Public Consultation Response
2nd Additional Protocol to the Budapest Convention on Cybercrime
4th Round of Consultation

INTRODUCTION

Facebook welcomes the Council of Europe ("CoE") and the Cybercrime Convention Committee's ("T-CY") continued international leadership in addressing the complex problem of global access to electronic evidence. The ability to detect, prevent and prosecute crime is an important concern for governments. Governments have a responsibility to protect people and their privacy. Technology companies headquartered in the U.S. are also key stakeholders in this discussion. We would like to reiterate that we take seriously our responsibility to maintain the safety, security, and privacy of our 2.7 billion users around the world. We are also committed to being transparent in the way that we do this.

As a member of the Reform Government Surveillance ("RGS") coalition[1], we believe the best way for countries to promote the security and privacy interests of their citizens, while also respecting the sovereignty of other nations, is to ensure that government access to data is targeted, lawful, proportionate, necessary, transparent and avoids conflicts of law. This is a significant achievement that should not be underestimated.

We recognise that it is in the interests of our users that their local law enforcement agencies carry out investigations into suspected criminal activity. We acknowledge that the combination of national and international procedures in this area can make the process of seeking data lawfully confusing for many governments, NGOs and users. We also acknowledge that the legal framework governing cross-border requests needs to be significantly improved.

We therefore welcome the opportunity to provide feedback to the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime during this fourth round of consultations. We hope that the finalisation and implementation of the 2nd Additional Protocol will provide clear and high standards that continue to move forward the debate on international data access standards and Mutual Legal Assistance Treaties ("MLAT") reform.

[1] www.reformgovernmentsurveillance.com

Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lambe, Yvonne Cunnane
Company No. 462932

GENERAL CONSIDERATIONS

There are some preliminary considerations that shape Facebook's view of what good regulation in this area looks like:

Maintaining a Voluntary Process as a First Option

The primary concern animating the need for this 2nd Additional Protocol is the regular and significant delay law enforcement authorities experience when making cross-border data requests. These delays are exacerbated by significant backlogs in processing mutual legal assistance ("MLA") requests in the central authority of most governments. The voluntary process established in Article 4, which generally matches existing practices in some jurisdictions, is critical to ensuring that governments can continue to make direct requests of service providers for data, while improving governments' ability to access certain data that is controlled by providers in other jurisdictions.

Recommendation: Additional standards and safeguards recommended in the following section should be built into Articles 4 and 5 to ensure that both the voluntary and compulsory processes for producing data in response to requests provide robust protections for privacy and human rights.

Establishment of a Single Point of Contact

Whilst Facebook, as a large service provider, has the resources to manage the authentication of legal processes, we support the need for smaller companies to have a reliable authentication process. It may be difficult for small providers operating in jurisdictions across the globe to verify each national authority's stamp and signature. A preferred option to address this concern would be to ensure that all requests issued under the 2nd Additional Protocol be issued from and directed to a national Single Point of Contact ("SPOC"), rather than directly sent by jurisdictional authorities. This could include individual SPOCs (or groups of SPOCs) in each region, law enforcement agency or city, or it could be a national unit or group of SPOCs. Establishing a clear point of contact for providers creates huge value for both the requesting jurisdiction and the service provider that receives data requests. SPOCs increase opportunities for advice and training, and the development of expertise, and they help to ensure harmonisation and a secure method of data transfer.

Recommendation: Article 4 should be amended to require requests made pursuant to the 2nd Additional Protocol be made through a SPOC.

Conflict of Law

Whilst we support the necessary work to improve the processes for making cross-border data requests and reducing the burden on MLA processes around the world, it is critical that any new legal mechanism for making requests or compelling data production articulate how it will prevent any conflict of law from arising, or address one that does arise. For example, Parties such as the Member States of the European Union are considering, and will ultimately implement, mechanisms like the European Production Order ("EPO") as part of the E-Evidence Regulation

Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lambe, Yvonne Cunnane
Company No. 462932

that would compel data production. If the Plenary Drafting Party does not address this possibility in the text of the 2nd Additional Protocol, Parties may make requests that create conflicts of law, or raise questions about which legal regime should be treated as the primary process for making data requests.

Recommendation: The Plenary Drafting Party should clarify that where there is an existing compulsory intergovernmental regime for issuing demands for digital evidence, Parties that are subject to those compulsory regimes should solely rely on them to obtain digital evidence.

SPECIFIC CONSIDERATIONS – STANDARDS AND SAFEGUARDS

We very much welcome the establishment of a process for making cross-border requests for basic subscriber information and traffic data. However, we believe that the following provisions should be amended to provide additional certainty and stronger protections for human rights:

Notice to Users

We believe it is critical that service providers be able to inform users who are the subject of a data request without undue delay where there is no explicit gag order from the issuing authority required. The provisional text does not offer any guidance or legal certainty to ensure that providers can fulfil this obligation to their users, unless there is a compelling reason to delay notice.

Recommendation: Article 4.1.4(f) should be strengthened to ensure that a requesting party may not issue a gag order on the service provider unless there is a compelling reason to do so, and where there is such a justification, jurisdictions should be subject to a requirement to time limit gag orders. Once the gag order expires, service providers should be subject to a clear mandate to inform users (without attracting criminal liability for 'tipping off') once this time limit has expired. Additionally, the explanatory text should articulate appropriate justifications for the issuance of a gag order, such as if notification would interfere with an investigation, pose a threat to national security, or threaten the safety of any person.

Third Country Notification

We also believe that the 2nd Additional Protocol should have explicit notification procedures for both a Party when an order is issued to a service provider in its territory, and for third countries, including those that are not Parties to the Convention, if a link - such as residency or citizenship - is established. Those procedures should obligate the issuing authority to notify other relevant countries of their request.

Recommendation: Article 4.1.5(a) should be amended to include a mandatory requirement that Parties notify third countries, including those who are not a Party to the Convention, if the request has a link to that jurisdiction.

Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lambe, Yvonne Cunnane
Company No. 462932

Ensuring Judicial Oversight for the Most Sensitive Data

In view of the more sensitive character of traffic data, the issuing or validation of these data requests pursuant to this 2nd Additional Protocol should require review by a judge or other independent oversight body. As basic subscriber information is less sensitive, requests for these data need not require judicial review of every such request.

Recommendation: Article 4 should be amended to require a judge or other independent oversight body to review and approve any request for transactional or traffic data before it is presented to the service provider. Article 5 should be amended to require a judge or other independent oversight body to review and approve any request for traffic data before a central authority seeking to give effect to the Party's request presents a demand to the relevant service provider.

Stronger Human Rights Protections

Whilst Facebook takes its responsibility to ensure public safety both on and off of our platform seriously, we are equally committed to protecting our users' privacy and human rights. The provisional text of the 2nd Additional Protocol places only one limit on the types of investigations under which data can be requested -- prohibiting requests that are related to investigations into political speech -- and makes no mention of service providers and Parties' obligations to protect human rights more generally. If this provisional text is not amended to include clear limits on in what circumstances requests can be made, or of specific obligations to protect users rights to privacy and free expression, the 2nd Additional Protocol could result in increased pressure pursuant to Article 4 requests, or new obligations in the case of Article 5 demands, on service providers to produce data in situations that would threaten or degrade human rights.

Recommendation: Article 4.1 should be amended to insert a new paragraph under paragraph 2 that requires that all requests adhere to international human rights norms. A new paragraph should also be added to the Draft Explanatory Report explaining that requests for data may not be issued to further investigations that would violate human rights guaranteed under the International Covenant on Civil and Political Rights (ICCPR), the Universal Declaration of Human Rights, or the Charter of Fundamental Rights of the European Union. Article 5 should also be amended to require that all requests made to central authorities to give effect to voluntary data requests made under Article 4 adhere to international human rights norms. The Article 5 protection should be further strengthened by incorporating a dual criminality requirement. This can help Parties that receive requests under Article 5 fulfill their obligation to protect human rights by ensuring that no request that they receive would violate their domestic laws and protections.

Clearly Define "Emergency" Situations

Article 3 of the 2nd Additional Protocol provides important clarity around the obligations and process that Parties must adhere to when responding to MLA requests in emergency situations. However, to ensure the efficacy of this section is not diluted in practice by improper requests, it is critical to narrowly define what instances constitute an emergency. Section 3.2.1 of the Draft Explanatory Report defines "emergency" as a situation "in which there is a significant and

Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lambe, Yvonne Cunnane
Company No. 462932

imminent risk to the life or safety of a natural person." However, the inclusion of "safety" in this definition, rather than a narrower phrase such as "serious bodily injury," opens the standard up to widely varied interpretations in different jurisdictions.

Recommendation: Section 3.2.1 of the Draft Explanatory Report should be amended to define "emergency" as a situation "in which there is a significant and imminent risk to life or serious bodily injury of a natural person."

Registered Office: Facebook Ireland Limited
4 Grand Canal Square
Grand Canal Harbour Dublin 2

Registered in Ireland as a private listed company
Directors: Gareth Lambe, Yvonne Cunnane
Company No. 462932