

GLACY+ Global Action on Cybercrime Extended

Funded
by the European Union
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe



International conference on online investigations:

Darknet and online sexual violence against children

30 September - 1 October 2019
The Hague, Netherlands

Formal assistance requests during internet investigations on Darknet and online sexual violence against children

Preparing, receiving, executing and responding to formal requests from foreign authorities for assistance to obtain electronic evidence

Rules and good practices; issues encountered



Eurojust – CoE / Glacy +

- Necessity

- To act quickly
- To research evidences
- To keep evidences
- During a small part of time

- Issues

- Evidences around the world
- Difficulty to maintain them on darknet websites
- Many countries do not response
 - Lack of legislation
 - Lac of willing
 - Lack of knowledge
 - Corruption



Eurojust – CoE / Glacy +

Official


- Border exchanges :
commissariats
transfrontaliers (EU)
- Regional level : EU / West
Africa / ASEAN
- International level : Interpol


Non-official

- Same levels
- Associations (IPA / Francopol
/ Gendarmeries ...)
- Friendship networks
- Direct access

Cybercrime : new context : PPP
More and more NGO or private organisations

Making cooperation more efficient - standardization of MLA requests


महाराष्ट्र विधानसभा

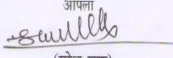

विधान सभा
महाराष्ट्र

सुरेश लाड
आमदार, कर्जत


प्रति,
प्रा. मिलिंद सोहनी
आय आय टी, मुंबई

अभिनेदन पत्र !

आय आय टी ने गेल्या दोन वर्षांपासून कर्जत, जि. रायगड तालुक्यातील सहा ग्रामपंचायतीत पिण्याच्या पाण्याचा प्रश्न सोडवणेच्या अनुसंधाने विद्यार्थी व दिशाकेंद्राचे कार्यकर्ते यांच्या सहकार्याने संशोधन प्रकल्प तयार केला त्यांचे हे कार्य कौतुकार्ह आहे .
त्यांचे मनापूर्वक अभिनेदन

आपला

(सुरेश लाड)
विधानसभा सदस्य
कर्जत

'मनोवा' आमदार निवास, जे-४५, मुंबई. क्र : २२८५४५४५
निवास : मु. पो. लहिवली, ता. कर्जत, जि. रायगड, पिन ४१० २०१ क्र : ०२१४८-२२२३२९


深圳市人民政府外事办公室


邀请确认函
Confirmation Letter of Invitation

编号/ No.: 1501-1103-0906


中华人民共和国驻巴基斯坦大使馆 (总领馆 / 领事馆 / 处) 或
中华人民共和国外交部驻 (空白) 特别行政区特派员公署:
The Embassy (Consulate General / Consulate / Office) of the P. R. China in PAKISTAN or the
Commissioner's Office of the Foreign Ministry of the P. R. China in (空白) SAR;

兹确认 深圳市雅讯达液晶显示设备有限公司 (邀请单位名称)
) 邀请的 AHMAD NAEEM NASIR (姓名) 等 3 人将于
2011.04.19 (入境时间) 来华, 停留 15 天, 从事 商务-业务洽
谈 活动, 需申请 3 个月有效 1 次入境签证。
被邀请人员名单附后。

As a duly authorized unit, hereinafter confirms that, SHENZHEN YAXUDA DISPLAY
EQUIPMENT CO., LTD. has invited AHMAD NAEEM NASIR, etc. altogether 3
persons to come to China on 2011.04.19 and stay for 15 days to hold trade talks,
and need to apply single entry (or entries) visa valid for 3 months. Name list of the
invited enclosed.


邀请单位联系人: 刘晓敏 联系电话: 27661355
Contact Person of the Company Tel.
被授权单位名称: 深圳市人民政府外事办公室
Name of Duly Authorized Unit
联系人: 陈湛鑫 联系电话: 0755-82105509
Contact Person Tel.
被授权单位盖章及负责人签署
Seal and Signature

(深圳市人民政府外事办公室印)
2011年03月28日
Year/Month/Day

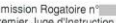
注: 1. 此确认函须与邀请单位邀请语一起使用。
2. 被邀请人员名单附另纸并加盖授权单位印章。
Notes: 1. Please present this letter together with the invitation letter of the company to apply for
visas.
2. Please attach the name list of the invited on another separate paper with seal of the duly
authorized unit.


PREFECTURE DE POLICE
DIRECTION DE LA POLICE JUDICIAIRE
Brigade de Répression de la Délinquance contre la Personne
122-126 rue du Château des Rentiers 75013 PARIS
Tél. : 01.55.75.24.55 / Fax : 01.55.75.26.04

2015/01098 PARIS (75), le 7 janvier 2016

REQUISITION JUDICIAIRE

Nous, 
Gardien de la Paix
Officier de Police Judiciaire
en fonction à la B.R.D.P.


Agissant en vertu et pour l'exécution de la Commission Rogatoire n°  délivrée le 23
novembre 2015 par Monsieur Yves MADRE, Premier Juge d'Instruction au Tribunal de Grande
Instance de PARIS, dans le cadre d'une information contre X des chefs de diffamation publique
envers un particulier, et de diffamation publique à caractère racial, suite à une plainte avec
constitution de partie civile déposée par la société COCO DESIGN DBA OPHIS, par la société
OPHIS VAPE, par Monsieur Benjamin GUEZ, et par Monsieur Rudy HALICUA.

Vu les articles 81, 151 et suivants du Code de Procédure Pénale,

Prisons et au besoin requérons :
Monsieur Alain BONNET dit SORAL
Président de l'association « Egalité et Réconciliation »
3 rue du Fort de la Brèche 93200 SAINT DENIS
et toute personne par lui désignée.

A l'effet de procéder aux actes suivants :

- Nous fournir la date de publication de l'article intitulé «La vraie arnaque de la première e-cigarette de luxe 100% cachère». URL <http://www.egaliteetrecconciliation.fr/la-vraie-arnaque-de-la-premiere-e-cigarette-de-luxe-100-cachere-29491.html>
- Nous communiquer l'identité complète du directeur de publication à la date de mise en ligne de l'article visé ci-dessus. (nom, prénom, date et lieu de naissance, filiation, nationalité, adresse personnelle).
- Nous communiquer l'identité complète de l'auteur de l'article visé ci-dessus. (nom, prénom, date et lieu de naissance, filiation, nationalité, adresse personnelle).
- Nous indiquer si un principe de modération est en vigueur sur votre site internet (concernant les commentaires) ainsi que les chiffres d'audience de l'article visé.
- Nous communiquer tous les éléments permettant l'identification des internautes utilisant les pseudonymes suivants : Leïla, goy pride, samra, curtis newton, Muhammad (le belge), Age of Oppression, Cyni, argos, ivan le terribile, Christian 4TTL, con, nicolas, paraguay avec moustache, Rollers.


OBSERVATION PREFECTURE DE POLICE
DIRECTION DE LA POLICE JUDICIAIRE

Law Enforcement



Request Access



Email

Enter your email address to receive a unique link to the Law Enforcement Online Request System. The link will give you access to the system for one hour.

Cancel

Submit

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent who is authorized to gather evidence in connection with an official investigation, you may request records from Facebook through this system.

I am an authorized law enforcement agent and this is an official request

Request Access

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the [Law Enforcement Guidelines](#).



You are here: Cybercrime > Resources

International Cooperation against Cybercrime



Cybercrime is very much transnational crime. **Urgent measures** that are needed to preserve data at the national level are also necessary within the framework of international co-operation.

Chapter III of the **Convention on Cybercrime** provides a legal framework for international cooperation with general and specific measures, including the obligation of countries to cooperate to the widest extent possible, urgent measures to preserve data and efficient mutual legal assistance.

- ▶ [Overview of the international cooperation provisions of the Convention](#)
- ▶ List of competent authorities for judicial cooperation and 24/7 points of contact
- ▶ About 24/7 points of contact

The Convention on Cybercrime is complemented by a wide range of other treaties of the Council of Europe on international cooperation in criminal matters (see Transnational Criminal Justice).



Protecting You and Your Rights in Cyberspace

CONTACT US

An opportunity for investigators

24/7 network

Necessity / Interest for a country

- A single point of contact
- Gathering domestic informations – Cleaning its own garden !
- Usefull for different missions (Interpol, CoE ...)
- Understanding intern criminality (statistics e.g;)



Article 35

- **Obligation to create a permanently available contact point**
 - a so called *24/7 network* of contact points
- **General objectives of these contact points**
 - to facilitate international co-operation
 - giving technical advisory to other contact points
 - activating the proper mechanism to expedited preservation of data
 - urgently collecting evidence
 - identifying and discovering suspects



24/7 Contact Points

- **Operational network** of experts on high-tech criminality
- Provide **help and cooperation very quickly** even if a formal cooperation request must follow this informal way
- One single point of contact for each country, **available 24 hours a day, 7 days a week**
- **Direct communications between the points**
- Mainly planned to provide the possibility to immediately preserve traffic data and other stored data worldwide



24/7 Contact Points

- Most of the contact points are police based contact points
- Some of them are Prosecution Services contact points
- Budapest Convention provided a legal basis to the 24/7 network of contact points, that are recognised as one of the most useful tools regarding international cooperation

PPP : to exchange more



Rapport
**Global
de Suivi**
de la mise en œuvre des actions
de lutte contre l'exploitation sexuelle des
enfants à des fins commerciales



The International Society for Prevention of Child Abuse and Neglect (ISPCAN)

245 W. Roosevelt Road Building 8, Suite 39
West Chicago
IL 60185
USA

<http://www.ispcan.org>



24/7 Contact Points

- Issues
 - Capacity to domestic organization
 - Language
 - Training



24/7 Contact Points

- Interest for countries
 - To live inquiries at the same or practically same speed than internet
 - To “clean their own garden”
 - To have a national overview of their inquiries and to avoid doubles
 - To get reciprocity



Resources

Interpol/ IOCP/ OIPC

- 190 members (by April 2017)
- Law enforcement agencies
- From all over the world - all the continents
- NCB/BCN
- **Objective**
 - to enhance and facilitate international police co-operation
 - to organise a global police communication system
 - to develop specific databases and police information analyses



Cybercrime

Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

Although there is no single universal definition of cybercrime, law enforcement generally makes a distinction between two main types of Internet-related crime:

- **Advanced cybercrime** (or high-tech crime) – sophisticated attacks against computer hardware and software;
- **Cyber-enabled crime** – many 'traditional' crimes have taken a new turn with the advent of the Internet, such as [crimes against children](#), [financial crimes](#) and even [terrorism](#).

Read about [online safety](#): how to protect yourself and your devices from cyberthreats.

The changing nature of cybercrime

New trends in cybercrime are emerging all the time, with estimated costs to the global economy running to billions of dollars.

In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing highly complex cybercriminal networks bring together individuals from across the globe in real time to commit crimes on an unprecedented scale.

Criminal organizations turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. The crimes themselves are not necessarily new – such as theft, fraud, illegal gambling, sale of fake medicines – but they are evolving in line with the opportunities presented online and therefore becoming more widespread and damaging.

INTERPOL's role

INTERPOL is committed to the global fight against cybercrime, as well as tackling cyber-enabled

EVENTS



4th INTERPOL-Europol
Cybercrime Conference



DOCUMENTS

Stratégie mondiale de lutte contre la
cybercriminalité - Résumé





Interpol National Central Reference Points – NCRP

- **To provide assistance to its members** on a permanent basis (24 hours a day, 7 days a week)
- **More than 1ç0 reference points all over the world** (April 2017)
 - Adopted the layout of the 24/7 contact points of Budapest Convention
 - Some Parties of the Convention appointed the same reference point to Interpol – NCRP and also to the G8 Network of Contact Points
 - G8 contact points were included into this network
- **Objective**
 - To enable police to immediately identify experts in other countries
 - Obtain immediate assistance in computer-related investigations and evidence collection



NCRP

- **To provide** and exchange police information and technical and operational support
- **To ensure** that typical police information can be exchanged as soon as possible
 - suspected terrorists, wanted persons, fingerprints, DNA profiles
 - lost or stolen travel documents, stolen motor vehicles, stolen works of art
 - Other
- **Cannot** be used to urgently request
 - of preservation of computer data
 - or preservation of traffic data
 - or any kind of measure in order to obtain or conserve evidence



GPEN

Global Prosecutors E-Crime Network

Enabling an international, knowledge led,
↳ co-ordinated approach to prosecuting
cybercrime

Europol

- **European Union Agency**



- Role

- To improve the effectiveness of co-operation between law enforcement authorities from each European Union Member State
- Operational since 1999
 - facilitating the analysis of criminal information
 - sharing of data between Member States
- European Cybercrime Centre, EC3 (opened January 2013)

Eurojust



- **Cooperation in the fight against crime**
- **Objective of coordinating** the activities carried out by the national authorities responsible for prosecution

Eurojust has competence for:

- Promoting coordination between the competent authorities of the various Member States
- Facilitating the implementation of international mutual legal assistance and of extradition requests

Cyber Crime and Prosecution Setup

- Prosecutors as criminal justice officials who, irrespective of different legal systems and traditions, are primarily responsible for presenting and supporting evidence of the state in criminal proceedings;
- In many jurisdictions, this authority is also coupled with oversight role for the conduct of investigations;
- Quite often Prosecutor/Attorney General's offices are designated central authorities dealing with mutual legal assistance requests in criminal cases at the stage of pre-trial investigations;

Enumeration of competences for the 24/7 point of contact

- Article 35
- Desirable combination is designated to deliver:
 - immediate assistance:
 - for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or
 - for the collection of evidence in electronic form of a criminal offence.

Enumeration of competences for the 24/7 point of contact

- Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
 - the provision of technical advice;
 - the preservation of data pursuant to Articles 29 and 30;
 - the collection of evidence, the provision of legal information, and locating of suspects.

Capacities

- Following should be accepted as representing capacities to deal with, but not limited to:
 - technical aspects of a computer crime or the particularities given by the use of a computer system in a crime (modus operandi, characteristics of electronic evidence such as volatility, ease tamper or harm, location of the evidence, how to be found, the shape that confer admissibility under the law etc.);
 - legal aspects and proceedings in criminal matters;
 - legal aspects related to transfer of such evidence under mutual legal assistance;

Capacities

- different levels of understanding of foreign languages (reading, writing), though English is the most used language for correspondence;
- bad translations;
- different means of communication;
- different ways of describing summary of facts (sometime too lapidary to fully understand what is needed and why is needed, what crime had been committed);
- different understanding of legal or technical terms; and
- immediate action.



24/7 network as a channel of communication

- **NOT** meant to bypass the consecrated ways of communication with respect to mutual legal assistance;
- **INTENDED** to complement the efforts in rendering at a widest extent and in an expedited manner mutual legal assistance in criminal matters, particularly in cybercrime and with respect to electronic evidence;
- **STRONG UNDERSTANDING** of the legal issues of the international cooperation in criminal matters is highly desirable;



So necessary legal framework





Article 29

- **Expedited preservation of data stored in a computer system**
- Parallel framework to the internal provision
 - allows one contracting Party to require from other Party the expedited preservation of data
 - if at the same time expresses its intention of sending a formal request of assistance for a search, or a seizure, or any similar measure
- **The requested party must act as necessary**, with all the due diligence, to preserve the requested data, according to its own national law
- **Dual criminality cannot be required by the requested party**, as a condition of preservation of the data



Article 29

- **A new tool of international cooperation**
- **Specificity of the digital environment** - the necessity to preserve something that, in very short moments, can be completely deleted
- **Only a preservation measure**, for urgent reasons and does not imply automatically disclosure of the preserved data
 - in the cases where disclosure is permitted, there are very narrow rules to do that, above all if the data are not merely traffic data
- **In practical cases, it can be done an expedited preservation** of data and then, latter on, it can be assumed that there are no conditions to pursue to the disclosure of those data to the requesting party



Remembers

- Priorities of competent authorities while considering and proceeding request:
 - **speedy acquisition** of information to progress an aspect of an investigation;
 - **obtaining of evidence for trial;**
 - **initiation of an investigation** in another state and **coordinated parallel investigations;**
 - **establishment of a JIT;**



Remembers

- Competent authorities should consider:
 - combination of information channels and legal frameworks that are available based on the offence under investigation;
 - necessity of taking the path of international cooperation, e.g. whether the type of assistance required is available without resort to formal international cooperation;
 - **if previous positive**, then can or will information in question be provided in a form admissible at trial;



Remembers

- **If party to the Cybercrime Convention:**
 - Art. 32 trans-border access to stored computer data: whereby **publicly available** data can be accessed regardless of where it is located geographically, or whether other stored computer data **can be accessed by consent**;
 - possibilities offered by Article 32 in respect of subscriber information are likely to be much faster than other channels;
- **No specific procedures** relating to the obtaining of subscriber information in the UNTOC or other regional conventions;



Article 26

Spontaneous Information

- The authorities from a Party, within an internal investigation, discover that some of the information they obtained must be forwarded to the authorities of other Party
- It can be done if the information seems to be useful or necessary to the beginning or the developing of an investigation respecting to a criminal offence in the framework of the Convention
- According to Article 26, 2, this dispatch of information can be submitted to certain conditions, mainly of confidentiality



Article 26

Spontaneous Information

1 - A Party may, within the limits of its domestic law and without prior request, **forward to another Party information obtained within the framework of its own investigations** when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 - Prior to providing such information, **the providing Party may request that it be kept confidential or only used subject to conditions.** If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.



Art. 26 in motion

- Priorities may include the initiation of an investigation in another state or of a parallel investigation there;
- Allows information obtained by one state in the course of its own investigations to be passed to another state;
- Passing may generate the transmission of mutual assistance requests between the states concerned and networks or organizations such as Eurojust;



JIT

- Joint Investigation Team;
- One investigation, contracts and funding;
- The CoE Convention, EU MAC and UNTOC all provide a legal framework for the establishment of JITs (2nd Additional Protocol, Article 20., EU MAC, Article 13., UNTOC, Article 19.)
- Most significant experience concerning the establishment of JITs exists within the EU and the JITs Network and/or Eurojust)



Procedural placing of MLA request

- Once requests for preservation have been made and if successful competent authorities will be in a position to make a mutual assistance request for obtaining the material.
- Article 18 – production order and Article 19 – search and seizure of stored computer data, can support the execution of mutual assistance requests for stored data made pursuant to Article 31;
- Coercive measures will then be used in the requested state to obtain the computer data pursuant to the request;
- Dual criminality tests applies;



Article 18 - Production order

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities **to order:**
 - a) **a person** in its territory **to submit specified computer data in that person's possession or control**, which is stored in a computer system or a computer-data storage medium; and
 - b) **a service provider offering its services in the territory of the Party to submit subscriber information** relating to such services in that service provider's possession or control.



Article 18 - Production order – Subscriber data

- 3 For the **purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form** that is held by a service provider, relating to subscribers of its services **other than traffic or content data** and by which can be established:
- a) the **type of communication service used**, the technical provisions taken thereto and the period of service;
 - b) **the subscriber’s identity**, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
 - c) **any other information on the site of the installation of communication equipment**, available on the basis of the service agreement or arrangement.



Article 19

Search and Seizure of Stored Computer Data

- 3 Each Party shall adopt such legislative and other measures as may be necessary to **empower its competent authorities to seize or similarly secure computer data** accessed according to paragraphs 1 or 2. These measures shall include the power to:
- a) **seize or similarly secure** a computer system or part of it or a computer-data storage medium;
 - b) **make and retain a copy** of those computer data;
 - c) **maintain the integrity of the relevant** stored computer data;
 - d) **render inaccessible or remove** those computer data in the accessed computer system.



Preparing MLA request

- Competent authorities should bear in mind:
 - **any domestic provisions** relating to the admissibility of evidence at trial;
 - **good practice to consult in advance** where there are any doubts;
 - **sufficient information should be included** in the request to satisfy any requirements;
 - **consultation on these procedures** should yield the information needed to be included in the request;



Preparing MLA request

- Consider the confidentiality of the assistance requested;
- Translation is required?
- Reliable translation services should be used (inadequate translation is a major cause of delay in the execution of mutual assistance requests);
- Transmission and channels used;



Requesting states

- **Competent or central authorities should keep in touch with counterparts (use the CoE 24/7 Network as appropriate);**
- **If the receipt of the request is not acknowledged by the requested state, it should be followed up;**
- **If unsure, clarification should be obtained regarding the transmission arrangements for the evidence once obtained;**
- **Any difficulties relating to the admissibility or presentation of the evidence at trial should be noted as a lesson learned;**



Requested states

- **An acknowledgement of receipt should be sent;**
- **If the translation is of poor quality, the requesting state should be informed immediately;**
- **If the request reveals substantive or procedural flaws, the requesting state should be informed immediately** with a view to consultation on resolution of the issue where possible.
- **Competent authorities should always consider will actions compromise the confidentiality of the request** - if so, requesting state should be informed with a view to dialogue on how to resolve the issue.



Requested states

- **If certain procedures are difficult to follow**, the requesting state should be informed with a view to resolving the issue;
- **Where a request is passed by a central authority to an executing authority**, it should be followed up noting any requirements for urgency or expeditious execution;
- **Any issues arising to be noted** for the future or as a lesson learned;



Article 29

Expedited Preservation of Stored Computer Data

- 1 - A Party may request another Party to **order or otherwise obtain the expeditious preservation of data stored by means of a computer system**, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.



Article 30

Expedited Disclosure of Preserved Traffic Data


- 1 . Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.



Article 30

Expedited Disclosure of Preserved Traffic Data

- 2. Disclosure of traffic data under paragraph 1 may only be withheld if:
 - a.) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
 - b.) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests



Article 31 - Mutual Assistance Regarding Accessing of Stored Computer Data

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29
2. (...)
3. The request shall be responded to on an expedited basis where:
 - (a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
 - (b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.



Article 32 – Transborder Access to Stored Computer Data with Consent or Where Publicly Available

A Party may, without the authorisation of another Party:

- a) - access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b) - access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Law Enforcement Online Requests



Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent who is authorized to gather evidence in connection with an official investigation, you may request records from Facebook through this system.

I am an authorized law enforcement agent and this is an official request

Request Access

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the [Law Enforcement Guidelines](#).

Online resources

- Council of Europe Action Against Cybercrime:
<https://www.coe.int/en/web/cybercrime/home>
- Convention on Cybercrime (ETS. 185):
<https://www.coe.int/en/web/cybercrime/the-budapest-convention>



Online resources

- Council of Europe “Budapest Convention” Comettee:
<https://www.coe.int/en/web/cybercrime/tcy>
- CoE Worldwide capacity building:
<https://www.coe.int/en/web/cybercrime/capacity-building-programmes>



Online resources

- Resources:

<https://www.coe.int/en/web/cybercrime/resources>

- Reports:

<http://www.coe.int/en/web/cybercrime/all-reports>

- Prevention:

<http://www.coe.int/en/web/cybercrime/preventing-cybercrime>





Online resources

- Training on Cybercrime – Cybercrime Octopus Community:
<http://www.coe.int/en/web/octopus/home>
- Country Legislation:
<https://www.coe.int/en/web/cybercrime/country-profiles>
- Contact Points
- Protecting children:
<https://www.coe.int/en/web/cybercrime/protecting-children>

Online resources

- International Cooperation:

<https://www.coe.int/en/web/cybercrime/international-cooperation>

- LEA/ISP Cooperation:

<https://www.coe.int/en/web/cybercrime/lea/-/isp-cooperation>

- **CoE Data Preservation Request – Art. 29 standard form**



