable to Chapter II
Article [5] General principles applicable to Chapter II
Section 2 – Procedures enhancing direct cooperation with providers and entities in other Parties
Article [6] Request for domain name registration information
Article [7] Disclosure of subscriber information
Section [3] – Procedures enhancing international cooperation between authorities for the disclosure of stored computer data
Article [8] Giving effect to orders from another party for expedited production of subscriber information and traffic data
Article [9] Expedited disclosure of stored computer data in an emergency
Section [4] – Procedures pertaining to emergency mutual assistance
Article [10] Emergency mutual assistance
Section [5] – Procedures pertaining to international cooperation in the absence of applicable international agreements
Article [11] Video conferencing
Article [12] Joint investigation teams and joint investigations

General comments:

- Mutual assistance should be favoured over direct requests or orders.

Mandatory judicial or other independent approval of requests or orders:

- All cross-border data requests must be subject to prior or simultaneous independent review (including by the judiciary) to establish a proper legal basis and dual criminality and to protect legal professional privilege and professional secrecy
- Requests for WHOIS data, expedited disclosure of stored computer data in an emergency, direct disclosure of subscriber information and the disclosure of IP addresses must be issued only with independent authorisation, including judicial authorisation. Giving effect to another Party's order and JIT agreements also require such authorisation
- WHOIS data and direct disclosure of subscriber data: such prior authorisation must be done by the Party where the provider is located, at least to establish dual criminality and a proper legal basis
- Expedited disclosure of stored computer data in an emergency: only a judicial or similar independent authority may issue such requests, after a special showing of imminence, impossibility, etc, to ensure that the emergency differs from cases where emergency MLA could be used.
- Ensure that suspected or accused persons, or their lawyers are able to request the issuing of international production or preservation orders in an equally efficient way as is possible for law enforcement authorities, so as to ensure the observance of the principle of equality of arms between the prosecution and defence, without which the defendant is placed at a significant disadvantage.

13

Chapter II: Summary of comments received

Mandatory notification to the authorities or requested States or States of residence:

- All WHOIS data and direct disclosure of subscriber data: when requests are sent directly to domain name entities or service providers in another State, that State must be notified.
- Direct disclosure of subscriber data: consider notifying the affected person's country of residence when requests are sent directly to service providers.

Mandatory notification to the person whose data is sought

- Data protection laws may require notification to data subjects if their personal data is processed for a purpose other than the one for which it was collected or if disclosed to a third party. A request for non-notification cannot override data protection obligations
- WHOIS data: at the earliest opportunity (or immediately after any jeopardy to an investigation has ceased), the targeted person must be notified of the request. Domain name entities must be able to do such notifications

14

Allowing private sector entities to consult with authorities regarding a request and/or to object to it

- Direct disclosure of subscriber information and expedited disclosure of stored computer data in an emergency: service providers must be able to consult with authorities before executing requests and to challenge requests
- WHOIS data: domain name entities must be able to object to data access requests by foreign authorities and to require additional information from them
- Service providers or State authorities must be given enough information to be able to reject manifestly abusive requests

Creation of public oversight mechanisms

- All cross-border requests, especially expedited disclosure of stored computer data in an emergency: the Protocol must include accountability and public oversight mechanisms, including penalties for blatant or systemic misuse of emergency powers
- Annual statistical and qualitative reporting on all cross-border requests [or on the number of expedited disclosures] must be published by requesting and responding Parties. Service providers must also publish transparency reports
- JITs: JITs must be subject to independent oversight mechanisms in each participating Party. Oversight bodies must be able to access all relevant information about JITs and joint team activities, including confidential information. Each Party must publish periodic reports about the lawfulness of JIT actions and their compliance with principles
- Direct disclosure of subscriber information: consider independent oversight of the issuing authority

Chapter II: Summary of comments received

Article 6 Request for domain name registration information

- Clarify whether Article 6 (WHOIS) applies to "entities providing domain name REGISTRATION services" or any "entities providing domain name services", including domain name resolution services, resellers, privacy proxy providers etc.
- Explain interplay between Articles 6 and 7. Could Article 7 be used to order the production of WHOIS data or does Article 6 block Article 7?
- The voluntary regime of Article 6 and the required 6.1.f-type balancing test by entities is likely to slow down or exclude international transfers.
- Add to Article 6(2): Each Party shall adopt such legislative and other measures as may be necessary to permit an entity in its territory to disclose such information in response to a request under paragraph 1, subject to reasonable and proportionate conditions provided by domestic law, including a clear legal basis.
- Article 6 must include an explicit reference to appropriate safeguards pursuant to Articles 13 and 14 of the protocol, including grounds for objection

17

Chapter II: Summary of comments received

Article 6 Request for domain name registration information

- WHOIS data and direct disclosure of subscriber data: when requests are sent directly to domain name entities or service providers in another State, that State must be notified
- WHOIS data: at the earliest opportunity (or immediately after any jeopardy to an investigation has ceased), the targeted person must be notified of the request. Domain name entities must be able to do such notifications
- WHOIS data: domain name entities must be able to object to data access requests by foreign authorities and to require additional information from them.
- WHOIS data: requests must state a necessary and proportionate legal basis under the applicable domestic law, including data protection law
- WHOIS data: requesting third countries Parties must be bound to comply with proportionality when addressing requests to an EU Member State and it must be clear that proportionality can be invoked as a ground for refusal

18

Chapter II: Summary of comments received

Article 7 Disclosure of subscriber information

- All production orders under the Protocol: professional secrecy, legal professional privilege and dual criminality must be explicit grounds for declining execution. Reference must be made to immunities and privileges applicable under the laws of the Parties where the service provider is located, where the person whose data is sought resides, and where that person is bound by obligations or privileges
- Broad concept of "subscriber information". IP addresses should not be included if they reveal intimate details and conclusions to be drawn of a person's life or everyday actions.

19

Chapter II: Summary of comments received

Article 7 Disclosure of subscriber information

- Avoid confusion between (future) EU E-evidence Regulation and this Protocol
- Mandatory introduction of a unified electronic data exchange system
- The drafting and subsequent use of templates
- Installation of a single point of contact (SPOC)
- Ex-ante review of a production order under Article 7 by a judge or other independent authority
- Exclusion of SMEs
- Cost reimbursement in the receiving Party

20

Chapter II: Summary of comments received

Article 11 Video conferencing

- Art. 11 (1) in conjunction with Art. 11 (5): The *ne bis in idem* principle could be reflected in the Protocol to avoid double penalization of the witness in case of a false statement or perjury/false oath, if both states administered the oaths, warnings and instructions.
- Art. 11 (7): If video conferencing technology is generally permitted by the Protocol, it should also accommodate witness protection measures available at national level, such as e.g. face or voice distortion.

21

Chapter II: Summary of comments received

Article 12 Joint investigation teams and joint investigations

- The terms in JIT agreements regarding accessing personal information and electronic or other evidence must be publicly accessible
- JITs must be limited to investigative measures that are authorised under the domestic laws of all participating Parties, especially those of the territory where the investigation is carried out. Domestic laws governing potentially very intrusive investigative measures are likely to differ considerably or may be prohibited/permitted in certain Parties
- JIT-obtained data must be repurposable only in emergencies
- JITs: JITs must be subject to independent oversight mechanisms in each participating Party. Oversight bodies must be able to access all relevant information about JITs and joint team activities, including confidential information. Each Party must publish periodic reports about the lawfulness of JIT actions and their compliance with principles

22

Chapter III: Conditions and safeguards

Safeguards

- Criminal justice treaty: Specified data needed in specific criminal investigations
- Differentiated approach regarding categories of data
- Confidentiality, use limitation, grounds for refusal
- Notification, reservations, declarations
- Article 13 – Conditions and safeguards
- Article 14 – Protection of personal data

Chapter III – Conditions and safeguards

Article [13] Conditions and safeguards

Article [14] Protection of personal data

1. Scope
2. Purpose and use
3. Quality and integrity
4. Sensitive data
5. Retention periods
6. Automated decisions
7. Data security and security incidents
8. Maintaining records
9. Onward sharing within a Party
10. Onward transfers to another State or organisation
11. Transparency and notice
12. Access and rectification
13. Judicial and non-judicial remedies
14. Oversight
15. Consultation and suspension

23

Chapter III: Summary of comments received

- Transfers of personal data have to be compatible with EU law (GDPR)
- Accession to data protection Convention 108+ should be a requirement for Parties to the Protocol
- Data protection safeguards must include lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and access, rectification, erasure, effective judicial redress for data subjects and notification of the data subject (at least once this no longer endangers the investigation). Any restrictions must be limited by proportionality. These principles, rights and obligations must apply to all authorities processing the data in the requesting Party. Personal data must be collected only when the collection is adequate, relevant and necessary for the stated purpose; Parties must establish an authority with expertise in data protection; that authority must oversee the proportionality of the orders, requests and transfers of data

24

Article 14

- Article 14(2) Purpose and use: Processing should be proportionate and a legitimate purpose should be pursued. This article should explicitly state that processing will be done for a legitimate purpose only and any processing done will be proportionate.
- Article 14(5) Retention periods: It should be specified that personal information shall not be retained for longer than required. In other words personal information should be retained until there is a lawful purpose to retain such personal information.
- Article 14 (5): The retention periods could be defined further, clarifying:
  - whether the data should be kept until an investigation is concluded, until a judgment is delivered, until a judgment is final or until a sentence is served;
  - when a "proceeding" is to be considered finished; and
  - for how long after such proceedings and for what particular reasons the data shall be kept.
- Article 14 (8): Further guidance concerning the records to be maintained could also be considered. This guidance could clarify to what personal data these records should be limited and when and under which circumstances (maintained) records will be deleted.
- Article 14(10)(a) Onward transfer to another State or international organisation: The article should include that personal information can be transferred with the authorisation of the transferring authority and when the other state or international organisation has comparable privacy safeguards.
- Article 14(11): Transparency and notice: consider requirement for receiving Parties to publish aggregate data on requests from foreign law enforcement.
- Article 14(13): Judicial and non-judicial remedies: more detailed requirements should be provided

Article 14.1.d (data protection scope) + Article 7 Direct disclosure

- Article 14.1.d: The wording proposed is unclear as on the one hand, it stipulates that the disclosure of personal data based on the Second Additional Protocol shall be considered "to meet the requirements of data protection frameworks for international data transfers" and shall need "no further authorization". *It* remains unclear to what extent the disclosure of personal data which falls under the scope of the GDPR to a law enforcement authority in a third country, would be permitted.
- Considering that the Protocol is not directly applicable for neither the concerned service providers nor the affected users, this assessment will also have to consider the national implementation of the safeguards foreseen in Article 14. Nevertheless, it should be avoided that it is left to the service providers concerned to carry out this legal assessment on a case-by-case basis.
- Reciprocal trust of Parties' data protection framework under Article 14 (1)(d) must be replaced by each Party's assessment of the other Party's adequacy.