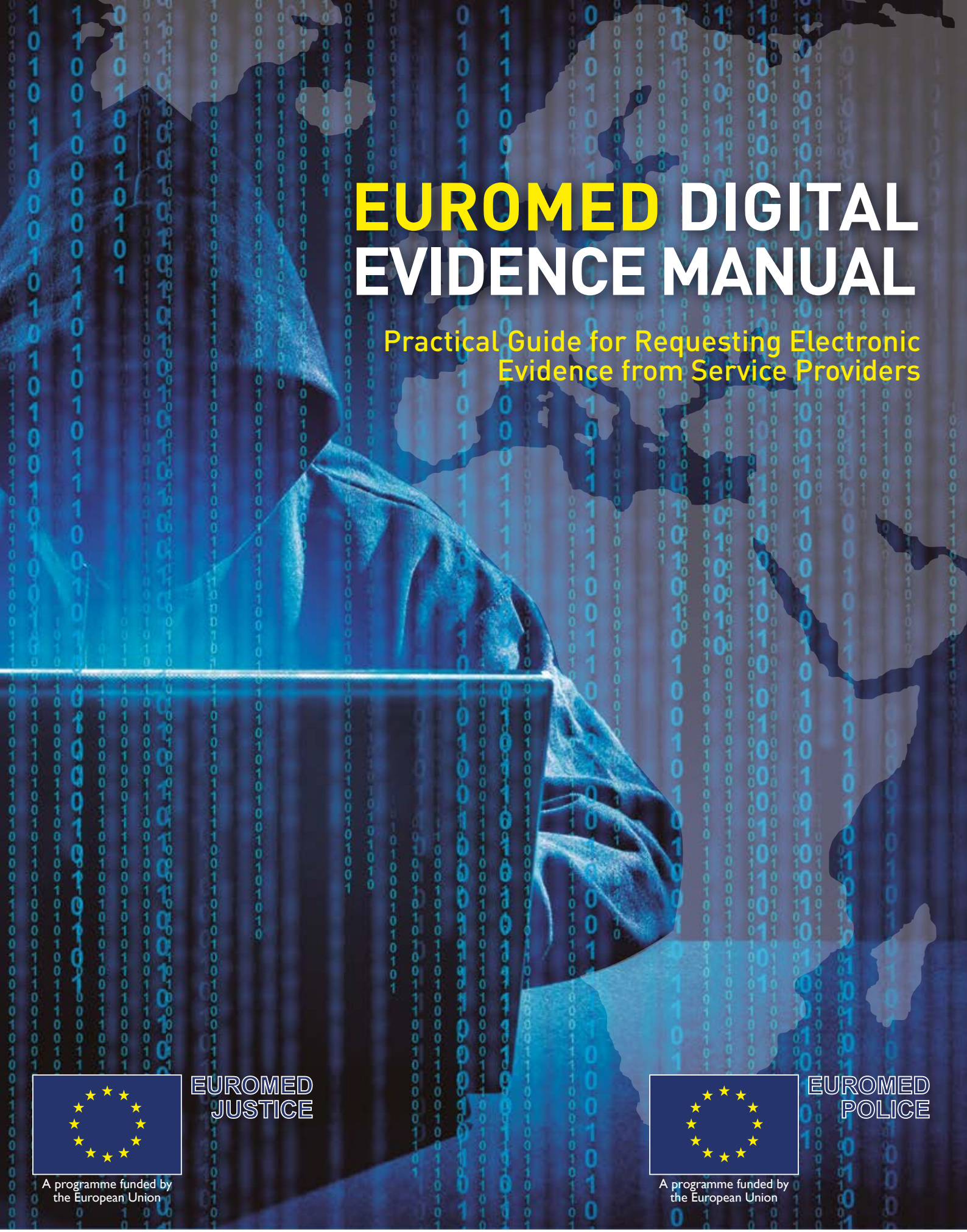


EUROMED DIGITAL EVIDENCE MANUAL

Practical Guide for Requesting Electronic Evidence from Service Providers

EUROMED JUSTICE

A programme funded by the European Union

EUROMED POLICE

A programme funded by the European Union

FIIAPP COOPERACIÓN ESPAÑOLA

Implemented by a consortium led by CIVIPOL CONSEIL

With the support of:

UNODC

UNITED NATIONS SECURITY COUNCIL COUNTER-TERRORISM COMMITTEE EXECUTIVE DIRECTORATE (CTED)

IAP International Association of Prosecutors

AUTHORS:
The EuroMed Manual on Digital Evidence has been written by *Mr. Daniel Benjamin Suter*, Director of iJust International Justice Consultants (UK) Former UK Liaison Prosecutor to US, in collaboration with: *Mr. Jorge Carrera*, Spanish Liaison Magistrate to US, Justice Counsellor, Former Court of Appeal Judge (Spain), *Ms. Marie-Laurence Navarri*, French Liaison Magistrate to US, *Mr. Marc L. Varri* retired Federal Bureau of Investigation Senior Manager (US), and *Ms. Lina Cepeda* Expert

EDITORS AND COORDINATORS:
The Manual benefited from the contributions, comments and feedback of:

Mr. Virgil Ivan-Cucu, EuroMed Justice Key Expert, EIPA Senior Lecturer
Mr. Carlos Garcia, EuroMed Police Capacity building and Training Coordinator

LINGUISTIC VERSIONS
Original: EN Manuscript completed in September 2018.

Acknowledgment

The design of the *Digital Evidence Manual* began in November 2016 February 2017 when *EuroMed Justice and Police* initiated the complex process of expert consultation and content drafting.

Due to the constant and active presence in the MENA region and high-level of expertise in the development of several tools in the fields of countering terrorism and organised crime, *Counter Terrorism Committee Executive Directorate (CTED)* steadily supported EuroMed initiative.

The entire process benefited from the assistance and contribution of relevant EU agencies, *Eurojust, Europol, European Judicial Network in criminal matters, Eurojust Task Force on Cybercrime, the European Judicial Cybercrime Network*, international organizations and networks such as, *UNODC, Interpol and International Association of Prosecutors*, which provided insights and expertise that greatly assisted the research.

Special thanks are dedicated to DG NEAR who assured a closer collaboration with other EU financed projects, Cyber-South, CT MENA and Interpol South.

The Manual would not have been possible without the dedication and the hard work done by the members of the EuroMed Justice CrimEx group and the EuroMed Police team of experts.

For the production of this manual EuroMed counted on the essential help of the Internet service providers to better address the judicial and law enforcement requests, with particular support from Google, Facebook, Twitter, WhatsApp, Microsoft, JustPaste.it, Apple, among others.

Executive summary

Introduction

In an evolving and volatile cybercrime environment, investigating authorities are unable to use domestic investigative tools to secure and obtain electronic evidence quickly and effectively. Law enforcement and judicial authorities experience difficulties to access such data, frequently categorised as account subscriber information, traffic information or metadata, and content data.[1]

The Joint EuroMed Justice and Police Manual on Digital Evidence constitutes an important tool for successful cross-border investigations and prosecutions, and creates the conditions to identify and overcome the difficulties and obstacles of legal or practical nature and to ease the cooperation in gathering e-evidence.

The purpose of the EuroMed Manual is to focus on the practical measures that could help judges, prosecutors and law enforcement officers to mitigate the malicious use by the terrorists and organised criminal groups of Internet, by creating a common guideline for the Law Enforcement Agencies and Judicial Authorities to address the requests for cross-border digital evidence.

Within EU, agencies such as Europol, which is a EuroMed Police partner, have taken actions to advance in the field of counter radicalisation with the creation of the Internet Referral Unit, which detects and requests the elimination from Internet all the contents that could be considered as a potential vector of radicalisation.

In 2016 Eurojust, which is a EuroMed Justice stakeholder, established the European Judicial Cybercrime Network to facilitate and enhance cooperation between the competent judicial authorities dealing with cybercrime and to foster the dialogue among the different actors and stakeholders that have a role in ensuring the rule of law in cyberspace.

The EuroMed Conference on Digital Evidence (Lisbon, 23-25 April 2018) represented a major step forward in the development of the Digital Evidence Manual. The Conference converged the EuroMed Justice CrimEx and the EuroMed Police expert group with the relevant international and regional stakeholders (70 participants), creating a unique opportunity to assure the synergies, to share the experience and to exchange the best practices between the existing initiatives and the international and regional agencies regarding the access to digital evidence from a legal, procedural, and technical points of view.

These evolutions prove that a process of judicial and law enforcement cooperation for the gathering of cross-border electronic evidences and collaboration with the different service providers has to a certain extent, advanced.

1. Definitions of these data categories can be found in the Council of Europe Budapest Convention (CETS No 185), in the proposal for a Regulation on Privacy and Electronic Communications, COM(2017) 10 final) and the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters. COM(2018) 225 final.

However, different service providers have different interpretations on the contents of a request (e.g. basic subscriber information) that can be delivered upon a court order or subpoena. Furthermore, the type of request that courts have to send to these providers differ from one company to another, even when the targeted data are sometimes quite similar; additionally, a given company may require different conditions to be fulfilled depending on the requesting country.

Given the current situation, EuroMed Justice and Police Project Teams considered appropriate to go further in the standardisation of the requesting procedures, and notably with regard to the procedures that require a judicial and police intervention.

Finally, procedures that require Mutual Legal Assistance or a Letter rogatory entail the involvement of the judicial system of the country that hosts the service provider. In a high percentage of the cases this falls under the responsibility of the United States of America thus, it was appropriate to indicate, within the Manual, the support the FBI and the US Department of Justice can play in order to address correctly these documents. It was considered opportune, to work on the standardisation of those documents, so they could be better addressed and structured, avoiding the requests that will not meet the USA judicial system requirements.

Euromed tools for gathering electronic evidences

Digital Evidence Manual provides for the following tools:

1. **Mapping** of the Service Providers relevant for the EuroMed region[2] includes the following information:

   - SPs contacts and their focal points for cooperation with judicial and law enforcement
   - SPs rules for cooperation with law enforcement and Justice.
   - The cases in which the Service providers authorise direct requests from foreign law enforcement services.

2. **Judicial request guidelines**

   In order to produce the guidelines manual to request internet-related data and content within the framework of counter-terrorism and accessory crimes investigations, prosecution and trials EuroMed Police and Justice described the **types of requests** (Judicial and non-Judicial), **the content** and the **procedure** for each one of the requests, in order to be correctly processed by the US Justice.

3. **Standardization of procedures**

   A **Simplified Uniform Request** (**SUR**) is proposed for urgent requests, preservations requests and direct requests (when they are possible) together with some other templates to be used in the cases where the Service Provider does not have a dedicated template.

2. People's Democratic Republic of Algeria, the Arab Republic of Egypt, Israel, the Kingdom of Jordan, Lebanon, Libya, the Syrian Arab Republic, the Kingdom of Morocco, Palestine and the Republic of Tunisia

4. Practical approach to the EU law and policies

Several EU documents[3] stressed the importance of e-evidence in criminal proceedings for all types of crimes and in particular the need "*to find ways to secure and obtain e-evidence more quickly and effectively by intensifying cooperation with third countries and with service providers that are active on European territory... and direct contacts with law enforcement authorities and to identify concrete measures to address this complex matter*"[4].

Proposals for a legal framework authorising competent national authorities to directly request or compel a service provider in another Member State to disclose e-evidence processed in the EU on the basis of certain conditions and safeguards have been presented by the Commission to the Council in the first quarter of 2018[5].

4.I. EU model for cross-border gathering of electronic evidences

On 17 April 2018 the European Commission presented two legislative proposals to enhance cross-border gathering of electronic evidence: Proposal for a Regulation[6] on European Production and Preservation Orders for electronic evidence in criminal matters and a Proposal for a Directive[7] on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

The Regulation envisages the creation on an **European Preservation Order** allowing a judicial authority to request to a Service Provider (SP) or its legal representative in another EU Member State (EU MS) to preserve specific data in view of a subsequent request to produce this data via **mutual legal assistance, a European Investigation Order or a European Production Order**. The second instrument created is the **European Production Order** allowing a judicial authority to obtain electronic evidence (such as emails, text or messages in apps, information to identify a perpetrator) directly from a SP or its legal representative in another EU MS, which will be obliged to respond within 10 days, and within 6 hours in cases of emergency (compared to up to 120 days for the existing European Investigation Order or an average of 10 months for a Mutual Legal Assistance procedure). Based on the right to protection of personal data the SPs and persons whose data is being sought will benefit from various safeguards and be entitled to legal remedies;

The proposal for the Directive on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, provides for the SPs the obligation to design a legal representative in the EU: for the receipt of, compliance with and enforcement of decisions and orders, even if their headquarters are in a third country

3. Commission Communication on a European Agenda on Security, COM(2015) 185 final; Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST 9579/16; COM(2016) 710 final; Common challenges in combating cybercrime as identified by Eurojust (EJ) and Europol (EP) http://data.consilium.europa.eu/doc/document/ST-7021-2017-INIT/en/pdf : all documents and more information are available at https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en
4. Council conclusions of 9 June 2016 on improving criminal justice in cyberspace 10007/16.
5. Council Note - Improving cross-border access to e-evidence - Brussels, 26 February 2018 (OR. en) 6339/18
6. https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF
7. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0226&from=EN

4.2. EU model for data protection

GDPR - General Data Protection Regulation (EU) 2016/679[8], in force from 25 May 2018 lays down general rules to protect natural persons in relation to the processing of personal data. GDPR recital (19) stipulates that this Regulation **should not apply** to processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, which are the subject of a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council.

DPDC - Directive (EU) 2016/680[9] in force on 6 May 2018, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/J

Sustainability

One of the aspects to take into consideration is the sustainability of the procedure described in the Manual, therefore, the contact points mapped and the procedures at judicial level have to be updated regularly.

To achieve that goal, the **EuroMed Police and Justice Project Teams will liaise with their supporting partners Europol, Eurojust and EJN among others**, in order to arrange with these agencies, the **necessary mechanisms** to upload and maintain up-to-date the aforementioned contents.

The technical infrastructure for EuroMed Police exists already and is fully operational, which is the **EuroMed Police Threat Forum,** hosted within the Europol Platform for Experts

8. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
9. https://publications.europa.eu/en/publication-detail/-/publication/182703d1-11bd-11e6-ba9a-01aa75ed71a1/language-en

Contents

INTRODUCTION 13
Context 13
Southern partner countries - Cyberthreats 13
International dimensions of cybercrime 14
Electronic evidence 15
Guide Outline 16
Annexes 17
Other guides and tools produced by international organizations 17
Methodology 18

PART 1. EMERGENCY DICLOSURE REQUESTS 19
Introduction 20
The U.S. legal standard on emergency disclosures 20
What happens with requests from abroad? 21
Standard information to be provided for an emergency request 22
Type of Data provided 22
Checklist for emergency requests to U.S. service providers 23
Southern partner countries 24

PART 2. PRESERVATION 26
Introduction 27
STEP ONE - Locating where the sp has custody and control of the electronic evidence 27
STEP TWO – Is the electronic evidence available 27
STEP THREE – Making the preservation request 28
STEP FOUR - ExtenDING 30
Data retention 31

PART 3. REQUESTING ELECTRONIC EVIDENCE WITHOUT MUTUAL LEGAL ASSISTANCE 32
Introduction 33
Context 33
Open source searches 34
Useful Links *34*
Voluntary disclosure 34
Consent *35*
Direct requests *35*
User notification *36*
Police-to-police cooperation 36
General data protection regulation 39

PART 4. SERVICE PROVIDER MAPPING 40
Adobe 41
AirBNB 42
Amazon 44

Apple 45
AskFM 49
Atlassian 52
Baaz 54
Box 55
Dropbox 56
Ebay 57
Facebook 59
Google 62
JustPaste.it 66
Kik 67
Linkedin 68
Microsoft 70
Pinterest 73
Signal 75
Skype 76
Snapchat 78
Surespot 80
Tumblr 81
Twitter 83
Uber 86
WhatsApp 88
Wikr 90
Yahoo 92
Zello 95

PART 5. MUTUAL LEGAL ASSISTANCE 97
Introduction 98
Drafting an MLAR for electronic evidence 99
- Language 99
- Urgency 99
- Legal basis 100
- Purpose of the request 102
- The relevant law 102
- Summary of facts 102
- Basic subscriber information – U.S. MLAR 103
  - *Legal standard 103*
- Traffic data – U.S. MLAR 104
  - *Legal Standard 104*
- Content – U.S. MLAR 104
  - *Legal Standard 104*
  - *Do the facts meet Probable Cause? 105*
  - *Freedom of Expression 107*
- Real-time collection of Traffic Data – U.S. MLAR 108
  - *Legal Standard 108*
- The Date Range 109

Assistance requested 109
Type of BSI available *110*
Types of traffic data available *111*
Types of content available *111*
Real-Time Collection of Traffic Data *112*
Use of evidence obtained 113
Preferred form of evidence 114
Confidentiality 114
Transmission of electronic evidence 115
ReciprocAL procedural laws of a Requesting and Requested States 116
Contacts 116
Translation 116
The cloud act 128
Proposed European Rules 128

GLOSSARY 130

ANNEXES 139
ANNEX A: Links to Service Provider Law Enforcement Guidelines 140
ANNEX Bi: Model MLAR for Stored Electronic Evidence 142
ANNEX Bii: Model MLAR for real-time collection of traffic data or content 157
ANNEX C: MLAR checklist 162
ANNEX D: Legal Instruments 169
ANNEX E: Model direct request form for voluntary disclosure 171
ANNEX Ei: APPLE Government / Law Enforcement Information Request 173
ANNEX F: Simplified uniform request for preservation and emergency: disclosure requests 175
ANNEX Fi: GOOGLE emergency disclosure request form 178
ANNEX Fii: APPLE Emergency Government / Law Enforcement Information request 180
ANNEX G: Law and procedure in SPCs 182
ANNEX H: Law and Procedure in Selected States with SPs 196
ANNEX I: European Union cooperation with third countries 201

Abbreviations

AU	African Union
AUC	African Union Convention on Cyber Security and Personal Data Protection
BC	Budapest Convention on Cybercrime of the Council of Europe
BSI	Basic Subscriber Information
CA	Central Authority
CITO	Arab League Convention on Combating Information Technology Offences
CoE	Council of Europe
DPDC	Data Protection Directive in Criminal Matters, EU 2016/680
EDR	Emergency Disclosure Request
ECPA	Electronic Communications Privacy Act
EU	European Union
EUMS	European Union Member State
GDPR	General Data Protection Regulation, EU 2016/679
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
MAC	Media Access Control
MLA	Mutual Legal Assistance
MLAR	Mutual Legal Assistance Request
MLAT	Mutual Legal Assistance Treaty
OIA	Office of International Affairs – Central Authority for the U.S.
SP	Service Provider
SPC	Southern Partner Country
SPOC	Single Point of Contact
SUR	Simplified Uniform Request
UNSCR	United Nations Security Council Resolution
UNTOC	United Nations Convention Against Transnational Organized Crime
TOS	Terms of Service
URL	Uniform Resource Locator
U.S.	United States of America

The Guide includes the following

	**PRACTICAL NOTES** To assist with application of relevant processes
	**IMPORTANT NOTES** To highlight priority issues
	**CASE STUDIES** Applying best practice to common challenges
	**Useful links and online resources**
	**MODEL FORMS** To assist preservation and requests for electronic evidence

Introduction

Context

1.1. Use of the internet is growing exponentially, with more than 3.8 billion internet users worldwide, which accounts for almost 47 percent of the global population. It is estimated an individual will spend five years of their life on social media.[10] It is estimated that the cost of cybercrime could be $2.1 trillion USD globally by 2019.[11] Upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized crime with online black markets, computer infection and harvesting of personal and financial data. Terrorists use social media to spread propaganda, raise funds, recruit, plan attacks and to share information. This electronic evidence can be important information to show where a suspect is located, who they are associating with and what they are communicating.

Southern partner countries - Cyberthreats

1.2. A cybercrime threat report for the MENA region in 2014 identified that most cyber- attacks that target Information Communication Technology (ICT) infrastructure were Distributed Denial of Service or website defacement.[12] The report further highlights the vulnerability to cyberattacks due to the lack of regulation and proper legal frameworks.[13]

1.3. The challenges raise in significance with the knowledge that 55% of households surveyed in the Arab Social Media Report have 2-5 internet enabled devices (other than computers and laptops) and another 25% have 6-10 internet connected devices.[14]

1.4. The Arab States had 161 million internet users in 2016[15] and since the Arab Spring use of social media platforms has significantly increased. Facebook has 156 million users which is an increase of over 40 million from last year.[16] Egypt gained more than 14 millions Facebook users, Algeria 9.3 million and Morocco 5.5 million.[17] The use of Twitter is significant, with Egypt producing 152 million tweets per month and Algeria 71 million.[18] This greater use of social media enables[19] identity theft,

10. How Much Time Will the Average Person Spend on Social Media in their Life – Adweek 22 March 2017 - http://www.adweek.com/digital/mediakix-time-spent-social-media-infographic/
11. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion
12. Mohamed N. El-Guindy (2014) Middle East Security Threat Report
13. Ibid.
14. Arab Social Media Report 2017 www.arabsocialmediareport.com
15. http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
16. Ibid p 33
17. Ibid p 37
18. Ibid p 48
19. https://www.internetmatters.org/issues/

cyberbullying, sexting and radicalisation[20] Significantly social media has also created a conduit for terrorist fundraising, recruitment, propaganda and use of open source information[21] for attacks.

International dimensions of cybercrime

1.5. To effectively investigate and prosecute cybercrime, close cooperation is required between States. The present system of Mutual Legal Assistance (MLA) can be complex and bureaucratic in some States, resulting in length delays to request evidence. This does not resonate with the quick paced nature of cybercrime, where the internet has no borders. In addition, jurisdictional issues[22] have been created through cloud computing, requiring careful consideration where a Mutual Legal Assistance Request (MLAR) is transmitted. Setting up procedures for quick responses to emergency incidents, preservation of evidence and MLA, are vital[23]

1.6. This is brought into focus when considering the results of a recent EU survey[24] that confirmed:

- More than half of investigations include a request for cross-border access to electronic evidence
- Electronic evidence in any form is relevant in around 85% of total (criminal) investigations
- In almost two thirds (65%) of the investigations where electronic evidence is relevant, a request to SPs based in another jurisdiction is needed

1.7. Electronic evidence, therefore, can is an essential component for investigations and prosecutions and this Guide will assist with when and how to request electronic evidence from Service Providers (SPs). This will include:

- Summarising major SP procedures for preserving electronic evidence to ensure this is immediately requested
- Making Direct Requests to SPs or using police-to-police cooperation for disclosure of electronic evidence (without the need of transmitting an MLAR) to reduce delays
- Drafting a compliant MLAR to ensure faster production of electronic evidence, with guidance on the higher legal standard of probable cause in the United States (where most major SPs are located)
- Law enforcement emergency disclosure requests to SPs to avert risk of death and serious physical injury

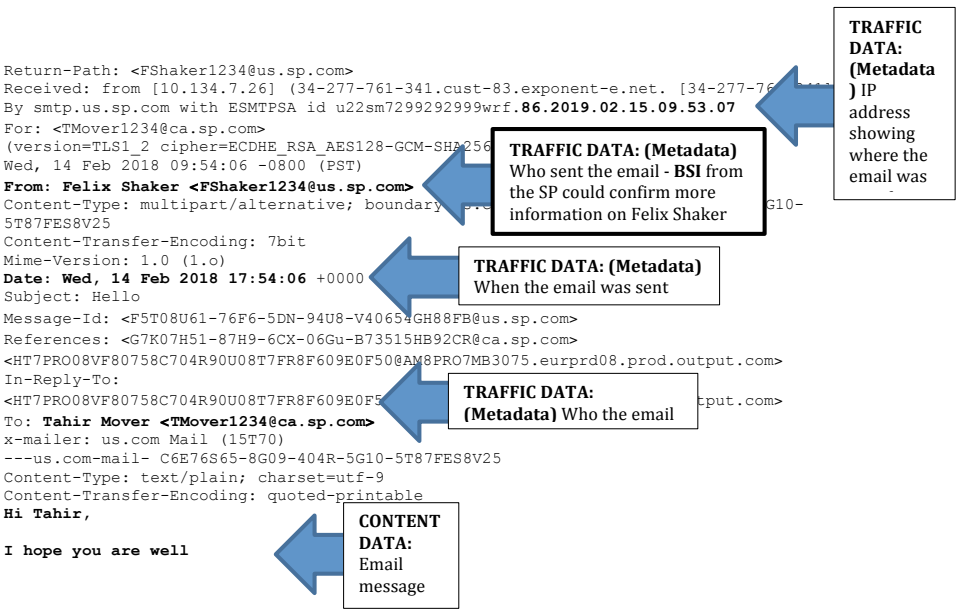
20. http://www.independent.co.uk/news/world/middle-east/what-makes-people-join-isis-expert-says-foreign-fighters-are-almost-never-recruited-at-mosque-a6748251.html
21. http://www.bbc.co.uk/news/world-middle-east-18532839
22. See: Strategic Seminar "Keys to Cyberspace" Eurojust, The Hague, 2 June 2016 Outcome Report
23. Understanding Cybercrime: Phenomena, Challenge and legal Responses (ITU) page 3
24. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN page 14

Electronic evidence

1.8. The table below summarizes the two basic categories of electronic evidence that are routinely requested:

Stored electronic evidence	
Basic Subscriber Information (BSI)	The name of the subscriber/user and may include how long the subscriber has used that specific service and the Internet Protocol (IP) address of the first login
Traffic Data (Non-Content Data)	Metadata, which relates to the provision of services and includes data relative to the connection, traffic or location of the communication (for example IP or MAC addresses) Access logs, which record the time and date an individual has accessed a service, and the IP address from which the service was accessed; Transaction logs, which identify products or services an individual has obtained from a provider or a third party (e.g. purchase of cloud storage space)[25]
Content Data	The body or text of an email, message, blog or post, videos, images, sound stored in a digital format (other than subscriber or metadata)
Real-time collection of electronic evidence	
Traffic Data	Interception of who a subject is contacting and where from – for example static and dynamic IP addresses
Content Data	Interception of the body or text of an email, message, blog or post, videos, images, sound stored in a digital format (other than subscriber or metadata)

The raw message format of an email below shows stored electronic evidence



25. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN page 43

Example of real-time collection of electronic evidence

CASE STUDY

Through intelligence it was known that email accounts from a U.S. service provider were used for communications between a terrorist network. The users of these email accounts were unknown and the police needed the traffic data to locate where the emails were sent from and then identify the users. An MLAR was sent for real-time collection of static IP addresses to the U.S. to confirm where the emails were being sent from. The IP addresses resolved to cyber cafes and the police in the Requesting State commenced covert observations on these locations. After receiving the live transmission of the real time collection of the IP addresses the police identified those sending the emails and made arrests.

Guide Outline

1.9. The Guide will assist with the following:

- **PART 1 Emergency Disclosure Requests (EDR):** Requesting **BSI** or **Traffic Data** to avert an imminent threat to life or serious physical harm to an individual/s
- **PART 2 Preservation**: A request from a foreign law enforcement officer, prosecutor or judicial authority to preserve electronic evidence before it is deleted or otherwise disposed of or destroyed
- **PART 3 Voluntary Disclosure by SPs**: Either through a non-MLA direct request to a SP for **BSI** or **Traffic Data** rather than compelling disclosure through Mutual Legal Assistance (MLA) of by consent of the user
- **PART 4 SP Mapping**: Summary of SP procedures, with links to law enforcement guidelines, contact points for EDRs, preservation and voluntary disclosure
- **PART 5 Mutual Legal Assistance**: Formally requesting **BSI**, **Traffic Data** (if not obtained through a Direct Request) or **Content Data** through MLA by sending a Mutual Legal Assistance Request (MLAR) to the State where the data is stored and compelling disclosure

Annexes

1.10.  The Annexes to the Guide provide the following additional information and model forms:

- **Annex A:** SP Law Enforcement Guideline links to assist the investigator and prosecutor on the latest policies and contacts for preservation, direct requests and emergency requests – also see http://www.search.org/resources/isp-list/ for a database of SP law enforcement guidelines
- **Annex Bi:** A Model MLAR to request stored electronic evidence
- **Annex Bii:** A Model MLAR to request real-time collection of electronic evidence
- **Annex C:** An MLAR checklist to confirm the step-by-step procedures to draft an MLAR for electronic evidence
- **Annex D:** International Legal Instruments
- **Annex E:** Model Voluntary Disclosure Request Form
- **Annex F:** Simplified Uniform Request for Preservation or Emergency Requests
- **Annex G:** Relevant law and procedure in SPCs for requests for electronic evidence
- **Annex H**: Relevant law and procedure in selected States with SPs
- **Annex I:** EU Member States and Agencies cooperation with 3rd countries

Other guides and tools produced by international organizations

1.11.  This Guide will compliment UNODC, CoE, INTERPOL and Europol Guides and tools regarding cross-border access to electronic evidence as follows:

- Basic Tips For Investigators And Prosecutors For Requesting Electronic Evidence From Foreign Jurisdictions, UNODC, 2014 (available in English, French and Russian)
- Mutual Legal Assistance Request Writer Tool (with a separate Module on Requesting Electronic Evidence), UNODC, 2017
- Guidelines for the Cooperation Between Law Enforcement and Internet Service Providers Against Cyber Crime, CoE, 2008
- Criminal justice access to data in the cloud: Cooperation with "foreign" service providers Background paper prepared by the T-CY Cloud Evidence Group, CoE, 2016
- The Europol SIRIUS Platform to facilitate on-line investigations, 2017
- INTERPOL E-Collection Guidance and e-MLA Initiative re secure transmission of MLAR
- ICANN draft disclosure framework for Privacy and Proxy Services

Additional protocol to the Council of Europe Budapest Convention on Cybercrime to improve international legal cooperation processes

Methodology

1.12. The Guide has been prepared jointly by EuroMed Police and EuroMed Justice, following a EuroMed Conference with the Southern Partner Countries (SPC), Regional and International Institutions and SPs in Lisbon, Portugal 23 – 25 April 2018.

1.13. To ensure SP procedures were accurate, EuroMed Police sent questionnaires to the major U.S. SPs and mapped their terms of service (TOS) to provide essential information to enable effective law enforcement and international judicial cooperation – this mapping will be presented in **Part 4** of the Guide outlining for relevant SPs for SPCs as follows:

- Contact Points
- Links to Law Enforcement Guidelines
- Procedures for:
  - Emergency Disclosure Requests
  - Preservation of electronic evidence
  - Requests for electronic evidence through non-MLA routes (voluntary disclosure) and by consent of the user

IMPORTANT NOTE: This Guide is intended to be a practical tool to aide practitioners in this ever-changing field – it is incumbent on the reader to keep up to date with relevant SP policies, evolving technologies and changing laws

PART 1

EMERGENCY DICLOSURE REQUESTS

This Part will assist with:

- Law in the United States
- Data that can be obtained
- Emergency Disclosure Request Process

Introduction

There can be many situations where disclosure of data held by an SP can be a life or death situation. This Part will review procedures law enforcement should use to request data from SPs to prevent an imminent threat of death or serious physical harm. The data secured will be used to avert the emergency, such as preventing a terrorist attack by identifying where a user of a messaging app is sending communications from. The emergency disclosure process should not be confused with urgently requesting electronic evidence through an MLAR.

The mapping table in **Part 4** will confirm the contact points and requirements necessary for Emergency Disclosure Requests (EDR) to SPs. In the absence of a SP specific form, the Simplified Uniform Request (SUR) in **Annex F** has been drafted to assist with the drafting of an EDR by law enforcement officers in the SPCs to ensure relevant information is submitted. As the major SPs are based in the U.S. this Part will mainly refer to the law in the U.S. for emergency disclosures[26]

IMPORTANT NOTE: The SP EDR procedures are correct at the time of publication – it is incumbent on practitioners to ensure they are following the correct procedure by referring to the current SP's Law Enforcement Guidelines

The U.S. legal standard on emergency disclosures

1.1.  According to the U.S. law, an emergency is considered as an *imminent danger of death or physical serious injury to any person* (18 US Code § 2702 - Voluntary disclosure of customer communications or records, (b) (8) and (c) (4)) Additionally, the standard makes it clear that there must be a need for disclosure without delay.

1.2. It is important to note imminence is essential when determining if there is an actual emergency situation. If the imminence of death or serious physical injury can no longer be sustained, there will be no basis to request disclosure of data.

1.3. Some cases, necessitate that a request is executed urgently for different reasons:

- To speed up investigations
- Risk of new crimes
- Identification of a perpetrator
- Proceeding time limits, etc

1.4. None of those will be an emergency if there is not an *imminent danger of death or serious physical injury to any person.* An urgent MLAR could be transmitted, but this should not be confused with sending an EDR to a SP.

26. See Annex H for laws and procedures in Selected States

IMPORTANT NOTE: Consideration should be given to drafting an urgent MLAR in an emergency situation as a backup to an EDR sent directly to a SP. Communication is essential with the U.S. Central Authority the Office of International Affairs (OIA), so they are kept informed about the status of any EDR to the SP and if an MLAR is required, so measures can be put in place to execute the MLAR expeditiously if necessary

What happens with requests from abroad?

1.5. In general, the language used by U.S. SPs in their law enforcement guidelines makes no clear distinction about who may make an EDR. They simply offer the possibility of disclosing '*information*' or '*user data*' with no further distinction.

1.6. In most cases, a SP would accept an EDR for **BSI** and **Traffic Data** from a non-U.S. law enforcement agency, particularly if the person making the request can establish they are genuinely a public official, such as by use of an email address from an official government domain and by providing official address and telephone contact details. If a public official in a Requesting State cannot satisfy these requirements to establish their bona fides, it may be necessary for their request to be made via a recognised third party, such as by seeking the assistance of the FBI attaché in the local U.S. Embassy.

1.7. Although, in most cases, a SP would accept an emergency request for **BSI or Traffic Data** from a non-U.S. law enforcement agency, when the request refers to **Content Data**, it could be more problematic. Some SPs may accept such an EDR relying primarily on their own policies. If **Content Data** is sought, it is probably best to go through the FBI attaché in the U.S. Embassy of the SPC.

CASE STUDY - France

Following the Charlie Hebdo terrorist attack on 7 January 2015, the French authorities contacted the FBI, who made an Emergency Disclosure Request to Microsoft for emails of two accounts. The request arrived electronically before 6am and Microsoft were able to review, extract the relevant data and send to the FBI in 45 minutes for transmission to the French authorities

Standard information to be provided for an emergency request

1.8. When submitting an EDR the following information should be provided (see SUR at **Annex F**):

- Account or user identifier, depending on the service and the specific policies of the SP. Please consult the law enforcement guidelines for each SP on this point to ensure the correct identifier is provided **IMPORTANT NOTE: Get this wrong by a letter or misplaced number and lives are at stake!**
- The nature of the emergency (e.g., report of suicide, bomb threat)
- The imminence of the threatened death or serious physical injury. It can be helpful to provide information that suggests that there is a specific deadline before which it is necessary to receive the requested information
- Explain/describe how the information sought will assist in averting the threatened death or serious physical injury
- Explain why a direct request for **BSI** and/or **Traffic Data** are insufficient to obtain the information sought
- All other available details or context regarding the particular circumstances
- Identity of the person who is in danger of death or serious physical injury
- Identification of the specific information believed to be in the SP's possession, and how that information relates to the claimed emergency

PRACTICAL NOTE

Whenever possible, it is recommended in an emergency to get immediately in contact with the FBI attaché at the local U.S. local embassy and follow his/her directions. This can lead to a quicker outcome to secure the required data to avert the emergency.

Type of Data provided

1.9. Be aware that SPs can be restrictive on their output, by providing data that would only enable law enforcement to avert the emergency. Other data necessary for the investigation or electronic evidence for a prosecution would need to be requested through an MLAR.

1.10. Also consider if the data received can be used at trial or an MLAR would have to be sent to establish provenance. If an MLAR is needed refer to the fact that the data has been disclosed under an EDR – but an MLAR is required to use at trial

IMPORTANT NOTE: If the U.S. SP decides not to disclose all or some of the data requested voluntarily, there is no appeal, even if the request has been transmitted through a FBI attaché. In this case, the SPC should issue an urgent MLAR. When this happens, it is recommended to contact the Office of International Affairs at the Department of Justice (email oia.mla@usdoj.gov or telephone number: +1 202-514-0000) to coordinate the execution of the MLAR as a priority.

Checklist for emergency requests to U.S. service providers

Is this an emergency?

Check imminent danger of death or physical serious injury to ay person
Check why the data needs to be disclosed without delay

Check sp's procedure for emergencies

Google sp's name + law enforcement + emergency requests (or similar) and Read the Guidance to Confirm required procedure
Ask colleagues, networks, fbi LEGAL attaché at the SPC u.s. embassy for assistance

Check account and or user identifier

Check sp policy related to account and or user identifier to ensure correct information provided
Provide the sp with all factual data, complementary information and pieces of evidence in the edr

Determine the type of data sought

If Content strongly consider proceeding through FBI attaché at the SPC U.S. Embassy) who can verify the emergency situation and contact the SP
If another SP has already provided emergency disclosure – confirm to the requested SP and explain how data not already provided by the other SP will avert the emergency

EXAMPLE CASE STUDIES

Someone has had an accident. His or her life is at risk. The hospital has no health records but someone states that the patient has an Internet-based service where he or she stores crucial health records. Unfortunately, the password is not available.

Conclusion: this is an emergency

Intelligence services have intercepted some communications from a terrorist group. It seems that a bombing attack could be imminent. To prevent the attack, there is need of geolocation data produced by the cell phones of the terrorists.

Conclusion: this is an emergency

A young girl has disappeared with no traces of violence. She has a Facebook account with some private information. IP related activity and private content could help investigators to locate her and to know about the disappearing causes. Initially, an MLAR based on probable cause was issued with no success due to difficulties to fulfil the standards. After some months investigators tried with an emergency request.

Conclusion: this is no longer an emergency as investigators could not prove the imminent danger of death or physical serious injury. Nevertheless, it can be an urgent MLAR where priority is requested for execution

Southern partner countries

1.11. Requesting States cannot make direct approaches to SPs in the SPCs for emergency disclosures. This means that an urgent MLAR will have to be sent or enquiries made through *police-to-police* channels in an emergency. *Police-to-police* channels are to be preferred as emergencies can be time critical and the MLAR process would be too slow.

1.12. Only Israel has any domestic legislation - the Criminal Procedure (Communication's Data) Law, 2007 Article 4 – which mandates disclosure when:

- An SP with a Bezeq Licence must provide **BSI**, **Traffic Data** or **Content Data**
- Is requested by an Israeli police chief superintendent
- To prevent immediate loss of life or
- To prevent a criminal act that endangers the safety of others

Where a SP does not have a Bezeq Licence, there is a silent agreement that in case of life and death the required data will be disclosed to the Police. It is recommended that a Requesting State send an EDR to the Cyber Fusion Centre of the Israeli National Police to expeditiously execute.

1.13. When the Requesting State is a signatory of the Budapest Convention[27], use should be made of Article 25(3) of the Convention also provides for rapid means of communication – which should always be used in an emergency situation.

1.14. The 24/7 Network of contact points, in Article 35 of the Budapest Convention and the Article 43 Specialized Body in CITO[28] could be used for Requested States to make initial contact to confirm the quickest way to handle an emergency request and ensure the required information is shared with the Requesting State expeditiously.

1.15. For those States who do not have a 24/7 Network or Specialized Body - Interpol National Bureaus should be contacted.

27. Israel and Morocco have ratified
28. Algeria, Egypt and Jordan have ratified but no 24/7 networks have been established to date

PART 2

PRESERVATION

This Part will assist with:

- Why, when and how to make a Preservation Request
- Possible notice to a user
- Major SP requirements for preservation

Introduction

It is essential to preserve electronic evidence from the outset, so it cannot be changed in format or deleted. The preservation will be a "*snap shot*" of the user's account sought to be preserved at the time the request is received and processed by the SP. Many SPs have policies to allow law enforcement authorities to contact them directly to preserve electronic evidence. This Part will review the essential steps to take to preserve electronic evidence from SPs.

IMPORTANT NOTE: The SP preservation procedures are correct at the time of publication – it is incumbent on practitioners to ensure they are following the correct procedure by referring to the current SP's Law Enforcement Guidelines when available (see SP mapping in Part 4)

STEP ONE - Locating where the sp has custody and control of the electronic evidence

1.1. It is essential to confirm where a preservation request should be sent. A SP may have data stored in different parts of the world but this does not mean that a preservation request is sent to where the SP stores the data. The preservation request should be sent to where the SP has custody and control of the data – refer to the law enforcement guidelines of the SP when available to confirm where the preservation request should be sent (see SP Mapping in **Part 4**)

STEP TWO – Is the electronic evidence available

1.2. Consider if the electronic evidence is still stored by the SP by referring to the SP's law enforcement guidelines (if available) or through police-to-police channels. The SP will just preserve what is stored in the account at the time of the preservation and will not make checks to confirm if the account has any data.

1.3. Due to the service provided to their users – some SPs store limited data for only a short period of time. Two examples are Snapchat and WhatsApp – see the table below.

Snapchat	Snapchat store logs for the last 31 days of Snaps sent and received, for 24 hours of posted stories, and for any unopened chats or those saved by a sender or recipient. This **Content Data** is removed once all recipients have viewed it or 30 days after it was sent when unopened
WhatsApp	WhatsApp do not store messages once they are delivered and opened or store the **Traffic Data** of such delivered messages. Undelivered messages are deleted from WhatsApp servers after 30 days

IMPORTANT NOTE: If a user has deleted a message this may only be retained by an SP for as little as 48 hours. This means that once an SP deletes the electronic evidence from its server it cannot be retrieved. To prevent electronic evidence being irretrievable through deletion, preservation must be a priority.

1.4. Another issue to consider is the nature of the criminal offence. Whilst there is not a dual criminality requirement to preserve, if the offence investigated will not result in execution of an MLAR, then there may be no purpose to preserve the electronic evidence. For example, the U.S. has a de minimis provision and will not execute MLARs for investigations or prosecutions of offences with a sentence of imprisonment of 12 months or less or damages below $5,000. Whilst there is not a de minimis provision for preservation it is always advisable to contact the Central Authority of the State concerned to confirm if the offence is one for which an MLAR will be executed and to seek advice about how to proceed.

IMPORTANT NOTE: If in doubt always preserve so the electronic evidence is not lost. If it is subsequently determined that the electronic evidence is no longer required, the preservation can be withdrawn by contacting the SP

STEP THREE – Making the preservation request

1.5. This is a simple procedure that can be completed in one of the following methods:

- By a foreign law enforcement officer, prosecutor or judicial authority directly contacting a SP – where a SP does not have a standard form use the SUR at **Annex F**
- Through *police-to-police* channels (where direct contact with SPs is not an option) using one of the established 24/7 networks - G7 24/7 Network, CoE Budapest 24/7 Network, or i24/7 Interpol Network. The G7 Network currently is at 82 countries and the US receives over 800 incoming requests to preserve and makes over 800 outgoing requests to preserve
- Transmitting an MLAR where the laws or policies of the Requested State do not allow direct contact with SPs from the Requesting State and police-to-police cooperation is not possible

PRACTICAL NOTE

Sending an MLAR for preservation of data will be much slower than direct contact with the SP or police-to-police channels. If an MLAR has to be sent, consideration should be given to requesting in the MLAR an appropriate legal order to produce the data immediately – rather than simply requesting preservation

1.6. The major U.S. and Canadian SPs[29] will generally accept requests for preservation directly from law enforcement authorities from an official email address (i.e. not a Yahoo or Gmail account etc). This is a voluntary practice by the SPs, the procedures and practices regarding preservation requests

29. See Annex H for laws and procedures in Selected States

vary; therefore, law enforcement authorities are encouraged to review the relevant SP law enforcement guidelines and verify the procedure directly with the SP in question.

1.7.  SPs may have a specific portal (i.e. Facebook) or a specific form to complete for preservation. **IMPORTANT NOTE: When available, online portals are the fastest, most efficient way to contact SPs and should be the preferred method whenever possible**

1.8.  Where a preservation request is sent directly to a SP the following information should be included (also see the SUR at **Annex F**):

- The specific crimes being investigated;
- The specific account/IP address/website that is to be preserved
- Identification of the law enforcement agency: Name, badge or ID number, email address
- A statement that an MLAR will be sent after the data is preserved

1.9. When a preservation request is submitted directly to a SP, there is a possibility that the account holder may learn of the inquiry, either because of the SPs technical design built into their servers or because the SP makes a notification. Generally, however, the execution of a preservation request will not be apparent to customers of the larger, more well-known SPs.

IMPORTANT NOTE: If a foreign law enforcement officer, prosecutor or judicial authority requests preservation in the U.S. or Canada the present prevailing SP policy is not to notify the user - it is recommended, due to some SP exceptions, to always include the following paragraph requesting non-disclosure:

I request that you do not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the Account(s), or otherwise alert any user of the Account(s) as to your actions to preserve the information described below, please contact me as soon as possible and before taking action.

PRACTICAL NOTE

Once an account is preserved a reference number will be provided. This should be detailed in any other correspondence with the SP – for example to extend the preservation. Additionally, this preservation reference number should be included in the MLAR to confirm the requested electronic evidence is still available. Once a court order is served on the SP the preservation reference in the MLAR will be included so the SP knows where to quickly access the electronic evidence

IMPORTANT NOTE: When making preservation requests to SPs, keep in mind that not all are reputable. Significantly, there is very little regulation of the SP industry in many States. There are occasions, for example, when a SP is actually run by a criminal enterprise, in which case a preservation request could alert the person being investigated. Therefore, before making a request directly to an unknown SP, consider the appropriate route to preserve. In the U.S. contact the 24/7 Hi-Tech Crime Network (email: 24.7@usdoj.gov) or the Central Authority - Office of International Affairs (email: oia.mla@usdoj.gov or telephone number: +1 202-514-0000) or local U.S. Embassy legal attaché. In Canada, in the event a SP refuses to preserve, foreign law enforcement should contact the 24/7 network (email: Federal_Policing_Intake_Unit@mp-grc.gc.ca) who can make a mandatory preservation demand which can be followed up by a preservation order if necessary.

PRACTICAL NOTE

If a State does not have data preservation as a domestic legal provision (see Annex G for any provisions in the SPCs) production orders or search and seizure orders could be requested by a Requesting State urgently to request the electronic evidence. Or if there is nexus between investigations in the Requesting and Requested States, a court order for production and/or seizure might be obtained as part of a domestic investigation in the Requested State and the product shared with the Requesting State.

STEP FOUR - ExtenDING

1.10. Most U.S. SPs will maintain electronic evidence for 90 days once a preservation request is received, and it can be renewed for an additional 90 days upon written request. Regardless of the method chosen, as soon as preservation has been requested, law enforcement officers, prosecutors or judicial authorities should begin pursuing one of the methods available for obtaining disclosure of the data (for example, direct request or sending an MLAR).

IMPORTANT NOTE: Submit the request to extend the preservation before the expiry of the 90 days otherwise the electronic evidence will be deleted. If a further extension is required beyond 180 days and an MLAR has been transmitted - contact the Central Authority in the Requested State to assist with a further extension until execution of the MLAR

Data retention

1.11. Preservation is different to data retention, as the former relates to a targeted request to preserve the specific user's data under criminal investigation.

IMPORTANT NOTE: Data retention/minimisation are the minimum or maximum periods of time a SP may be mandated by law to maintain data – this can assist a Requesting State to know if a SP may have the data so it can be preserved pending a legal order to produce the electronic evidence. Data that continues to be preserved should in most cases be retained after data retention laws ordinarily permit or mandate its deletion

1.12. For example, there are no mandatory data retention rules in the U.S., or at EU level, since the Data Retention Directive[30] was declared invalid by the European Court of Justice in 2014[31]. At the same time, data minimisation requirements force SPs to delete data more quickly. This contributes to the volatility of electronic evidence and results in less data being available for shorter periods of time – making the need for immediate preservation even more important.[32]

IMPORTANT NOTE: As of May 25 2018, EU users under the General Data Protection Regulation (GDPR) have the right to know exactly what data a SP is storing, get a copy of it, and have it deleted if they ask. The GDPR and EU Police Directive include requirements as regards user notification. For more information on the GDPR see the European Commission website

30. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
31. ECLI:EU:C:2014:238 (case C-293/12, Digital Rights Ireland Ltd v Minister for Communications) and The Tele2/Watson case of December 2016, ECLI:EU:C:2016:970 (case C-203/15, Tele 2 Sverige),
32. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN page 20

PART 3

REQUESTING ELECTRONIC EVIDENCE WITHOUT MUTUAL LEGAL ASSISTANCE

This Part will assist with:

- Open source information
- Evidence by consent
- Direct Request to a SP
- Police-to-Police Channels

Investigations and Prosecutions requiring electronic evidence can be sophisticated, complex and quick moving. To obtain electronic evidence at the earliest opportunity – non-MLA methods may, where available, often be appropriate.

Introduction

IMPORTANT NOTE: Each SPC should determine according to their national law if they can use the non-MLA methods outlined below and if the product can be used at trial

1.1. MLARs are not automatically required to obtain electronic evidence from SPs in all foreign States and thus might be able to be obtained more quickly than an MLAR by:

- Open source searches
- Direct Requests to a SP
- Direct contact with an account user to provide electronic evidence they download from their account
- Consent of an account user or their next of kin[33] for the SP to provide electronic evidence from an account
- Police-to-police[34] cooperation obtained by police in the Requested State by legal process or voluntary disclosure

Context

The fact the electronic evidence is not requested through MLA does not mean that the data is ONLY for '*intelligence only*' or not for use '*in court*'. It refers to the method by which the evidence is obtained i.e. not via an MLAR.

IMPORTANT NOTE: An MLAR will be necessary if obtaining the electronic evidence by coercive powers or a court or legal order is a legal requirement to adduce admissible electronic evidence in the Requesting State

1.2. It must be emphasised that, before obtaining electronic evidence from another State without an MLAR, the Requesting State must be satisfied that:

- They are not committing a criminal offence in the Requested State by requesting data directly or the SP is in contravention of a Requested States' law by disclosing data
- Obtaining electronic evidence by non-MLA means will be adequate for the purpose for which it has been sought by the Requesting State. For example, production of the data through non-MLA channels is admissible if needed for that purpose in the Requested State

33. In July 2018 Germany's Federal Court of Justice ruled that social media accounts are no different than personal letters and diaries and can be inherited – however - most SPs will still require a domestic court order of the Requesting State for production of the electronic evidence
34. Although specific reference is made to police there can also be cooperation between prosecution or judicial authorities

1.3. This Part must be read in conjunction with the specific laws of the SPC and Requested States to confirm if the electronic evidence can be obtained and used for any investigation or prosecution. This Part is intended to outline the possibilities for securing electronic evidence without the need for an MLAR and **NOT** to provide guidance on the use of the electronic evidence obtained at trial. The use of the electronic evidence requested without MLA should be discussed with the relevant prosecutor or judicial authorities to determine its use in the absence of an MLAR.

IMPORTANT NOTE: An MLAR must be sent if coercive powers or a court order is needed to request the electronic evidence in the Requested State

Open source searches

IMPORTANT NOTE: The use of electronic evidence from open source searches should be discussed with the relevant prosecutor or judicial authorities to determine its use in the absence of an MLAR

1.4. National resources should be exhausted before requesting electronic evidence through non-MLA or MLA routes – this includes making Open Source Searches to:

- Locate a user through online and publicly available tools – such as an IP address
- Identifying owners of domain names[35]
- Evidence criminality through publicly available social media accounts – this can range from images or videos posted by individuals or posts of incriminating criminal behaviou

Useful Links

1.5. Information on Open Source Searches is available in the following publications:

- Foreign Terrorist Fighters, Manual for Judicial Training Institutes South-Eastern Europe, UNODC, 2017, Chapter 4.2 On-Line Investigations, Open Source Investigations, pages 30-40
- Electronic Evidence Guide – A Basic Guide for Police Officers, Prosecutors and Judges, CoE 2014, Chapter 4.3 On-line Sources of Information, pages 101 – 110; **restricted**, can be obtain by practitioners via the CoE portal Octopus Cybercrime Community

Voluntary disclosure

1.6. SPs might voluntarily disclose electronic evidence to a law enforcement officer, prosecutor or judicial authority of a Requesting State in the following non-emergency situations:

- Where the user consents

35. Please note the whois database is subject to the General Data Protection Regulation and records may not be accurate

- If the user is deceased - where his or her next-of-kin consent to disclosure and a domestic court order for production is obtained in the Requesting State
- Following a direct request to a SP for **BSI** or **Traffic Data** by SPC law enforcement officer, prosecutor or judicial authority

1.7. Each SP will have a different policy – or no policy at all (see the SP Mapping in **Part 4**). Although, SPs will generally not disclose **Content Data** voluntarily following a direct request from a foreign law enforcement officer, prosecutor or judicial authority.

Consent

1.8. An MLAR for **Content Data** will be required - unless the user's consent is obtained to:

- Access a device where relevant **Content Data** is stored or
- To access an account or application by providing usernames and passwords

1.9. User consent can be a useful tactic to access an encrypted device or application. Also consider the possibility of accessing encrypted applications or content by obtaining consent from the recipient.

Direct requests

1.10. The SPs may respond to direct requests by SPC law enforcement, judicial authorities or prosecutors and voluntarily disclose **BSI** or **Traffic Data**.

1.11. SPs will ensure their customer's data remains private unless disclosure is justified. The following are standard requirements for any direct request for a user's data:

- Bona-fide request for prevention, detection or investigation of offences
- The request is for relevant electronic evidence linked to the investigation (i.e. not fishing for information over the existence of the account)
- The location of the victim and perpetrator in the SPC
- Impact of harm caused by the criminality in the SPC

1.12. It is recommended that each SPC should have a Single Point of Contact (SPOC) responsible for liaising with SPs and obtaining the electronic evidence to avoid duplication.

1.13. It is incumbent upon law enforcement or prosecutor to consider a direct request to a SP as a first option for **BSI** or **Traffic Data**. This may avoid the necessity to send an MLAR or supplement information in an MLAR to satisfy the required legal standard for **Content Data** (i.e. probable cause in the U.S. see **Part 5** below)

IMPORTANT NOTE: Always consider if the data obtained through user consent or a direct request can be produced in evidence. SPs may provide a supporting statement (custodian of records declaration under U.S. law) upon request to establish the provenance of the electronic evidence – others may confirm the electronic evidence is self-authenticating – other SPs may provide no information. If the product from voluntary disclosure cannot be used at trial – this may require an MLAR to ensure the electronic evidence is produced in the format required for proceedings in a SPC.

1.14.  A model form for direct requests for voluntary disclosure, when a SP does not have a specific template, is provided at **Annex E**. This requires a foreign law enforcement officer, prosecutor or judicial authority to provide the following information to a SP:

- The electronic evidence requested and user/account identifiers for the specific SP
- Any specific date range for **Traffic Data**
- Relevance of the **BSI** and/or **Traffic Data** to the offence
- Who authorised the request – this could be a senior law enforcement officer, prosecutor or investigating judge
- A signed legal order (translated into English) obtained in the Requesting State to request the **BSI** and/or **Traffic Data** should be attached. Attaching a domestic order may not mandate a SP in another State to voluntarily disclose – but could allow the SP to justify voluntary disclosure (as required by Microsoft, Snapchat and Twitter)
- Confirm who the **BSI** and/or **Traffic Data** should be transmitted to
- Confirm if a statement or affidavit is required to authenticate the requested electronic evidence (if not self-authenticating)

User notification

1.15. SPs' user-notification policies are not clear for Direct Requests, so the SP should be instructed not to notify a user if this will impact the investigation. Include specific reasons why user notification would impact – for example notifying the user will alert them about a covert investigation and lead to destruction of electronic evidence.

1.16. If the investigation is sensitive or covert it may be considered best to send an MLAR requesting a court order to ensure confidentiality. This should be assessed on a case-by-case basis to determine the appropriate course of action. However, where a user can be notified (i.e. already arrested/questioned on evidence and preservation of the account is already in place) then the SP should be informed that notification is not an issue.

Police-to-police cooperation[36]

1.17. Police-to-police channels are designated single points of contact in States and can include Interpol National Crime Bureaus or 24/7 Networks. Some States may also have Memorandums of Understanding that allow for sharing of data with specific States.

1.18. Police-to-police cooperation can be a speedy route to produce **BSI** and **Traffic Data**. The State receiving any data using police-to-police cooperation will have to determine if this can be used evidentially and respect the Requested State's law if this requires sensitive handling.

36. The same principles in this section can include cooperation between prosecutors and judicial authorities in other States

1.19. If the data cannot be used evidentially it could also be used to:

- Confirm that the electronic evidence is available and should be preserved
- Direct or exclude other appropriate lines of investigative inquiry
- Include in an MLAR for electronic evidence as supporting grounds for a judicial order for disclosure of data from the SP

1.20. Police-to-police cooperation can also be used for spontaneous sharing of data (see Article 26 Budapest, UNTOC Article 18(4) and UNCAC Article 46(4)) relating to investigations or proceedings, within the limits imposed by domestic law, in the common interest of responding to criminal acts.

1.21. Good practices related to United States of America service providers and agencies:

1.22. For foreign judicial authorities the primary contact can be with representatives from the U.S. Department of Justice (DOJ) Criminal Division's Office of International Affairs (OIA). OIA is the U.S. Central Authority and can be an invaluable resource for foreign partners' ability to investigate and prosecute crime abroad by providing them with U.S. evidence and other assistance. OIA is DOJ's primary expert on international criminal matters, providing legal and strategic guidance to DOJ leadership with respect to present and future challenges in international criminal law enforcement. OIA and the Criminal Division currently have Department of Justice Attachés stationed in U.S. Embassies in Bangkok, Bogota, Brussels, London, Manila, Mexico City, Paris, and Rome. These Attachés work with U.S. prosecutors and law enforcement personnel as well as with foreign authorities in their assigned countries or regional areas on operational matters relating to criminal investigations and prosecutions, including requests for the return of fugitives and requests for mutual legal assistance.

1.23. Additionally, several U.S law enforcement agencies maintain law enforcement attaches (e.g. FBI, DEA, ICE, or U.S. Secret Service) in foreign countries. This extensive network of attaches is located in the U.S Embassies in those countries and can assist foreign partners with emergency disclosure requests, preservation requests, contact with the service provider and even reviewing draft mutual legal assistance treaty or letter rogatory requests. In certain exceptional circumstances in foreign investigations involving counterterrorism matters, the FBI is able to initiate a parallel investigation in the U.S. and thereby obtain and provide information which may be useful and/or critical in said foreign investigation. This would only be the circumstance when the terrorist or criminal organization or criminal activity is also a priority for the FBI.

PRACTICAL NOTE

If evidence has been obtained in the course of an extant investigation confirm if this could be shared through police-to-police cooperation without the need to send an MLAR (for the U.S. the **FBI attaché at the local U.S. Embassy** should be contacted) There may be occasions where information will only be passed on an intelligence basis through police-to-police cooperation (due to the covert nature of the investigation) and cannot be used in evidence in the Requesting State if an investigation is ongoing.

CASE STUDY - *Benedik v Slovenia*

In 2006, the Swiss police informed Slovenian law-enforcement authorities about a dynamic IP address that was being used in a peer-to-peer file-sharing network linked to the sharing of child pornography. The Slovenian police, without first obtaining a court order, requested and obtained from a Slovenian SP data regarding the user of the dynamic IP address. The European Court of Human Rights in its judgement held there had been a violation of Article 8 (right to respect for private and family life) with regard to the failure of the Slovenian police to obtain a court order before accessing **BSI** associated with the dynamic IP address. This means that relevant legal safeguards must be put in place when law enforcement authorities want

PRACTICAL NOTE

If information is received from an overseas SP or through police-to-police cooperation it is important that any IP address is resolved through appropriate court orders

General data protection regulation

1.24. The SPCs should be aware of the General Data Protection Regulation (see **Annex I**) that governs international transfer of personal data for law enforcement or criminal justice purposes belonging to an individual ('data subject'). The GDPR ensures the data subject's interests are protected.

1.25. Transfer between EU Member States and the SPCs will be subject to the GDPR and each State concerned must ensure compliance. This could be through an adequacy decision that the SPC concerned has appropriate procedures in place or safeguards to protect the interests of the data subject. Data can also be transferred in order to protect the interests of the data subject, prevent the immediate and serious threat to public security of an EU Member State or third-party State or if in the public interest.

PART 4

SERVICE PROVIDER MAPPING[37]

37. This mapping will be available and updated in the Euromed Threat Forum

Below is a summary of SP Contact Points and procedures for preservation, EDRs and voluntary disclosure - produced from the EuroMed Police Mapping:

Adobe is a multinational software company best known for Photoshop, an image editing software, Acrobat Reader, the Portable Document Format (PDF) and Adobe Creative Suite, as well as its successor Adobe Creative Cloud. For all Adobe customers outside of the U.S. procedure is governed by Irish law.

LE Guidelines https://www.adobe.com/legal/lawenforcementrequests/law-enforcement-intl.html

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Adobe may choose to disclose data they have to protect human life if:
  - They receive information that gives them a reasonable good faith belief that there is a risk of imminent harm (i.e., death or serious physical injury) to a person, and
  - That they have information in their possession that may avert that harm.

Use SUR at **Annex F**

Contact

It is recommended to contact the following numbers in the U.S.:

- Adobe's U.S. Law Enforcement Response Hotline: **415-832-7614**
- U.S. Law Enforcement Response Fax Line: **415-723-7869**

PRESERVATION REQUESTS

Procedure

- The length of time Adobe keeps different types of customer data varies depending upon the nature of the service and type of data at issue
- For example, Adobe keeps internet protocol (IP) address logs related to Adobe ID sign-ins for 90 days, but **Content Data** a customer has deleted from their Creative Cloud account generally is not recoverable after 72 hours
- When Adobe receive a preservation request from an agency investigating a crime for data stored in the U.S., Adobe will preserve then-existing customer data for 90 days in anticipation of receiving an MLAR
- For data stored outside of the U.S. the telephone number below should be contacted.

Use SUR at **Annex F**

Contact

- Adobe's U.S. Law Enforcement Response Hotline: **415-832-7614**
- U.S. Law Enforcement Response Fax Line: **415-723-7869**

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- Where a law enforcement request relates solely to fraudulent use of a credit card to purchase goods or services on Adobe.com, Adobe may voluntarily and in its sole discretion, disclose basic purchase and delivery data in response to legal process that is valid in the jurisdiction where the purchase was made

Use Model Form at **Annex E**

Contact

- Direct Requests must be made to Adobe Ireland using the contact information below and accompanied by an English language translation
- Adobe Systems Software Ireland Limited Attn: Law Enforcement Requests 4-6 Riverwalk, City West Business Campus Saggart, Dublin 24, Ireland

airbnb

Airbnb is an online marketplace and hospitality service for people to lease or rent short-term lodging including holiday cottages, apartments, homestays, hostel beds, or hotel rooms – U.S. or Irish law applies

LE Guidelines https://www.airbnb.co.uk/help/article/960/how-does-airbnb-respond-to-data-requests-from-law-enforcement

EMERGENCY DISCLOSURE REQUESTS

Procedure

- In the event of an emergency involving the danger of death or serious physical injury to a person, law enforcement agents may make an emergency disclosure request by email with the subject: **Emergency Disclosure Request.**

Use SUR at **Annex F**

Contact
Email to: leoinfo@airbnb.com

PRESERVATION REQUESTS

Procedure
- The Airbnb law enforcement guidelines do not specifically refer to preservation requests
- Airbnb will research if the concerned user is likely a non-U.S. resident or a U.S. resident
- If a non-U.S. resident law enforcement serve the request on Airbnb Ireland

Use SUR at **Annex F**

Contact
Email to: leoinfo@airbnb.com

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed
- In case of alleged crimes against a person, a person's property or alleged fraud, a valid request on law enforcement agency letterhead is required for the disclosure of **BSI**, **Traffic Data** or basic payments-related data (not including contents of communications) to be considered by Airbnb Ireland
- For all other alleged crimes, a valid request on law enforcement agency letterhead is required for the disclosure of **BSI** to be considered by Airbnb Ireland and a valid order ("ordonnance judiciaire", "Decreto del Giudice per le Indagini Preliminari", subpoena, "Auskunftsersuchen", "richterlicher Beschluss/formelles Auskunftsersuchen") is required for the disclosure of **Traffic Data** relating to an account or payments-related data (not including contents of communications) to be considered by Airbnb Ireland
- For **Content Data**, an appropriate and binding court order (or equivalent local warrant procedure) is required for the disclosure to be considered by Airbnb Ireland
- Airbnb explicitly reserve the right to require an MLAR for the above if deemed appropriate
- Airbnb is unable to process overly broad or vague requests and will only consider law enforcement requests that are:

  - Typed
  - Duly signed and stamped by the appropriate law enforcement officer who is empowered by local law to represent the law enforcement unit that is making the request
  - Addressed to Airbnb, Inc. or Airbnb Ireland (as appropriate) and sent to Airbnb, Inc. or Airbnb Ireland (as appropriate) directly
  - Translated into English
  - Requests should explicitly mention the following elements:
  - All known email addresses, names, and aliases of data subject or all known physical addresses and telephone numbers of the data subject
  - Law enforcement officer's name, department, street address, telephone number, fax number, and email address.

- Exactly what information is requested, why it is requested, and how it pertains to the relevant investigation
- The applicable act or law under which the law enforcement agency is requesting the data

Use Model Form at **Annex E**

Contact

- Requests should be sent to:
  Airbnb Ireland
  Law Enforcement Liaison
  The Watermarque Building
  South Lotts Road
  Ringsend
  Dublin 4
  Ireland

Amazon is an electronic commerce and cloud computing company headquartered in Seattle Washington – U.S. law applies

LE Guidelines https://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Amazon reserves the right to respond immediately to urgent law enforcement requests for information in cases involving a threat to public safety or risk of harm to any person
- These requests must be submitted using Amazon's Emergency Law Enforcement Information Request Form https://d1.awsstatic.com/certifications/amazon-emergency-law-enforcement-information-request-form.pdf

Contact

Email to: emergency-LE-request@amazon.com

PRESERVATION REQUESTS

Procedure

- Upon receipt of a lawful and binding request Amazon will preserve requested information for up to 90 days

Use SUR at **Annex F**

Contact
Email to: sta-ermittlungen@amazon.de

VOLUNTARY DISCLOSURE

Not available

Apple

Apple is a technology company, headquartered in Cupertino, California, that designs, develops and sells consumer electronics (e.g. iPhones), computer software (e.g. iOS) and online services (e.g. iCloud) – U.S. law applies

CONTACT INFORMATION

- If investigators need assistance, use the Government/Law Enforcement Information Request template and transmit it to the relevant email address for their geographical region
- The template can be found here: https://www.apple.com/legal/privacy/gle-inforequest.pdf
- Government agencies in Europe, Middle-East, India and Africa via email: law.enf.emeia@apple.com
- **LE Guidelines** https://images.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Emergency Requests relate to circumstances involving imminent danger of death or serious physical injury to any person. Apple considers a request to be an emergency request when it relates to circumstance(s) involving imminent and serious threat(s) to:

  – The life/safety of individual(s)
  – The security of a State
  – The security of critical infrastructure/installation(s)

Use the Request Form at: https://www.apple.com/legal/privacy/le-emergencyrequest.pdf - see Annex Fii

Contact

- Apple allows direct transmission from the official government or law enforcement agency email address to the mailbox: exigent@apple.com with the words "***Emergency Request***" in the subject line
- If the government or law enforcement agency needs to contact Apple after hours (before 8:00 am or after 5:00 pm Pacific time) for an emergency inquiry, it can be done calling Apple's Global Security Operations Center (GSOC) at **(408) 974-2095**
- In the event that Apple produces customer data in response to an Emergency Government & Law Enforcement Information Request, a supervisor for the government or law enforcement agent who submitted the Emergency Government & Law Enforcement Information Request may be contacted and asked to confirm to Apple that the emergency request was legitimate. The government or law enforcement agent who submits the Emergency Government & Law Enforcement Information Request should provide the supervisor's contact information in the request

PRESERVATION REQUESTS

Procedure

- Apple will preserve data for 90 days plus a 90-day extension, but will continue the preservation for longer periods of time for MLAR cases
- Preservation requests must include the relevant Apple ID/account email address, or full name and phone number, and/or full name and physical address of the subject Apple account.
- Apple will make sure preservations are aligned with the MLAR process later received before they will turn over preserved data

Contact

 Use SUR at **Annex F**

- A request to preserve data in advance should be sent by email to the mailbox: subpoenas@apple.com

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- Device Registration Information:
  - **BSI**, including, name, address, email address, and telephone number provided to Apple by customers when registering an Apple device.
  - Date of registration, purchase date and device type may be included.
  - **IMPORTANT NOTE:** Apple do not verify this information, and it may not reflect the owner of the device

- Customer Service Records:
  - Contacts with Apple customer service regarding a device or service. This information may include records of support interactions with customers regarding a particular Apple device or service
  - Information regarding the device, warranty, and repair

- iTunes Information:

  - BSI such as name, physical address, email address, and telephone number
  - Information on iTunes purchase/download transactions and connections, update/re-download connections
  - iTunes Match connections
  - iTunes connection logs with IP addresses

    » **IMPORTANT NOTE:** ITunes purchase/download transactional records are controlled by iTunes S.à.r.l., which is a Luxembourg company

    » Due to legislative provisions, iTunes can only respond to requests when they have been validated by the Public Prosecutor of Luxembourg and forwarded to iTunes for response. Requests for these records should be submitted to the Public Prosecutor of Luxembourg at the following address: Parquet Général, Procureur Général d''Etat, Cité Judiciaire Bât. CR, Plateau du St Esprit, L-2080 LUXEMBOURG, fax number: +352 47 05 50, email: parquet.general@justice.etat.lu

- Apple Retail Store Transactions:

  - Point of Sale transactions are cash, credit/debit card, or gift card transactions that occur at an Apple Retail Store.
  - Information regarding the type of card associated with a particular purchase, name of the purchaser, email address, date/time of the transaction, amount of the transaction, and store location

- Apple Online Store Purchases:

  - Online purchase information including name, shipping address, telephone number, email address, product purchased, purchase amount, and IP address of where a purchase was made.

- iTunes Gift Cards:

  - Apple can determine whether the card has been activated or redeemed as well as whether any purchases have been made with the card.
  - When iTunes gift cards are activated, Apple records the name of the store, location, date, and time.
  - When iTunes gift cards are redeemed through purchases made on the iTunes store, the gift card will be linked to a user account.
  - Information about online iTunes store purchases made with the card will require a request to be submitted to the Public Prosecutor of Luxembourg at the following address: Parquet Général, Procureur Général d''Etat, Cité Judiciaire Bât. CR, Plateau du St Esprit, L-2080 LUXEMBOURG, fax number: +352 47 05 50, email: parquet.general@justice.etat.lu parquet.general@justice.etat.lu

- iCloud:

  - iCloud is Apple's cloud service that allows users to access their music, photos, documents, and more from all their devices. iCloud also enables subscribers to back up their iOS devices to iCloud. With the iCloud service, subscribers can set up an iCloud.com email account. iCloud email domains can be @icloud.com, @me.com and @mac.com. The following information may be available from iCloud:

  - » BSI: When a customer sets up an iCloud account, BSI such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available.
  - » Mail Logs: iCloud mail logs are retained for approximately a period of 60 days. Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses.

- MAC Address:
  - A Media Access Control address (MAC address), is a unique identifier assigned to network interfaces for communications on the physical network segment. Any Apple product with network interfaces will have one or more MAC addresses, such as Bluetooth, Ethernet, Wi-Fi, or FireWire. The MAC address can be available by providing Apple with a serial number (or in the case of an iOS device, IMEI, MEID, or UDID)

- Game Center Information:
  - Game Center is Apple's social gaming network. The following may be available:
  - Game Center connections for a user or a device.
  - Connection logs with IP addresses and transactional records

- iOS Device Activation:
  - When a customer activates an iOS device or upgrades the software, certain information is provided to Apple from the service provider or from the device, depending on the event. IP addresses of the event, ICCID numbers, and other device identifiers may be available.

- Sign-on Logs:
  - Sign-on activity, including connection logs with IP addresses and transactional records, for a user or a device to Apple services such as iTunes, iCloud, My Apple ID, (and Apple Discussions, when available) may be obtained from Apple.

- Find My iPhone:
  - Location information for a device located through the Find My iPhone feature is user facing. Therefore, Apple does not have records of maps or email alerts provided through the service. The following can be available:
  - Find My iPhone connection logs. **IMPORTANT NOTE:** Apple does not have GPS information for a specific device or user

- Password Activity Logs:
  - Apple ID password activity logs, including connection logs with IP addresses and transactional records, for a user.
  - Information regarding password activity actions including password reset information for a user may.
  - The request should be sent to Apple Distribution International in Ireland.
  - Apple will provide a certificate of authenticity if requested

IMPORTANT NOTE: Apple, if asked by the user, will provide full details about a law enforcement request

Procedure

Use the Form at https://www.apple.com/legal/privacy/gle-inforequest.pdf) – see Annex Ei

Contact

Email to: law.enf.emeia@apple.com

DISCLOSURE BY CONSENT

- A user or next-of-kin (if under 18) can sign a notarized consent to request a download of a user's account or to unlock a device
- Apple will not provide a statement authenticating the content produced by consent

IMPORTANT NOTE: Use of iOS 8 and above means a device cannot be unlocked - unless the pin is known. This means Apple cannot provide any electronic evidence even with notarized consent

ASKfm is a global social networking site where users create profiles and can send each other questions. The site was founded in 2010 in Latvia and its headquarters was moved to Dublin, Ireland – both Irish and U.S. law applies

LE Guidelines http://safety.ask.fm/ask-fm-guide-for-law-enforcement-requests/

EMERGENCY DISCLOSURE REQUESTS

- All requests for emergency disclosures must be made by law enforcement in the same way set out for direct requests
- ASKfm will also need answers to the following questions:
  - What is the nature of the emergency involving death or serious physical injury?
  - Whose death or serious physical injury is threatened?
  - What is the imminent nature of the threat? Include information that suggests that there is a specific deadline before which it is necessary to receive the requested information and/or that suggests that there is a specific deadline on which the emergency involving death or serious physical injury will occur (e.g., tonight, tomorrow at noon)
  - Explain/describe how the information will assist in averting the threatened death or serious physical injury?

- Also include the law enforcement officer's:
  - Full name
  - Title
  - Rank
  - Badge number and
- Confirmation that the information provided is complete and accurate

Use SUR at **Annex F**

Contact

- The information must be sent via email as a ".pdf" of a letter on official letterhead or via an official government email account to lawenforcement@ask.fm

PRESERVATION REQUESTS

Procedure

- ASKfm accept requests from law enforcement agencies to preserve records which constitute potentially relevant evidence in criminal proceedings pending the service of valid legal process
- ASKfm will preserve, but not disclose, a one-time temporary snapshot of the then-existing user account record for 90 days pending service of valid legal process
- This period may be extended pending an MLAR or service of valid and mandatory legal process in the case of Irish law enforcement

Use SUR at **Annex F**

Contact

Email to: lawenforcement@ask.fm

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- Where ASKfm may in limited circumstances provide non- content information
- This non-content information may be disclosed where ASKfm forms a good faith belief that the request is justifiable (under ASKfm's policies), having assessed it on its merits and taking into account the relevant parts of ASKfm's Privacy Policy and Terms of Service
- In making this assessment, ASKfm will apply the follow analysis:
  - Does the request accord with legal standards in the jurisdiction from which it is made?
  - Is the request intended to protect ASKfm's users or ASKfm or the public?
  - Is the request consistent with internationally recognised norms, such as freedom of speech?

However, except in the case of emergency situations ASKfm will not disclose content unless otherwise obliged to do so by Irish law

Procedure
All direct requests for non-content data must comply with the following formalities:

- Be made by a dated request addressed to ASKfm Europe Limited;
- Issued on government or official letterhead, or has a caption identifying the court or agency that issued the request;
- Signed by a judge or other senior official or officer who provides their title and contact information;
- Be consistent with the legal requirements of the Requesting State;
- Be consistent with Irish law;
- Identify the target, for which electronic evidence is requested, by providing as much of the following information as possible:

  – The account login;
  – The account email address;
  – The full name of user as registered with ASKfm; and
  – The full URL of the question and answer at issue (e.g. http://ask.fm/askfm/answer/119942892554)

- Specify the types of non-content account electronic evidence being requested;
- Specify the legal basis (applicable law) for the request, including the alleged offence (if relevant);
- Specify why the relevant electronic evidence is being sought; and
- Specify to whom or how the information being requested is to be delivered

 Use the Model Form at **Annex E**

Contact
Email to: lawenforcement@ask.fm

DISCLOSURE BY CONSENT

- ASKfm will disclose information based on user consent where sufficient information is provided to verify that the person providing the consent is the actual creator of the account and where law enforcement endorses the authenticity of the consent
- ASKfm will not release information if the user is unable or unwilling to provide registration information that corresponds with the information on record with ASKfm
- In the event that the information provided by the user does not match the information on record with ASKfm, proper legal process will be required before any information is released

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Data outlined above if not obtained voluntarily
- ASKfm username
- Email address
- Account creation date
- Access log data
- Content including images, unanswered questions and answers

Atlassian is an Australian owned enterprise software company that develops products for software developers, project managers and content management. It is best known for its issue tracking application, Jira, and its team collaboration and wiki product, Confluence. U.S. Law applies

LE Guidelines https://www.atlassian.com/legal/guidelines-for-law-enforcement

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Atlassian evaluates emergency requests on a case-by-case basis.
- If information is provided that gives Atlassian a good faith belief that there is an emergency involving imminent danger of death or serious physical injury to any person, they may provide information necessary to prevent that harm if they are in a position to do so, consistent with applicable law
- Use this form

Contact

- Emergency requests can be sent by email to lawenforcement@atlassian.com ***with the subject line: "Emergency Disclosure Request"***

PRESERVATION REQUESTS

Procedure

- Atlassian will preserve Customer Information for 90 days upon receipt of a valid law enforcement request
- Atlassian will preserve information for an additional 90-day period upon receipt of a valid request to extend the preservation
- If Atlassian does not receive formal legal process via MLAR for the preserved information before the end of the preservation period, the preserved information may be deleted when the preservation period expires
- Preservation requests must be sent on official law enforcement agency letterhead, signed by a law enforcement official, and must include:

  - The relevant account information identified below for the customer whose information is requested to be preserved;
  - A valid return email address; and
  - A statement that steps are being taken to obtain a court order or other legal process for the data sought to be preserved

 Use SUR at **Annex F**

Contact
Email to: lawenforcement@atlassian.com

VOLUNTARY DISCLOSURE

Not available

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Basic Customer Account Information (Atlassian systems): Username, email address, URL, Support Entitlement Number (SEN)
- Customer Information involving Atlassian products:

  - Bamboo: email address
  - Bitbucket Cloud: Username, team name, email address, and/or repository URL
  - Confluence: User ID, email address, IP address, URL, SEN
  - Crucible: email address
  - Fisheye: email address
  - Hipchat: User ID, email address associated with the user account, and/or Hipchat group name and group administrator's email address
  - JIRA (core, service desk or software): username, email address, URL, SEN
  - OnDemand: username, email address, URL, SEN
  - Sourcetree: email address
  - StatusPage: email address and status page URL
  - Stride: User ID, email address associated with the user account, group name, group administrator's email address
  - Trello: Username, email address, URL (for board(s))

Baaz is a social media platform providing multiple perspectives on news and enables sharing of news across all social platforms – had been used by IS to share online posts. Headquartered in San Francisco, California – U.S. law applies

EMERGENCY DISCLOSURE REQUESTS

Procedure

- No specific emergency policies. Baaz may disclose any information to law enforcement or other government officials as they believe necessary or appropriate, in connection with an investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose them to legal liability.

Use SUR at **Annex F**

Contact

Email to: infor@baaz.com

PRESERVATION REQUESTS

Procedure

- May preserve and store account information and content if it believes in good faith that such preservation is necessary to comply with legal processes, respond to claims that the content violates the rights of third parties, to protect the rights, property or personal safety of Baaz, its users and the public

Use SUR at **Annex F**

Contact

Email to: infor@baaz.com

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- May disclose any information to law enforcement or other government officials as they believe necessary or appropriate, in connection with an investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose Baaz to legal liability

Procedure

Use the Model Form at **Annex E**

Contact

Email to: info@baaz.com

File-syncing storage and sharing application which allows a user to securely store in the cloud, manage and share files. Headquartered in Redwood City, California – U.S. law applies

EMERGENCY DISCLOSURE REQUESTS

Procedure

- May disclose information to a third party if an emergency which Box believe in good faith requires disclosure of information to assist in preventing the death or serious bodily injury of any person

Use SUR at **Annex F**

Contact

- No specific contact address other than the general for privacy issues: privacy@box.com

PRESERVATION REQUESTS

Procedure

- No specific preservation policies

Use SUR at **Annex F**

Contact

- No specific contact address other than the general email for privacy issues: privacy@box.com

VOLUNTARY DISCLOSURE

Not available

DropBox is a file hosting service that offers cloud storage, file synchronization, personal cloud and client software. Headquartered in San Francisco, California – U.S. law applies

EMERGENCY DISCLOSURE REQUESTS

Procedure

- May disclose information to third parties if Dropbox determine that such disclosure is reasonably necessary to:
  - Comply with legal obligations
  - Protect any person at risk of death or serious injury
  - Prevent fraud or improper use of Dropbox or that affect Dropbox users
  - Protect the property rights of Dropbox.


Use SUR at **Annex F**

Contact

- No specific contact address other than the general for privacy issues: privacy@dropbox.com

PRESERVATION REQUESTS

Procedure

- No specific preservation policies


Use SUR at **Annex F**

Contact

- No specific contact address other than the general email for privacy issues: privacy@dropbox.com

VOLUNTARY DISCLOSURE

Not available

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Name provided by the user
- Email address provided by the user
- Time and date of account registration
- Type of account

- IP address recorded for the last account access
- IP addresses recorded for account log ins
- Devices associated with an account
- User content, whether in files or otherwise to include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with or relating to postings, communications and any other activities to or through the requested account, whether such records or other evidence are in electronic or other form.

A website for online auctions – U.S. law applies

EMERGENCY DISCLOSURE REQUESTS

Please refer to section on voluntary disclosure

PRESERVATION REQUESTS

Procedure

- No specific preservation policies

Use SUR at **Annex F**

Contact

- No specific contact address

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- User information
- The following will not be disclosed:
  - Item image and description:
    - » The listing for an item as seen on the site (available until archived 90 days after the listing end date)
  - User Agreement:
    - » Terms and conditions applicable to the use of our services

- About Me Page:
  - » Users can create an "About Me' page to tell others about themselves

Procedure:

- LEP (Law Enforcement Portal) is a tool that allows registered law enforcement officers to obtain eBay user information without the need of submitting a data request. An eBay User ID, email address or item number is required to obtain user data. The officer can download the information directly from the portal. Requests will be retrievable in 3-5 business days.
- LERS (Law Enforcement eRequest System) is an online web-form designed for law enforcement and government agencies to submit their eBay data requests, inclusive of uploading their supporting documents such as a letterhead, court order or subpoena. This site (https://lers.corp.ebay.com) may only be used by law enforcement personnel who will go through an authentication process. Requests submitted via LERS are handled manually by our team and are processed in approximately 20 business days.
- Requests submitted through LERS must comply with the following legal requirements:
  - Must be addressed to eBay, Inc.
  - Must be a typed official document bearing the logo of the requestor
  - Must be signed by an agent or court officer with the authority to issue compulsory orders.
- Also, all requests should include:
  - Requester's name, department, street address, telephone, email address and fax.
  - As much information about the subject as possible to locate accounts
  - User IDs, Email Address, or Item Numbers
  - Exactly what information is required and how it pertains to eBay and the investigation

IMPORTANT NOTE: Priority will be given only in particular circumstances and investigation types (i.e. life-threatening issues etc.) and only where the sense of urgency is appropriately specified. eBay, Inc. reserves the right to determine the urgency level based on an assessment of known facts

Facebook (including Instagram) is an online social media and social networking service, headquartered in Menlo Park, California – U.S. Law applies

CONTACT INFORMATION

Mr. Cristian Perrella - Email: cp@fb.com
Mailing address: Facebook Ireland Ltd | 4 Grand Canal Square | Dublin 2
Attention: Facebook Security, Law Enforcement Response Team
Law Enforcement Guidelines https://www.facebook.com/safety/groups/law/guidelines/

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Facebook will respond within minutes, 24/7 to a matter involving imminent harm to a child or risk of death or serious physical injury to any person
- **IMPORTANT NOTE:** Facebook will not review or respond to requests submitted by non-law enforcement officials
- A Request should include:

  - Name of issuing law enforcement agency
  - Badge or identification number of responsible agent
  - Email address from a law enforcement domain – so must not be from a google or yahoo email account etc.
  - Direct contact phone number
  - Signed by a law enforcement authority
  - A detailed explanation of the emergency and how it poses an imminent threat to human life and when it is thought will happen
  - Type of data being requested
  - Explanation on how data requested will assist in addressing the emergency

PRESERVATION REQUESTS

Procedure

- A request must include:

  - Name of issuing authority
  - Badge/ID number if a law enforcement agency request

  - Email address from a law enforcement agency domain (i.e. not a Yahoo!, Google, etc. address) and direct contact phone number;
  - The email address, user ID number or username of the Facebook profile

- **IMPORTANT NOTE:** The portal currently allows only two 90-day extensions. Facebook will only extend preservation after the second 90-day extension, for very serious matters and only in exceptional circumstances
- Preservations are automatically expunged once they expire (so do not miss an extension deadline!)

- If the Facebook portal does not allow preservation – this means there is no account for the user. This could mean the incorrect details have been provided or the account has been deleted
- Facebook can reassign their account, so that someone else may access their preservations and legal process requests on the portal if necessary
- **IMPORTANT NOTE:** Some of the actions a user does on Facebook may not be stored in that users account. For example, A may still have messages from B even after B deletes their account. That information remains after B deletes their account. Therefore, consider if it is appropriate to preserve both A and B's accounts
- It may take up to 90 days to delete all of the things a user has posted, like photos, status updates or other data stored in backup systems. While Facebook are deleting this information, it is inaccessible to other people using Facebook.
- Copies of some material (e.g. log records) may remain in Facebooks database for technical reasons. When a user deletes their account, this material is disassociated from any personal identifiers.

Contact

- Preservation requests should be made through the Law Enforcement Online Request System ("the portal") at https://www.facebook.com/records Or by mail to the address above

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- Facebook may disclose limited amount of BSI on a case-by-case basis upon receipt of a direct request

Procedure

- A request will require:

  - A domestic order requiring production
  - Name of requesting authority (prosecuting agency, judicial authority or law enforcement agency)
  - Official email address (i.e. not a google or yahoo address)
  - Direct contact telephone number

- The Requesting State must pass Facebook's assessments regarding rule of law, human rights, surveillance, and privacy protections
- Users must have a touchpoint within the jurisdiction making the request
- If the user does not have a touchpoint within the jurisdiction, Facebook may inform the Requesting State with which States the user does have a touchpoint and whether the user is not in the same State as the requestor

Contact

 Requests should be made through the Law Enforcement Online Request System ("the portal") at https://www.facebook.com/records (preferred method)

DISCLOSURE BY CONSENT

- Facebook will not provide any electronic evidence through consent of the user
- If a law enforcement officer is seeking information about a Facebook user who has provided consent to access or obtain the user's account, the user should be directed to obtain that information from their own account by downloading it

- For more information on what type of data is available for download see: https://www.facebook.com/help/405183566203254?helpref=page_content
- For account content, such as messages, photos, videos and wall posts, users can access Facebook's '*Download Your Information*' feature from their account settings. See http://www.facebook.com/help/?page=18830 for guidance.
- Users can also view recent IP addresses in their Account Settings under Security Settings/Active Sessions
- **IMPORTANT NOTE:** Users do not have access to historical IP information and this should be obtained through an MLAR
- **IMPORTANT NOTE:** Please be aware that any download will be sent to the user's email account used for registration. A user could delete before law enforcement review or interfere with it. Further, law enforcement officers should check that all relevant information is contained in the download

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- All subscriber information in respect of the accounts, including, but not limited to, names, addresses, dates of birth, contact details and any other personal information supplied by the subscriber such as the means and source of payment for any service.
- Any other information held by Facebook which might identify the subscriber
- All user connection information, including session times and durations and IP addresses assigned during the relevant period
- All other account and IP logging information recording account usage from XX to XX including e-mail and IP addresses of others with whom the account has corresponded, services utilised and material accessed via the account.
- All contact lists, address lists, buddy lists or other such data associated with the account
- Any opened or unopened communications and the content of other stored files including photographs and video files
- The Facebook wall history
- All wall postings
- Details of all deleted wall postings or deleted video postings on the account
- All private communications and messages sent or received
- Any deleted messages sent or received

For **Instagram**:

- Subscriber name, phone number, account creation date, email address and signup IP address
- Photographs, photo captions and other electronic communications
- Stored contents of any account, which may include messages, photos, comments and location information

Google is a multinational technology company specializing in internet-related services and products, headquartered in Menlo Park, California – U.S. law applies

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Google will respond to emergency requests 24/7
- Any information provided in response to the request is limited to what Google believe would help prevent the harm
- A Request should include:
  - A cover letter signed letter served by e-mail on law enforcement letter head
  - Email address from a law enforcement domain – so must not be from a google or yahoo email account etc.
  - A detailed explanation of the nature of the emergency and how it poses an imminent threat to human life
  - Type of data being requested (to identify or locate individual)
  - Specific Google Identifier
  - URL or Google account (e.g. site where threat was made)
  - Explanation on how data requested will assist in addressing the emergency

Contact

- Submit the Google form to EDRLawEnforcement@google.com, or by fax +1-650-469-0276 with a cover letter on agency letterhead. If submitting outside normal business hours[38], call +1-650-417-9011 and leave a message informing that an emergency request has been submitted
- Use the Google form at **Annex F**i

PRESERVATION REQUESTS

Procedure

- Google require a signed letter served by e-mail on law enforcement letter head

38. Normal business hours are 9:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday. Faxes and emails are only reviewed during normal business hours

- Any request must include:

  - Email address from a law enforcement domain (i.e. not a Yahoo!, Google, etc. address) and direct contact phone number;
  - Indicate target account
  - Specify information to be preserved

- Google will tell law enforcement whether an account identifier is a valid identifier (but will not provide information regarding the account holder or account without legal process)
- Preservation period: 1 year (with possibility of extension), if it is indicated that MLA process is being pursued (otherwise default period is 90 days with possibility of extension)

 Use SUR at **Annex F**

Contact
Email to: lis-global@google.com

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- If the user does not have a touchpoint with the Requesting State, Google will only inform law enforcement with which States the user does have a touchpoint
- Google will only provide the IP addresses that resolve to the jurisdiction requesting
- If Google believes freedom of speech protections are implicated, they may not honour the direct request for voluntary disclosure
- Google will provide a certificate of authenticity if requested
- Google will specifically provide the following upon receipt of a request:
- *Gmail:*

  - Subscriber registration information (e.g., name, account creation information, associated email addresses, phone number)
  - Sign-in IP addresses and associated time stamps
  - Non-content information (such as non-content email header information - the to and from, time sent and IP, with the subject line removed)

- *YouTube:*

  - Subscriber registration information
  - Sign-in IP addresses and associated time stamps
  - Video upload IP address and associated time stamp

- *Google Voice:*

  - Subscriber registration information
  - Sign-up IP address and associated time stamp
  - Telephone connection records

  - Billing information
  - Forwarding number

- *Blogger*

  - Blog registration page
  - Blog owner subscriber information
  - IP address and associated time stamp related to a specified blog post
  - IP address and associated time stamp related to a specified post comment

Procedure

- On a voluntary basis, Google may provide BSI data in response to valid legal process from non-U.S. government agencies, if those requests are consistent with international norms, U.S. law, Google's policies and the law of the Requesting State
- In cases where Google honours legal process issued directly from the non-U.S. law enforcement agency, the information disclosed could include, for example, Google or YouTube account registration information (name, account creation information and associated email addresses) and recent sign-in IP addresses and associated timestamps
- A request will require:

  - A domestic order requiring production
  - Name of requesting authority (prosecuting agency, judicial authority or law enforcement agency)
  - Official email address (i.e. not a google or yahoo address)
  - Direct contact telephone number

 Use the Model form at Annex E

Contact

Email to: lis-global@google.com

DISCLOSURE BY CONSENT

- Google will liaise with immediate family members and representatives and may provide content from a deceased user's account after a careful review.
- Google will not provide passwords or other login details
- If a law enforcement officer is seeking information from a user who has provided consent to access or obtain the user's account, the user should be directed to obtain that information from their own account either using:
  - Google Takeout allows users of Google products, such as YouTube and Gmail, to export their data to a downloadable ZIP file. However, this does not include search history or Google Wallet information (the latter data is stored in the UK and will require an MLAR); or
  - For Google Enterprise a tool is available to download all data

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Data outlined above if not obtained voluntarily
- All stored electronic communications and other files reflecting communications to or from the requested account.

- All records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with the requested account including, without limitation, subscriber names, user names, screen names or other identities, mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information, telephone numbers or other subscriber number or identity, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form; and
- All connection logs and records of user activity for the requested account, including:

  – Connection date and time
  – Disconnect date and time;
  – Method of connection (e.g., telnet, ftp, http);
  – User name associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
  – Telephone caller identification records; and
  – Connection information for other computers to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, the identities (account and screen names) and subscriber information, if known, for any person or entity to which such connection information relates, and all other information related to the connection from another SP or its subsidiaries.

- The contents held in the above account/s including:

  – All electronic communications (including email text, attachments and embedded files) in electronic storage by Google, or held by Google as a remote computing service, within the meaning of the Stored Communications Act;
  – All photos, files, data or information in whatever form and by whatever means they have been created and stored
  – Any other records and other evidence relating to the requested account. Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with or relating to postings, communications and any other activities to or through the requested account, whether such records or other evidence are in electronic or other form.

- For YouTube accounts:

  – The subscriber details provided by the YouTube user including any email/postal addresses, full name, profile picture and telephone number or other contact method (where available)
  – The IP login history including creation IP for the account
  – Any login geo-location data held by Google for the user of account
  – Any videos posted by the user of account on to YouTube
  – Comments posted by the user of account
  – Private messages held in the inbox of YouTube user

JustPaste.it is a social media website for sharing text and images online. The site allows users to paste text (including HTML) markup for formatting and display of images and distribute the resulting link. Based at Wise Web, Leszczynskiego 4 lo29, 50-078 Wrocław, Poland – the Polish Telecommunications Act applies

EMERGENCY DISCLOSURE REQUESTS

Procedure

- All emergency requests from a Requesting State need to go through the Polish Police.
- The Polish Police will make the relevant enquiries and can share police-to-police with the Requesting State

Use SUR at **Annex F**

Contact

Email Mr. Mariusz Żurawek (Founder) at: justpaste@protonmail.com

PRESERVATION REQUESTS

Procedure

- Send reservation requests by email on law enforcement headed paper
- No policy on notification to users – so confirm users should not be notified in any request
- Provide information about the type of crime committed

Use SUR at **Annex F**

Contact

Email Mr. Mariusz Żurawek (Founder) at: justpaste@protonmail.com

VOLUNTARY DISCLOSURE

Not available

Kik Messenger, commonly called Kik, is a freeware instant messaging mobile application that uses a smartphone's data plan or WiFi to transmit and receive messages, photos, videos, sketches, mobile webpages, and other content after users register a username. Kik is known for its features preserving users' anonymity, such as allowing users to register without providing a telephone number. The application logs user IP addresses which the company can use to determine location – Canadian law applies

LE Guidelines https://lawenforcement.kik.com/hc/en-us/articles/203419779-Download-our-Guide-for-Law-Enforcement

EMERGENCY DISCLOSURE REQUESTS

Procedure

- For emergency cases involving the imminent threat of death or serious physical injury to any person, Kik have established an Emergency Disclosure Request process to allow the release of limited basic subscriber data.
- Kik's Emergency Disclosure Request form, (along with instructions for completing and submitting the form correctly) can be downloaded from their Resource Center at: http://kik.com/lawenforcement
- Once Kik receive the completed form, they will review and acknowledge receipt of the Emergency Disclosure Request.
- If the investigation meets Kik's emergency criteria, they will provide the investigating officer with a Glossary of Terms along with the data response if there's data available.

Contact

- To ensure quick processing of an Emergency Disclosure Request, submit the request to lawenforcement@kik.com using the email subject line "EMERGENCY DISCLOSURE REQUEST".

PRESERVATION REQUESTS

Procedure

- Kik have a specific request form to complete for preservation
- Kik will preserve for an initial 90 days and a further 90 upon a request for an extension – this extension should be sent one week before the original 90 days expires
- Complete a new Preservation Request form and tick the 'extension box'.
- If the preservation request expires, Kik can't confirm that data still exists in their system.
- If Kik receive a preservation request with an invalid username, or a request that doesn't include a Kik username, they will not be able to preserve any information. In that situation, Kik will notify the applicant and request an updated preservation request form with the correct information
- See pages 4 and 5 of the Kik law enforcement guidelines to confirm how to identify the Kik username - which is the only unique identifier in their system.

Contact

- Completed Preservation Request Forms can be emailed to the Trust & Safety team at lawenforcement@kik.com
- Include the words "Preservation Request" in the subject line
- Kik will review and acknowledge receipt

VOLUNTARY DISCLOSURE

Not available

LinkedIn is a business- and employment-oriented service that operates via websites and mobile applications. For U.S. users – U.S. law applies – for non-U.S. users Irish law applies.

LE Guidelines https://help.linkedin.com/ci/fattach/get/7890851/0/filename/Law_Enforcement_Guidelines_January%202018.pdf

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Emergency Requests for Member information must be made using the Emergency Disclosure Request Form available in the law enforcement guidelines
- Emergency Requests are only appropriate in cases involving serious bodily harm or death, and LinkedIn respond to such Requests only when they believe in good faith that such harm may imminently occur if they do not respond without delay
- The Emergency Disclosure Request Form must be submitted by a law enforcement officer and signed under penalty of perjury

Contact

- Serve the Emergency Disclosure Request Form by fax to: 353 (0)-1-633-5996

PRESERVATION REQUESTS

Procedure

- Preservation requests must:

  – Identify the account(s) at issue
  – Identify the investigating law enforcement agency and/or specific pending official proceedings (signed Requests on law enforcement letterhead preferred – include the following:

  - » Requesting Agency Name
  - » Requesting Agent Name
  - » Requesting Agent Badge/Identification Number
  - » Requesting Agent Employer-Issued E-mail Address
  - » Requesting Agent Phone Number (including extension)
  - » Requesting Agent Mailing Address (P.O. Box will not be accepted)

- Include assurances that the requesting agency or individual is taking steps to obtain appropriate legal process for access to the data that we are being asked to retain

 Use SUR at **Annex F**

Contact

- Serve the Preservation Request by fax to: 353 (0)-1-633-5996

VOLUNTARY DISCLOSURE

Not available

DISCLOSURE BY CONSENT

Not available

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Email address associated to user
- Member Identification number
- Date and time stamp of account creation
- Billing information
- IP logs (to include) the LinkedIn Member ID accessing the account; the source IP address; the date the account was accessed; the number of times the LinkedIn.com website was accessed by that account
- Snapshot of the Member Profile Page (to include) Profile Summary of:
  - Experience
  - Recommendations
  - Groups
  - Network update stream
  - User profile photo
- Member Content – including but not limited to
  - Direct messages, including any video, photo or document attachments
  - Invitations
  - Connections

Microsoft is a multinational technology company specializing in computer software and hardware, social networking and cloud computing, headquartered in Richmond, Seattle – U.S. law applies

CONTACT

Microsoft may have a local representative who handles submissions of legal demands in the regular course of business. Please contact globalcc@microsoft.com if the local contacts' information is not known. Inquiries must be in English.

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Microsoft does, in limited circumstances, disclose information to law enforcement agencies where they believe the disclosure is necessary to prevent an emergency involving danger of death or serious physical injury to a person.
- Those requests must be in writing on official letterhead in English and signed by a law enforcement agency
- The request must contain a summary of the emergency, specific data sought, along with an explanation of how the data sought will assist law enforcement in addressing the emergency.
- Each request is carefully evaluated by Microsoft's compliance team before any data is disclosed, and the disclosure is limited to the data that they believe would enable law enforcement to address the emergency
- Some of the most common emergency requests involve suicide threats and kidnappings. (Law Enforcement Requests Report https://www.microsoft.com/en-us/about/corporate-responsibility/lerr)

Use SUR at **Annex F**

Contact

Email to: lealert@microsoft.com

PRESERVATION

Procedure

- Microsoft require a signed letter served by e-mail on law enforcement letter head and from an email address from a law enforcement domain (i.e. not a Yahoo!, Outlook, Google, etc. address)
- Microsoft will preserve records initially for 180 days and maintain the preservation for 90-day periods thereafter as long as timely extensions are sought and Microsoft is told that an MLAR is to be sent
- Microsoft will not tell law enforcement whether an account identifier is valid

 Use SUR at **Annex F**

Contact

- The Microsoft Law Enforcement and National Security (LENS) Team assists law enforcement officers and prosecutors requesting information in terrorism-related investigations.
- Each on-boarded region has their own local country contact. Country contacts may be obtained by contacting via email: globalcc@microsoft.com
- A preservation request should be submitted through the local country contact or via email to: globalcc@microsoft.com

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- Microsoft Account Data:
  - Registration Details (Information captured at the time of account registration)
  - Billing Information - may include address and payment instrument(s)
  - IP Logs (IP addresses captured at the time of the user login to a specific service)
  - Services Utilized
- Email Service Data:
  - Registration Details (Information captured at the time of account registration)
  - IP Logs (IP addresses captured at the time of the user login to the email service)
- XBOX Service Data:
  - Registration Details (Information captured at the time of account registration)
  - Serial Number or Gamertag
  - IP Logs (IP addresses captured at the time of the user login to the XBOX service)
  - Gamertag Change History
  - XBOX Contacts
  - XBOX Online Game History
  - Stored Communications
- OneDrive Service Data:
  - Registration Details (Information captured at the time of account registration)
  - Stored Files
  - Transaction Logs

Procedure

- Specify the types of records, described above, in connection with an investigation - if the request does not adequately describe the records sought, it will be construed narrowly to ensure that Microsoft Corporation is not disclosing customer records that the requestor is not authorized to obtain

- Authorized to obtain pursuant to a domestic Legal Order in the Requesting State - that is attached to the Direct Request
- Legal Order must be addressed to: **Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 USA**
- Valid Identifier Types: All searches for responsive records will be conducted based upon the identifiers in the valid legal order. Identifiers limited to a maximum of 25 per request.

  – Email Address/Microsoft Account (MSA)
  – Phone Number
  – CID or PUID
  – Credit Card Number
  – XBOX Gamertag or Serial Number

- If there is a safety threat involved, indicate this in the request so prioritized
- The request must specify the '*nature of the crime*' being investigated
- Include government-issued email address, phone number, and postal address
- All records are dated and time-stamped individually. Please see notes on the page for time zones.
- Microsoft is not able to comply with informal requests, verbal requests or letter requests, even if placed on department letterhead. All requests for records must be submitted in the form of a subpoena or local equivalent

 Use Model Form at **Annex E**

Contact

- Each on-boarded region has their own local country contact. Country contacts may be obtained by contacting via email: globalcc@microsoft.com

DISCLOSURE BY CONSENT

- Online Tools for Users: Users may download the content and Traffic Data from their own accounts provided they have access to the account
- Consent on behalf of minors: The Law Enforcement and National Security (LENS) Team will assist law enforcement and prosecutors requesting information in terrorism-related investigations
- Consent by next of kin: Microsoft must first be formally served with a Legal Order from a Requesting States to consider whether it is able to lawfully release a deceased or incapacitated user's information regarding a personal email account (this includes email accounts with addresses that end in Outlook.com, Live.com, Hotmail.com, and MSN.com)
- Microsoft will respond to non-criminal subpoenas and court orders served on Microsoft's registered agent in the Requesting State or region and is unable to respond to faxed or mailed requests for such matters. Any decision to provide the contents of a personal email account will be made only after careful review and consideration of applicable laws

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Data outlined above if not obtained voluntarily
- Microsoft Account Data

  – Billing Transactions

- Email Service Data
  - Email Headers
  - Email Content
  - Email Contacts
- XBOX Service Data
  - Gamertag Change History
  - XBOX Contacts
  - XBOX Online Game History
  - Stored Communications
- OneDrive Service Data
  - Stored Files
  - Transaction Logs

Pinterest is an online tool for collecting, organizing and discovering interests – U.S. law applies

LE Guidelines https://help.pinterest.com/en/articles/law-enforcement-guidelines

EMERGENCY DISCLOSURE REQUESTS

Procedure

- In a situation where there is an emergency involving danger of death or serious physical injury, law enforcement can submit a request for disclosure of user information to Pinterest

Use SUR at **Annex F**

Contact

Email to: lawenforcement@pinterest.com

PRESERVATION REQUESTS

Procedure

- The Pinterest Law Enforcement Request Form must be sent to preserve electronic evidence

Contact

- The Law Enforcement Request Form can be submitted online

VOLUNTARY DISCLOSURE

Not available

DISCLOSURE BY CONSENT

Not available

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Pinterset profile – including
  - Name
  - Username
  - Location
  - Profile description
  - Website
  - Profile picture
  - Facebook or Twitter linked accounts
  - Likes
  - Saved Pins
  - Boards
  - Secret Boards
  - IP logs (to include) the Pinterest profile accessing the account; the source IP address; the date the account was accessed; the number of times the Pinterest website was accessed by that URL.

Signal is an encrypted communications application that uses the internet to send one-to-one messages, voice notes, files, images, videos and can make one-to-one calls and video calls – U.S. law applies

LE Guidelines Not Available

EMERGENCY DISCLOSURE REQUESTS

Procedure

- No specific procedure available
- It should be noted the only information Signal would be able to produce would be the date and time a user registered with Signal and the last date of a user's connectivity to the Signal service

Use SUR at **Annex F**

Contact

- No specific contact address for law enforcement

PRESERVATION REQUESTS

Procedure

- No specific preservation policies

Use SUR at **Annex F**

Contact

- No specific contact address for law enforcement

VOLUNTARY DISCLOSURE

Not available

DISCLOSURE BY CONSENT

Not available

Skype (owned by Microsoft and based in Luxembourg) specializes in providing video chat and voice calls between computers, tablets, mobile devices, the Xbox One console, and smartwatches via the Internet and to regular telephones – law of Luxembourg applies

CONTACT

Skype Communications SARL has established a Law Enforcement Relationship Management (LERM) Team to ensure the safe and responsible use of its communications platforms and to encourage legal prosecution of those responsible for misconduct on them. LERM handles all inbound requests from law enforcement for records concerning Skype users
Email: LERM@skype.net
Fax: +352 26 20 15 82

LE Guidelines Not Available

EMERGENCY DISCLOSURE REQUESTS

Procedure
In case of an EMERGENCY, where there is an immediate threat to life indicating '**Urgent Skype Request**' in the subject line the email. Microsoft will forward the request to Skype in Luxembourg for processing.
Requests must be submitted in English, French or German, or must also include a translation into one of these languages.

Use SUR at **Annex F**

Contact
Email to: LEALERT@microsoft.com

PRESERVATION REQUESTS

Procedure
- No specific preservation policies

Use SUR at **Annex F**

Contact
Email to: LEALERT@microsoft.com

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- Registration Details (Information captured at time of account registration)
- Billing Address (User-provided billing address)
- Payment Method/Instrument Data
- IP Logs (IP addresses captured at the time of the user login to the Skype service)
- Skype Number Service History (List of Skype Number(s) subscribed to by a user)
- Skype Out Records (Historical call detail records for calls placed to the public switched telephone network (PSTN)
- Skype Number Records (Historical call detail records for calls received from the public switched telephone network (PSTN)

Procedure

- In order to ensure an appropriate response to the Direct Request, the types of records, described above, sought for the investigation must be specified
- If the Direct Request does not adequately describe the records sought, it will be construed narrowly to ensure that Skype is not disclosing customer records that a requestor is not authorized to obtain
- A domestic Legal Order of the Requesting State must authorize disclosure and be attached
- Skype is not able to comply with informal requests, verbal requests or letter requests, even if placed on department letterhead. **All requests for Skype records must be submitted in the form of a valid Legal Order.**
- Skype LERM is only able to produce records based upon one of the following identifier types (**maximum of 25 identifiers per request**):

  - Skype username/ID
  - Skype Number accompanied by the specific date range
  - Dialed PSTN Number that is accompanied by the specific date, time, and duration of the call
  - 16-digit credit card number
  - Skype Order Number

- If there is a safety threat involved, indicate this in the subject line of the email so LERM can prioritize.
- The request must specify the '*nature of the crime*' being investigated.
- Include government-issued e-mail address, phone number, fax number and postal address.
- Include the International Country Code with any Skype Number or Dialled PSTN number requests


Use Model Form at **Annex E**

Contact

Email to: LERM@skype.net

DISCLOSURE BY CONSENT

Not available

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST (TO LUXEMBOURG)

IMPORTANT NOTE:

- The Skype system is designed in such a way that voicemail is not centrally stored
- Calls, instant messages and other activities between Skype users do not create billing records
- All records are dated and timestamped individually. Please see notes on the page for time zones

AVAILABLE ELECTRONIC EVIDENCE via MLAR to LUXEMBOURG

- Data outlined above if not obtained voluntarily
- Purchase History (Transactional records)
- SMS Records (SMS historical detail records)
- E-mail Records (Historical record of e-mail change activity)
- Skype username's Contact/Buddy List
- Skype username's Chat/Media content

Snapchat is an imaging and multimedia application – U.S. law applies

LE Guidelines https://www.snapchat.com/lawenforcement

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Snapchat will voluntarily disclose information when they believe in good faith that an emergency posing a threat of imminent death or serious bodily injury requires the immediate disclosure of this information
- The emergency disclosure form is in the Snapchat law enforcement guide

Contact

- During non-holiday business hours (Monday to Friday, 9am – 5pm Pacific Time), sworn law enforcement officials may request user records on an emergency basis by sending a completed Emergency Disclosure Request Form via email to lawenforcement@snapchat.com or by calling **310-684-3062**
- During non-business hours, sworn law enforcement officials may call **310-684-3062**

PRESERVATION REQUESTS

Procedure

- SnapChat retains logs for the last 31 days of Snaps sent and received, for 24 hours of posted stories, and for any unopened chats or those saved by a sender or recipient. The content is removed once all recipients have viewed it or 30 days after it was sent when unopened
- Upon receiving a signed and dated preservation request on law enforcement department letterhead, will attempt to preserve available account information associated with any properly identified Snapchat user(s) in an offline file for up to 90 days and will extend the preservation for one additional 90-day period with a formal extension request.
- SnapChat will not comply with preservation requests or multiple extension requests beyond one additional 90-day period

Use SUR at **Annex F**

Contact

Email to: lawenforcement@snapchat.com

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- Snapchat may produce documents if a Requested State provides a domestically obtained order to produce **BSI** or **Traffic Data**
- Snapchat retains logs of previous messages sent and received. The logs contain metadata about the messages, but not the content
- **IMPORTANT NOTE:** Snapchat only retain logs of the previous 31-days of Snaps
- Sample Language for **BSI:**
  - "Basic subscriber information for the Snapchat account associated with the username _____ consisting of the email address, phone number, account creation date and timestamps and IP address for account logins/logouts."
- Sample Language for Logs of Previous Snaps:
  - "Logs, including sender, recipient, date, and time, concerning the previous Snaps sent to or from the Snapchat account with the username _____."
- Voluntary disclosure will be accompanied by a signed Certificate of Authenticity

Use Model Form at **Annex E**

Procedure

Email to: lawenforcement@snapchat.com

DISCLOSURE BY CONSENT

Not available

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Data outlined above if not obtained voluntarily Snapchat Username
- Email address associated with account
- Phone Number associated with account
- Facebook account synced
- Log of the last 200 Snaps sent and received
- Snapchat account creation date
- Any unopened Snaps

Surespot is an open source instant messaging application using end-to-end encryption – U.S. law applies

LE Guidelines https://www.surespot.me/documents/surespot_law_enforcement_guidelines.html

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Surespot has law enforcement guidelines but no specific policies on emergency disclosure

Use SUR at **Annex F**

Contact

Email to: legal@surespot.me

PRESERVATION REQUESTS

Procedure

- No specific preservation policies

Use SUR at **Annex F**

Contact

- Surespot, llc. 2995 55th Street #18034 Boulder, CO 80308
  Or email request to: legal@surespot.me

VOLUNTARY DISCLOSURE

Not available

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Usernames
- Friend relationships
- Conversation relationships
- Messages in the amount of MAX_MESSAGES_PER_USER with server timestamp, to username, from username, and encrypted content, or link to encrypted content (image or file)
- Encrypted message file data (image or other) including rackspace cloud files
- Total messages sent per user
- Total images sent per user
- Current message count per user
- Signing (DSA) public keys and versions
- Encryption (DH) public keys and versions
- Encrypted '*friend images*' or avatars and friend aliases that are assigned to certain usernames
- Google GCM id
- Apple APN token
- If voice messaging has been purchased any purchase token from Google or Apple which is related to the username in the Surespot database
- Server logs

Tumblr is a media network that allows users to create, post, share, and follow digital media – U.S. law applies

LE Guidelines https://www.tumblr.com/docs/law_enforcement

EMERGENCY DISCLOSURE REQUESTS

Procedure

- If Tumblr have data necessary to prevent death or serious physical injury to any person, law enforcement should submit an emergency disclosure request with the subject line EMERGENCY DISCLOSURE REQUEST
- Such requests should include all of the following:
- Identity of the individual in danger of death or serious physical injury
- Nature of the emergency

- Tumblr username/URL of the individual (e.g., http://staff.tumblr.com) of the account(s) containing information necessary to prevent the emergency
- Links to any specific posts containing relevant information
- The specific information requested and why that information is necessary to prevent the emergency
- Any other relevant details or context regarding the particular circumstances

 Use SUR at **Annex F**

Contact
Email to lawenforcement@tumblr.com

PRESERVATION REQUESTS

Procedure

- Tumblr will preserve account records, to the extent they are available, for 90 days upon receipt of a valid preservation request issued in accordance with applicable law

 Use SUR at **Annex F**

Contact
Email to: lawenforcement@tumblr.com

VOLUNTARY DISCLOSURE

- No specific policy for voluntary disclosure

DISCLOSURE BY CONSENT

- No specific policy for disclosure by consent
- Electronic Evidence available for a Mutual Legal Assistance Request
- Stored contents
- Blog posts
- Likes
- Reblogs
- All user profile information
- Length of service
- Registered email address(es)
- IP logins

Twitter is an online news and social networking service where users post and interact with messages called "tweets". Headquartered in San Francisco, California – U.S. Law applies

LE Guidelines https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Twitter evaluates emergency disclosure requests on a case-by-case basis
- If Twitter receives information that provides them with a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, Twitter may provide information necessary to prevent that harm, if they have it
- Twitter will generally only provide **BSI** in response to emergency disclosure requests and requests for contents of communications (e.g., Tweets, DMs, Periscope broadcasts) must be made by MLAR
- Twitter will not notify users of a law enforcement requests in emergencies regarding imminent threat to life; child sexual exploitation or terrorism
- A request should include:

  - An official email address (e.g. not a yahoo, google etc. account)
  - Twitter @username or public user identification number (UID) and/or Periscope @username of the subject account(s) whose data is necessary to prevent the emergency
  - Specific URLs to the content at issue[39]
  - Nature of the emergency
  - Type of account data being sought
  - Explanation why this information is necessary to prevent emergency
  - Additional information or context regarding the situation - any attachments that can be helpful for Twitter to evaluate the emergency

Contact

- Law enforcement officers can submit emergency disclosure requests, through Twitter's Legal Request Submissions site: https://legalrequests.twitter.com
- In case of time-sensitive or urgent requests, submit information via the Submissions Site and then reach out via: https://help.twitter.com/forms/lawenforcement
- Also consider a request for content to be withheld through the web form: https://support.twitter.com/forms/lawenforcement

39. Learn how to find the URL to an individual Tweet at: https://help.twitter.com/en/using-twitter/tweet-and-moment-url

PRESERVATION REQUESTS

Procedure

- Twitter accepts requests from law enforcement to preserve records, which constitute potentially relevant evidence in legal proceedings
- A request must include:

  - Internal reference number, if any;
  - Twitter @username or public user identification number (UID) and/or Periscope @username of the subject account(s)
  - Information types that are to be preserved;
  - Time frame for which preserved information is being requested

- Twitter will preserve a temporary snapshot of the relevant account records for 90 days pending service of valid legal process
- If more time is required to obtain a court order or other process, a law enforcement officer must submit a preservation extension request prior to the expiration of the 90 days. The officer will receive a reminder by email few days before expiration.
- Twitter may honor requests for extensions of preservation requests but encourages law enforcement agencies to seek records through the appropriate channels in a timely manner, as Twitter cannot guarantee that requested information will be available

Contact

Through its Legal Request Submissions Site: https://legalrequests.twitter.com

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- Under certain circumstances, Twitter may provide voluntary disclosure on a case-by-case basis where appropriate local legal process has been issued in the Requesting State
- When submitting requests through the submission site, the request should include all of the following:

  - Name of the requesting law enforcement agency
  - Name and title of the requesting law enforcement officer
  - Any law enforcement reference number
  - The local law(s) violated (e.g., violent or other serious crimes)
  - User account(s) at issue (e.g., https://twitter.com/twittersafety (@twittersafety) and/or Periscope account (Periscope username and URL (e.g., @twittersafety and https://periscope.tv/twittersafety) - To locate a Twitter UID or Periscope ID, see the Twitter Guidelines for Law Enforcement: https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support
  - Tweet(s) at issue
  - Relevant dates of the tweets
  - Domestic order or legal process for disclosure of the relevant tweets

- Twitter's policy is to notify users of requests for their account information, which includes a copy of the request, prior to or after disclosure unless prohibited.

- If user notice is prohibited ('*non-disclosure request*') the basis for prohibition must be included – this can include terrorism investigations
- Twitter request that non-disclosure requests include a specific duration (e.g. 30 days) during which Twitter is prohibited from notifying the user

Procedure

- Requests should be submitted through the Twitter Legal Request Submissions site: https://legalrequests.twitter.com
- Via email to tw-le-requests@twitter.com (may result in a delayed response)

DISCLOSURE BY CONSENT

- Registered Twitter users can obtain a download of Tweets posted to his or her Twitter account
- Directions on how a user can request information is available from: https://support.twitter.com/articles/20170160
- Twitter does not currently offer users a self-serve method to obtain other, non-public information (e.g., IP logs or private messages) about their Twitter accounts
- If a Twitter user requires his or her non-public account information, they can send a request to Twitter via their privacy form, (see a copy at: https://support.twitter.com/forms/privacy), who will then respond with further instructions

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- Data outlined above if not obtained voluntarily
- Account information for each specified Twitter and/or Persiscope account as supplied on creation, including but not limited to date of inception, IP address information at account creation, any names, addresses, dates of birth and any email address/es used by the account holder(s), mobile phone number associated with a Twitter account, if provided by the user profile photo, header photo, background image, bio and status updates.
- For Periscope accounts - Twitter or Digits IP session logs that are associated with the Periscope account.
- Any log in information for all accounts including dates and times and most importantly IP addresses which have been used to access the accounts on each occasion.
- Details of any tweets from the above username sent to username [**insert username and URL**] including any pictures attached to the said tweets.
- Any created or shared videos
- Any uploaded, created or shared photographs

Uber

Uber is a technology company with a proprietary technology application (the "App") that provides on-demand lead generation and related services. The App connects independent providers of transportation services with requests from riders requesting transportation services. Drivers provide transportation services to riders through a ranger of offerings based on vehicle type and/or the number of riders. The Company has expanded the App to enable the transport and delivery of food and packages.

LE Guidelines for law enforcement outside of the U.S. https://www.uber.com/en-GH/legal/data-requests/guidelines-for-law-enforcement-outside-the-united-states/en/

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Where there is an emergency or exigency that involves protecting a rider, driver-partner, or third party who has been physically harmed, or stopping illegal activity that poses an immediate threat of physical harm, or in cases of verifiable time-sensitive investigations Uber will disclose relevant data
- Uber review these requests on a case-by-case basis and may provide data when they have a good faith belief that doing so may protect riders, driver-partners, others, Uber, or otherwise assist with an exigent investigation
- Once the emergency or exigency has passed, Uber require law enforcement to follow up with the appropriate legal process

Contact

- An Emergency Request Form (which can be requested through LERT@uber.com) is used for requests outside the U.S. that describes in detail the nature of the emergency or urgency, including details about the nature of the alleged actual or threatened physical harm or exigency, must be submitted
- For requests in the U.S. an Emergency Request can be submitted through the Law Enforcement Portal at https://lert.uber.com

PRESERVATION REQUESTS

Procedure

- Upon receipt of a formal written Uber will work to preserve records in connection with official criminal investigations for 90 days
- Law enforcement may extend a preservation request, once, for an additional 90 days
- Uber do not maintain preserved materials unless we receive an extension request or legal process

Use SUR at **Annex F**

Contact
Email to: LERT@uber.com

VOLUNTARY DISCLOSURE

Procedure

- Law Enforcement in the Netherlands:
  - Uber require Dutch authorities with supervisory and investigative powers to provide a warrant, court order or other legally binding order to compel the disclosure of a Dutch person's (personal) data
- Law Enforcement Outside the Netherlands or U.S.:
  - Law enforcement agencies may submit a request directly to Uber B.V. seeking a discretionary disclosure of data.
  - A Direct Request must:
    - » Relate to an investigation of a crime that is alleged to have occurred in the Requesting State
    - » Relate to an alleged criminal act that is an offence under the ordinary criminal laws in the Netherlands as well as the laws of the Requesting State
    - » Be narrowly tailored to a legitimate law enforcement need
    - » Be made using appropriate legal process for the jurisdiction in which the alleged crime occurred
- Uber reserves the right to decline to exercise its discretion to produce requested information even if each of the above threshold conditions are met and require the submission of an MLAR
- Circumstances under which Uber. will refuse to honour Direct Requests include, but are not limited to:
  - If the Direct Request is inconsistent with international human rights laws or standards or the rule of law,
  - Is being made to facilitate a prosecution that is political in nature or relates to the subject's race, religion, national origin, disability, sexual orientation, sex, marital status, gender identity, age
  - Other characteristic protected under Dutch law
- Form of Request
  - Clear grounds for the legal basis
  - Detailed specifics on the information sought and how this particular information may benefit the investigation. Uber will be unable to process overly broad or vague requests that do not identify the information sought with particularity
  - The name of the issuing authority, badge/ID number of the responsible agent or officer, an email address from a law-enforcement domain, and a direct contact number for the responsible agent or officer

Use Model Form at **Annex E**

Contact

- Authorized law enforcement using an official government domain may send legal process to LERT@uber.com
- Law enforcement may address requests to
  Uber B.V.,
  Mr. Treublaan 7,
  1097 DP Amsterdam,
  The Netherlands
  Attention: Law Enforcement Response Team

DISCLOSURE BY CONSENT

No specific policy for disclosure by consent

WhatsApp is a freeware and cross-platform instant messaging and voice over IP (VoIP) service, headquartered in Menlo Park, California – U.S. Law applies

LE Guidelines https://faq.whatsapp.com/en/android/26000050/?category=5245250

EMERGENCY DISCLOSURE REQUESTS

Procedure

- In responding to a matter involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay, a law enforcement official can submit a request via email using the emergency disclosure form
- For expedited processing of such requests, it is recommended to include the word '**EMERGENCY**' in the subject line of any message

Contact

Email to: records@records.whatsapp.com

PRESERVATION REQUESTS

Procedure

- WhatsApp will not store messages once they are delivered or store the traffic data of such delivered messages. Undelivered messages and the traffic data are deleted from their servers after 30 days
- Ask WhatsApp to preserve all data linked to a certain telephone number
- WhatsApp will confirm the preservation of records or will tell law enforcement that there is no WhatsApp account linked to the provided number
- WhatsApp will preserve account records requested in connection with official criminal investigations for 90 days - pending receipt of formal legal process
- A request must include:

  – A letter on law enforcement agency letter head signed and dated
  – Name of issuing authority, badge/ID number of responsible agent, direct contact phone number
  – Specific information needed (specify if content is needed, otherwise only BSI will be preserved)
  – WhatsApp account number and country code of identified target

Use SUR at **Annex F**

Contact

- Email to: records@records.whatsapp.com
- Or by mail to:
  WhatsApp Inc.
  1601 Willow Road
  Menlo Park, California 94025 United States of America
  Attention: WhatsApp Inc., Law Enforcement Response Team

VOLUNTARY DISCLOSURE

No data will be disclosed voluntarily

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- All subscriber information in respect of the account, including, but not limited to: names, addresses, dates of birth, contact details, date when registered, device used and port number, email used to register and any other personal information supplied by the subscriber
- Profile picture
- Address book of phone when registered
- Information about groups (name, size and icons)
- Any unsent messages stored on the WhatsApp server
- Date of last known use
- Date of last IP address
- Date of last used port number

Wickr Messenger is a free application that provides end-to-end encryption of text, picture, audio and video messages. Senders control who can read their messages and when they expire. Encrypted messages are stored on their servers and are deleted after they are downloaded to the recipient's device(s). Wickr do not have plaintext copies of messages exchanged through their system or the keys to decrypt user content – U.S. law applies

LE Guidelines https://www.wickr.com/legal-process-guidelines/

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Wickr may provide information to law enforcement in response to a valid emergency disclosure request
- Wickr will review emergency disclosure requests on a case-by-case basis and evaluate them under U.S. law
- If Wickr receive information that gives them a good-faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, they may provide information to law enforcement to prevent that harm, if they have it
- Emergency disclosure requests must be on law enforcement letterhead and include the relevant Wickr ID (user name) of the subject account(s) whose information is necessary to prevent the emergency


Use SUR at **Annex F**

Contact

Email to: legal@wickr.com

PRESERVATION REQUESTS

Procedure

- Upon receipt of a valid preservation request from law enforcement Wickr will temporarily preserve the relevant account records for 90 days pending service of legal process under U.S. Law
- Preservation requests should be on law enforcement letterhead, signed by the requesting official, and include a valid official email address


Use SUR at **Annex F**

Contact

Email to: legal@wickr.com

VOLUNTARY DISCLOSURE

Procedure

- Law enforcement or government requests for user information must include:
- Identifying information of the entity being investigated, such as User ID
- A description of information being sought
- The descriptions should be as narrow and specific as possible in order to avoid misinterpretation and/or objections for overly broad requests. Wickr will construe received requests narrowly to maintain users' privacy and ensure that any information disclosed does not exceed the scope of the request.
- Further, Wickr requires law enforcement and/or government agencies to include the following information so that requests for user information may be validated:

  - Requesting law enforcement/government agency
  - Requesting agent name and badge/ID number
  - Valid agency e-mail address and physical return address
  - Phone number of requesting agent, including extension when applicable
  - Response due date
  - A copy of the court order, warrant, or subpoena

Use Model Form at **Annex E**

Contact

- Wickr accepts service of court orders, search warrants, and subpoenas for information by email from law enforcement and government agencies, provided that these legal requests are sent from an official government email address of the requesting agent. Law enforcement and/or government agencies should submit legal requests directly from their official government email address to legal@wickr.com.
- While electronic service is preferred, process may also be served by mail or courier to:
- Wickr Inc.
  Attn: Legal Department
  20 California street
  #250
  San Francisco, CA 94111
- If opting for electronic service, there is no need to serve duplicate hardcopy process on Wickr to the address above

DISCLOSURE BY CONSENT

No specific policy for disclosure by consent

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- For Wickr Messenger:

  - Date an account was created
  - Type of device(s) on which such account was used
  - Date of last use

  - Total number of sent/received messages
  - Number of external ID's (email addresses and phone numbers) connected to the account, but not the plain-text external IDs themselves
  - Limited records of recent changes to account settings such as changes to privacy list mode to block or allow users (does not include message content or routing and delivery information)
  - Wickr version number

- For Wickr Pro:
  - Network affiliation
  - Wickr Pro ID (email address)
  - Phone number, if provided by network administrator as a second form of authentication
  - Date an account was created
  - Type of device(s) on which an account was used
  - Date of last use
  - Total number of sent/received messages
  - Limited records of recent changes to account settings (i.e. adding or removing a device; does not include message content or routing and delivery information)

- For network administrator accounts on Wickr Pro:

  - Network membership
  - Payment-related information
  - Network-wide settings including limited records of recent changes to network settings (i.e. enabling or disabling federation)

Yahoo! is a web service provider known for its search engine and other services that include Yahoo! Mail and Flickr, headquartered in Sunnyvale, California – U.S. law applies

LE Guidelines https://transparency.yahoo.com/law-enforcement- guidelines

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Yahoo! will review emergency disclosure requests on a case-by-case basis, and evaluate them under U.S. law, in instances where they have been provided sufficient information to conclude that disclosure without delay is necessary to prevent imminent danger of death or serious physical injury to any person

- All emergency disclosure requests should be submitted in writing using their Emergency Disclosure Form.
- Yahoo! will, in its sole discretion, determine whether the circumstances warrant disclosure, utilizing the information provided on the Emergency Disclosure Form.
- Yahoo! reserve the right to only share information that they believe is necessary to avert an emergency situation.

Contact

- Email to: legalpoc@yahoo-inc.com
- To speak to someone at Yahoo!, call **408-349-3687** and leave a message in the voicemail for the Compliance Team. Yahoo! will use its best efforts to return all calls during the same business day, or within 24 hours, depending on call volume

PRESERVATION REQUESTS

Procedure

- Yahoo! will preserve data based on a direct request by law enforcement
- Yahoo! will tell law enforcement whether an account identifier is a valid identifier (but will not provide information regarding the account holder or account without legal process)
- Yahoo! will evaluate and suggest next steps (i.e. MLAR or contact a different Yahoo entity) or alternatively inform law enforcement if an account does not exist
- There is no limit on the number of permissible preservation extensions for law enforcement, but the preservation must be renewed through an extension request every 90 days
- Preservations are automatically expunged once they expire (do not miss extension deadline!)
- Yahoo! provides a new Internal Reference Number for each preservation and extension
- When all accounts in a preservation request made by a law enforcement official belong to one country's terms of service (TOS), Yahoo! will inform the requestor where the data is held
- If preserved accounts fall under the TOS of different States, Yahoo! will not tell the requestor
- Yahoo! requires a letter signed on law enforcement headed paper served by email

 Use SUR at **Annex F**

Contact

- Where to send the preservation request will depend on where the account has been created:
- If created in Europe i.e.it will be YAHOO Europe (YAHOO EMEA) - ie-legalpoc@yahoo-inc.com
- If created outside of Europe, it will be YAHOO USA (YAHOO INC) legalpoc@yahoo-inc.com
- If in doubt, contact both and when notified by either YAHOO USA or YAHOO EUROPE the location of the data will be known

VOLUNTARY DISCLOSURE

Electronic evidence that could be disclosed

- On a voluntary basis, Yahoo may provide **BSI** in response to valid legal process from non-U.S. government agencies, if those requests are consistent with international norms, U.S. law, Yahoo's policies and the law of the Requesting State

Use Model Form at **Annex E**

Contact
Compliance Team
Yahoo! Inc.
701 First Avenue
Sunnyvale, California 94089
Phone: **408-349-3687**
Fax: **408-349-7941**

- The phone number listed can be used to leave a message in the voicemail for the Compliance Team. Yahoo! will use its best efforts to return all calls during the same business day, or within 24 hours

DISCLOSURE BY CONSENT

- In order for Yahoo! to turn over any information to law enforcement based on a user's consent to search, the user's signed consent must be accompanied by a Legal Order from the Requesting State, and Yahoo! must be able to successfully verify the account of the user whose information is being sought. Along with the user's signed consent and a detailed description of the information the user is requesting from Yahoo!, the user must provide the information requested in a Consent to Search Form to Yahoo! in writing. (Yahoo!'s Law Enforcement guide includes sample a consent form.) If the user is unable to verify ownership of the account by providing registration information that matches what is in Yahoo!'s records, Yahoo! will be unable to produce records pursuant to the user consent

ELECTRONIC EVIDENCE AVAILABLE FOR A MUTUAL LEGAL ASSISTANCE REQUEST

- All subscriber information in respect of the account, including, but not limited to:
  - names, addresses, dates of birth, contact details and any other personal information supplied by the subscriber such as the means and source of payment for any service.
  - IP addresses and port numbers associated with log-ins to a user account
- For Yahoo! Mail:
  - Any content of emails available in the user's mail account, including the IP address of the computer used to send the mail
  - Any attachments, photos and contact lists
  - Any draft emails
  - Any available deleted emails
- For Yahoo! Chat/Messenger:
  - Friends list
  - Time, date and IP address for Chats and Messenger use
  - Archives of messenger communications
  - Archives of web Messenger communications

- For Yahoo! Groups:
  - Members list, email addresses of Members and date when Members joined the Group
  - Information about Group Moderators
  - Contents of the files, attachments, photos and Messenger sections
  - Group activity log describing when Members subscribe and unsubscribe, post or date files and other relevant events
- Yahoo! Geocities, Domains, Web-hosting and Stores:
  - Active files user has uploaded to the website and date of file upload
  - Transactional data for stores
- Yahoo! Flickr:
  - Contents in Flickr account and comments on other user's photos
  - IP address and timestamp of content uploaded to account
  - Flickr Groups to which a user belongs and Group content
- Yahoo! Profiles:
  - Contents of a user's profile
  - Time, date and IP address logs of content added

Zello Inc. is a push-to-talk app for mobile devices and PCs that enables live conversations between individuals and groups from around the world via public/private channels of up to 3500, headquartered in Austin, Texas – U.S. Law applies

LE Guidelines Not available online, but there are plans to add an article in Zello's Support Knowledge Base.

Address
Zello Inc.
1317 W. 6th St, Austin TX, 78703, USA

EMERGENCY DISCLOSURE REQUESTS

Procedure

- Zello will disclose data on a voluntary basis when it has credible evidence of immediate risk to human life

Use Model Form at **Annex C**

Contact
Email to: subpoena@zello.com

PRESERVATION REQUESTS

Procedure

- A request must include:
  - A letter on law enforcement agency letter head signed and dated
  - Contact details of the requesting officer
  - The list of Zello usernames
  - Specific information needed to be preserved

Use Model Form at **Annex B**

Contact
Email to: subpoena@zello.com

VOLUNTARY DISCLOSURE

- Zello adheres to MLAT agreements between the U.S. and other countries and will cooperate with requests made through those agreements
- Under certain circumstances, depending on scope and urgency or risk to national security, Zello may provide evidence on a voluntary disclosure basis (without MLAT) on a case-by-case basis where appropriate local legal process has been issued in the Requesting State
- Zello will provide a supporting affidavit authenticating the voluntary disclosure.
- Zello currently does not notify users that a disclosure has been requested or is being made
- Electronic Evidence Available
- Zello does not require verified personal information (such as name, address, email, or phone number) for an account to be created
- Zello does not store user content (audio, images, texts) on its servers
- Zello can provide:
  - Account names
  - Account names of contacts
  - Channel names
  - Recently used IP addresses
  - Timestamps of activity

DISCLOSURE BY CONSENT

- Conversation between contacts and within channels, including audio, texts, and images, are stored on the user's device in 'History''. Some of it can be shared with other users or on social media
- Zello can provide a supporting affidavit authenticating the data provided by consent.

PART 5

MUTUAL LEGAL ASSISTANCE

This Part will assist with:

- MLAR for basic subscriber information
- MLAR for traffic data
- MLAR for content
- Real-time collection

IMPORTANT NOTE: The guidance in this Part is correct at the time of publication – it is incumbent on practitioners to ensure they are following the correct procedure by referring to the current Requested State's MLA Guidelines[40] and law

Introduction

1.1. If admissible electronic evidence cannot be obtained through non-MLA mechanisms as:

- Electronic evidence is unavailable through open source searches; or
- SPs do not disclose electronic evidence in response to a Direct Request for **Traffic Data** or **BSI**; or
- **Content Data** is required; or
- The data cannot be preserved and must be obtained quickly to prevent deletion; or
- Electronic evidence obtained by voluntary disclosure is inadequate to satisfy the Requesting State's requirements for admissibility of the electronic evidence
- **The next step is to initiate the MLA process that includes, among other things, drafting an MLAR.**

1.2. This Part explains:

- Principles of drafting MLARs for
  - **BSI**
  - **Traffic Data**
  - **Content Data**
  - Real-time collection
- Legal requirements for MLARs to the U.S., the location of the major SPs
- A case study applying the principles of drafting an MLAR for electronic evidence

1.3. See **Annex Bi** for a Model MLAR for stored **BSI**, **Traffic Data** or **Content Data** and **Annex Bii** for real-time collection of electronic evidence**.** A checklist for the drafting of an MLAR for electronic evidence and essential steps is included at **Annex C**

1.4. The law of the Requested State must be respected and, where necessary, prior authority obtained from the relevant Central or Competent Authority for any actions undertaken. Failure to comply with the requirements of domestic legislation or any applicable bilateral treaty or convention, could lead to delays securing the evidence in the Requesting State and a legal challenge in the Requested State to the process to obtain any evidence.

40. See Annex H for selected States with SPs

Drafting an MLAR for electronic evidence

Language

1.5. An MLAR is a formal legal document that must be easily understood and capable of execution by the Requested State. This means the Requested State must be given all the information it will need to decide whether assistance should be given and how to do so.

1.6. The language used should be formal and courteous. When used, acronyms, such as IP address, must always be spelt in full when referred to for the first time.

1.7. Whilst colloquialisms and jargon should generally be avoided, it is important to use the language of the type of evidence requested from the SP. For example, Snapchat messages should be referred to as '*snaps*'. The aim is to produce an easy to read document, which immediately conveys to the reader what is required, whilst providing the clarity needed for any court orders.

Urgency

1.8. Do not mark the MLAR as urgent unless this is REALLY the case. Do not impose a deadline for the receipt of electronic evidence unless it is a genuine deadline – this could include the end of pre-trial custody. There is a risk that once the deadline is reached the Requested State will stop all enquiries and archive the MLAR. If the Requested State believes the deadline is unrealistic at the outset, it is possible that no enquiries will be undertaken at all, because it is considered to be impossible to provide the electronic evidence for the requested purpose.

1.9. Where appropriate the MLAR should be marked as urgent and an explanation provided why the MLAR should be given priority above others. This could include the seriousness of the allegation in a terrorism or organized crime investigation/prosecution and that the electronic evidence is critical to the investigation/prosecution or to locate others in the network yet to be identified.

1.10. The MLAR drafter should review an applicable Mutual Legal Assistance Treaty (MLAT) to confirm if an urgent request can be transmitted directly to a Requested State's Central Authority (CA) and **not** through diplomatic channels – in order to save time. Also, confirm if the Requesting State can transmit the MLAR using a secure email to reduce delay.

IMPORTANT NOTE: Diplomatic channels should be used only if the use of quicker alternative channels violates domestic laws of a Requesting and/or Requested State

Legal basis

1.11. Some States require only a treaty basis for MLA, while others are able to assist in the absence of relevant treaties, on the basis of the principles of reciprocity or comity or based on their domestic law.

1.12. If a Requested State requires a treaty basis for MLA, an MLAR for electronic evidence can be based on bilateral and\or multilateral (i.e. regional, sub-regional and global) treaties as in the cases regarding MLARs for traditional evidence.

1.13. Some of the treaties relate specifically to MLA in criminal matters, others focus on combatting certain offences and generally include provisions on MLA. Even though most of the treaties do not refer specifically to electronic evidence, they can serve as a legal basis for MLA for electronic evidence because of the types of MLA they generally include. For example, according to Article 18 of the UN Convention against Transnational Organised Crime (UNTOC), types of MLA that can be requested include, among others, "*taking evidence…*", "*providing evidentiary items…*", "*executing searches and seizures…*", and "*other type of assistance not contrary to the domestic law of the requested State*".

1.14. The following instruments and arrangements refer specifically to international cooperation and electronic evidence or cybercrime:

- The Council of Europe Convention on Cybercrime, 2001, also known as the Budapest Convention, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
- The African Union Convention on Cybersecurity and Personal Data Protection, 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
- The Arab Convention on Combating Information Technology Offences, 2010, http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences

1.15. Other regional and sub-regional treaties and arrangements regarding MLA in criminal matters were concluded and made under auspices of various regional organisations and structures including the African Union, the Cooperation Council for the Arab States of the Gulf, CoE, and the European Union.[41] Whilst these instruments do not refer specifically to electronic evidence they may serve as a legal basis for MLAR for electronic evidence as mentioned above. These instruments, as well as regional and sub-regional treaties and arrangements against terrorism, are listed in Annexes VI and IV of the UNODC Manual on International Cooperation in Criminal Matters related to Terrorism http://www.unodc.org/documents/terrorism/Publications/Manual_Int_Coop_Criminal_Matters/English.pdf

1.16. If a Requested and Requesting States are not parties to regional instruments, the MLAR can be based on global treaties. In particular, the universal legal framework against terrorism consists of

41. Information regarding the EU MS and Agencies judicial cooperation with third countries could be found in **ANNEX I.**
Within the European Union's Directive 2014/41/EU introduced the European Investigation Order (EIO) as the formal means by which Member States of the European Union can request evidence from other Member States, including electronic evidence, without an MLAR

19 conventions and protocols against terrorism (http://www.un.org/en/counterterrorism/legal-instruments.shtmland) and relevant United Nations Security Council Resolutions https://www.un.org/counterterrorism/ctitf/en/resolutions

1.17.  Under the Security Council Resolutions 1373 (2001), 2178 (2014) and 2322 (2016), 2396 (2017) States are required to afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence. The resolutions call upon the States to use applicable international instruments as a basis for MLA and in the absence of applicable instruments, to cooperate when possible on the basis of reciprocity or on a case by case basis. Resolution 2322 (2016), among other things, calls upon States to review and update existing laws on MLA in view of the substantial increase in volume of requests for electronic evidence. These Resolutions are binding as they were adopted under Chapter VII of the Charter of the United Nations, including for States that have not ratified all or some of the universal instruments. These resolutions are available at: http://www.un.org/en/sc/documents/resolutions/

1.18.  Not all 19 universal conventions and protocols against terrorism can serve as a legal basis for MLA. For a summary of the relevant articles of these instruments that are the basis for MLA, see annex V of the UNODC Manual on International Cooperation in Criminal Matters related to Terrorism: http://www.unodc.org/documents/terrorism/Publications/Manual_Int_Coop_Criminal_Matters/English.pdf

1.19.  Other global instruments, in particular, the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, (http://www.unodc.org/unodc/en/treaties/illicit-trafficking.html), the United Nations Convention against Transnational Organized Crime (https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html) and the United Nations Convention against Corruption (www.unodc.org/unodc/en/treaties/CAC/index.html) may also serve as a legal basis for MLA for electronic evidence. These conventions contain detailed provisions concerning MLA, to the extent that they are often referred to as '*mini-treaties on mutual legal assistance*'.

PRACTICAL NOTE

Early contact should be made with the Central Authority to establish a rapport and a line of communication to ensure all requirements of the Requested State are satisfied as far as possible. This can be essential to ensure the timely execution of an MLAR for electronic evidence.

Purpose of the request

1.20. The author of the MLAR should, at the outset of the MLAR, briefly note, or summarise, the following information:

- Subjects – as much detail as possible of each suspect / accused in the case, this can include full name, date and place of birth, nationality, address and passport number; also note the stage of the investigation or proceedings **IMPORTANT NOTE: Often the purpose of an MLAR is to identify the subject – in this situation include what is known to assist with identification - for example username or IP address**
- Note the electronic evidence or investigative method required in the MLAR and if any electronic evidence has already been obtained through alternatives to MLA (e.g. through a Direct Request to the SP)

The relevant law

1.21. In this section, a summary of the relevant law should be noted, i.e. the offences under investigation /prosecution. If a description of the law is unavoidably lengthy, place it in an annex. Always be aware that MLARs place an increased burden on Central and Competent Authorities who will already have a substantial workload. The more concise the body of the MLAR, the more likely that it will be considered quickly.

1.22. Some States may only be able to assist if dual criminality is found; another relevant consideration may be the penalty that can be imposed – use UNODC Sherloc or the UNODC Cybercrime Repository to research relevant offences.

Summary of facts

1.23. A summary only is required, not a lengthy recitation of all the details. Remember that the MLAR is a stand-alone document and the Requested State will have no other information on the matter. Facts are required that are relevant to identifying what the electronic evidence requested is, why it is necessary to the Requesting State and which are capable of satisfying the legal standard and any other legal requirements of the Requested State. The summary of facts should be set out clearly, concisely and accurately.

1.24. Ideally, the facts should demonstrate a prima facie case that each named accused has committed the identified criminal offences, or that a criminal offence has been committed (where suspects still to be identified). This may include for terrorism investigations/prosecutions, confirmation that a terrorist organisation is proscribed or designated. This can be established through domestic legislation, Consolidated UN Security Council Sanctions List UN or the EU Terrorist List.

1.25.  Further, the MLAR must provide sufficient supporting information to persuade and enable the Requesting State to take steps to legally compel the SP to provide the required electronic evidence. This means the MLAR drafter must review the legal standards of the Requested State to know what supporting information must be included - the Council of Europe website as well as the UNODC Cybercrime Repository and UNODC Sherloc (including its under-development resource on electronic evidence has relevant legislation from States around the world).

1.26. As most of the major SPs are U.S. based (Apple, Google, Microsoft, Facebook, Yahoo, Twitter, Ebay), a detailed knowledge of U.S. law and the procedures required to produce electronic evidence will enhance collection for counter-terrorism and organized crime investigations/prosecutions. Namely, that there should be evidence presented to connect the accounts to the criminal activity being investigated. Dates should also be included to show the dates of the crimes and the dates on which the accounts were used. This is critical information that is needed to execute an MLAR in the U.S.

1.27. Below is a summary of the requirements to include in an MLAR in the U.S. for stored electronic evidence and real-time collection of **Traffic Data**:

Basic subscriber information – U.S. MLAR

Legal standard

- In order to obtain **BSI**, it must be established that the evidence sought is **relevant** and **related** to the criminal investigation. It is not enough to show that the suspect or defendant had an email account or social media account; the account must have something to do with the crime being investigated. This is the lowest legal standard required of all investigative processes.

PRACTICAL NOTE

IP addresses frequently change, it is therefore important to always include the precise time – up to the second if available – as well as the time zone (e.g. Central European Time "CET") when asking for IP address information.

Traffic data – U.S. MLAR

Legal Standard

- In order to obtain most types of **Traffic Data**, **specific** facts detailing how the records or other information sought are **relevant and material to a criminal investigation**, must be provided. This is because U.S. law requires prosecutors to provide the court with a factual summary of the investigation and how the records requested will advance that investigation. This is an intermediate standard, higher than mere relevance, but not as a high a legal burden as "*probable cause*" for content. The court order is referred to as a d-order and named after section 2703**(d)** of the Electronic Communications Privacy Act (ECPA)

PRACTICAL NOTE

If the supporting and relevant facts are insufficient to prove a higher standard of proof for content – request **Traffic Data**. This could demonstrate contact between subjects at the time of the offence. Time can be wasted if an MLAR is sent for content that does not meet the required standard or proof. An incremental approach and requesting **Traffic Data** in the first instance can be useful to build the required legal standard for **Content Data**.

Content – U.S. MLAR

1.28. Each device or each account from which **Content Data** is needed is considered, as a separate place just like a house and for each, the judicial authority will apply a separate reasoning, account by account, device by device. This means the supporting grounds in the MLAR, must be set out account by account or device by device and a rationale for each applying the required legal standard.

Legal Standard

- The MLAR must provide **specific** facts supporting the belief that the evidence (content) sought will be found among the records of the SP, and that the evidence relates to a crime this is **probable cause**. This is the same standard that applies to the search of a house or a business in the U.S. The MLAR must provide sufficient detail describing:

  – The type of **Content Data** to be seized (e.g., an email communication)
  – The reason why the **Content Data** relates to the criminal offence being investigated
  – Only include those facts that are relevant to the evidence required and **always** confirm the source of the information in the MLAR

- The attribution of the account to the suspect: Use what is already available in the matter: e.g. suspect is using this Gmail account on basis of witness account **OR** the direct request to Facebook for **BSI** shows the suspect opened this Facebook account with the email address whose content is requested
- If the content is linked to a device - the exact identification of the device from which content is sought: E.g.:

  - Named suspect used iPhone 5 model xxxx
  - IMEI xxxx corresponding to
  - Phone number xxx
  - Subscriber of xxxxx account (if obtained through a direct request)

- Do not use sentences such as "*the investigations show*"; "*it seems that*" but detail what investigations? When? How the evidence shows this to be the case
- Link the person to the crime: is he the author? What facts support this?

PRACTICAL NOTE

Only include facts that support the conclusion that email content will contain evidence of the offence under investigation. The summary of facts in the MLAR must be relevant to the required assistance and **not** a summary of the complete investigation. Typical questions from the U.S. Central Authority are "*how do you know?*" "*When and how did you find this information?*" Considering these questions when drafting can save time executing the MLAR.

Do the facts meet Probable Cause?

1.29. This depends on the supporting facts in the case and ensuring a link to the criminality and evidence requested. Sometimes the supporting facts are insufficient to reach the probable cause standard. It is then advisable to draft an MLAR for **BSI** or **Traffic Data** in the first instance. This approach ensures an incremental building of the reasoning necessary to obtain content or a decision is made that there are insufficient supporting facts to request content.

1.30. For example, in a counter-terrorism case, an MLAR for **Traffic Data** (d-order) of the author's email can show before the attack or immediately after he used his email account to contact another individual. Due to the proximity to the attack, it is possible to show sufficient probable cause that the content of that communication speaks or is related to the crime and therefore can be presented to a judge for a search warrant of that communication.

IMPORTANT NOTE: Do not forget to update an MLAR after it has been transmitted to a Requested State by providing an amended MLAR or additional information to the Requested State. Too often, investigators send MLARs and wait for them to be executed without being proactive. Any new discovery in the investigation after the MLAR has been sent can help expedite its execution or reaching the legal standard of the Requested State; for instance, a recent interview revealing information about the suspect. Any additional supporting facts should, in the case of the U.S. be sent by email to the Central Authority – the U.S. Department of Justice's Office of International Affairs

1.31. "Current" or "fresh" information is the second requirement for obtaining the content of electronic communications. This means that at least some of the facts upon which the MLAR is based need to be relatively recent or indicate the likelihood that the evidence will still be located in the place to be searched. Courts will reject a request if the information presented is old or "*stale*." While this is somewhat case-specific (and while not a hard and fast rule), facts that are more than 60 – 180 days old, in the context of electronic evidence, are more likely to be considered *stale*. Equally, if an account has been inactive, the contents may have been deleted by the SP. To ensure time isn't wasted sending an MLAR, before preserving, an investigator should confirm if a SP has a policy of data removal if an account is inactive for certain periods.

1.32. Reliable information must be at the base of the reasoning. In U.S. law, all the evidence that is used in the proceedings but be reliable, i.e. coming from an authentic and verifiable source to which a high degree of credibility can be attributed. The knowledge of a fact by an investigator is not in itself sufficient and must be explained: *how did I get this knowledge?*

1.33. The supporting information in an MLAR need not be in a form that would be admissible at trial. However, the circumstances in an MLAR, viewed as a whole, should demonstrate the reliability of the information. In general, when deciding whether to issue a search warrant, a U.S. judge or magistrate will likely consider information in an affidavit reliable if it comes from any of these sources:

- A confidential police informant whose past reliability has been established or who has first-hand knowledge of illegal goings-on
- An informant who implicates himself or herself as well as the subject
- An informant whose information appears to be correct after at least partial verification by the police
- A victim of a crime related to the search
- A witness to the crime related to the search, or
- Another law enforcement officer

CASE STUDY

A terrorist murdered two police officers in their home. The terrorist had two Facebook accounts linked to an iPhone seized at the crime scene: One in his own name and another using an alias where he posted a video of the double murder and claimed the attack. The Requesting State transmitted an MLAR for Content Data for both Facebook accounts. The U.S. Central Authority advised probable cause was only met for the alias account due to the posting of the video of the murder and not the personal account. The alias account had a direct link to the criminality, whilst the personal account had no such link.

Freedom of Expression

1.34. A request for assistance may be declined if the conduct in question is protected under domestic laws of the Requested State as a breach of basic human rights, as recognized by that Requested State. For example, with respect to online propaganda by terrorists or their sympathizers, there may be a distinction between communications that incite acts of terrorism, which ought be criminalized in accordance with international law, and communications which are considered to be a legitimate exercise of the right to freedom of expression as well as other rights including the rights to freedom of thoughts, conscience and religion, belief and opinion.

1.35. For example, the U.S. Department of Justice Investigative Guide for Obtaining Electronic Evidence from the United States of 2012, states:

> "… *the U. S. would deny a request for assistance if it relates to an individual engaging in expression (written, spoken or other) that falls under the U.S. Constitution's protection of free expression (e.g., "hate" speech is generally protected by the Constitution, even though objectionable), unless facts are provided that indicate expression goes beyond permissible, protected speech (e.g., hate speech that includes calls for immediate, violent action). Because not all expression is protected by the U.S. Constitution, please consult with U.S. authorities to verify whether or not assistance can be offered in a particular case.*"

1.36. Given that various countries have strong protection of the basic human rights, it is advisable, when in doubt, always to consult with the relevant authority of the Requested State with regard to the conduct at issue.

1.37.  Information relevant to considering the distinction between the criminal offence of incitement of acts of terrorism and the right to freedom of expression is available in the following resources of the United Nations:

- UNODC, The Module on Human Rights and Criminal Justice Responses to Terrorism of the Counter Terrorism Legal Training Curriculum, 2014, Section 2.3

- UN OHCHR, "Human Rights, Terrorism and Counter-terrorism", Fact Sheet No. 32, 2008, Chapter III, Section H

PRACTICAL NOTE

SPCs should contact +1 202-514-0000 should they wish to obtain the contact information for the U.S. Central Authority Cyber Team attorney handling cases from that country in order to discuss any issues including Freedom of Speech.

Real-time collection of Traffic Data – U.S. MLAR

IMPORTANT NOTE: This technique can be both time-consuming and costly, and Requesting States should give careful consideration to whether the material sought can be obtained pursuant to a different form of assistance, and whether this real-time traffic collection is truly necessary for the investigation at hand.

Legal Standard

1.38. In order to obtain non-content information in real-time, the MLAR would have to demonstrate **specific** facts detailing how the records or other information sought are **relevant to a criminal investigation**. In other words, explain how the information requested relates to the investigation for which it is sought. Once a court issues its order, U.S. law enforcement may collect this information in real-time for up to 60 days and renew this request for another 60 days if needed (and approved by the court). This information may be provided to law enforcement promptly.

1.39. A Model MLAR is provided at **Annex Bii**

IMPORTANT NOTE: U.S. legal practice precludes prospective real-time collection of content solely on behalf of foreign governments. An exception to this rule exists, however, if there is a parallel or joint investigation with a U.S. law enforcement agency. In this situation, the U.S. authorities may be permitted to share the product with overseas law enforcement.

The Date Range

1.40. If the MLAR is for **Content Data**, the date range in the MLAR must be compatible with meeting the legal standard (for example probable cause in the U.S.) for the entire period. The MLAR needs to show both that there are reasonable grounds to believe that a suspect or accused committed the offence and also that that the requested SP material will hold evidence of its commission or the email account, messaging app, social media account or website was used to commit the offence, during the relevant time frame.

IMPORTANT NOTE: Be specific - if too long a period of time is requested before or after the crime, probable cause no longer exists. Very often, MLAR's are not satisfied because the period is far too broad. Ideally probable cause should be verified for each period asked. For example: offence committed in November 2015: *do I really need the content of the Facebook account one year before? And if so, why and how can I demonstrate that this content will give me evidence of a crime committed one year later?*

PRACTICAL NOTE

Always put complete dates in an MLAR i.e. 2nd June 2015 Rather than 2/6/2015 – which in the U.S. would mean 6th February 2015.

Assistance requested

1.41. The MLAR drafter will detail in this section the specific electronic evidence that is requested and assistance for each account that is sought, e.g. an appropriate court order or warrant to compel the specified SP to disclose the **BSI**, **Traffic Data** or **Content Data**.

1.42. It is vital that these paragraphs are clear and unambiguous. The reason for each enquiry should be evident having read the summary of facts (i.e. the nexus must have been established) and each request should be sequentially numbered for ease of reference.

1.43. The address of the SP, to serve any legal order for production, should also be included in this section of the MLAR

PRACTICAL NOTE

Include the preservation reference, so this can be included in any order or warrant. Further, this will ensure the preserved electronic evidence can be located quickly by the SP served with the order or warrant.

Type of BSI available

1.44. The following are types of **BSI** that may be available to be produced:

- The user (subscriber's) account or login name;
- The user's name and street address;
- The user's telephone number or numbers;
- The user's email address;
- Date and time of first registration, type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the user
- Any other relevant information pertaining to the identity of the user/subscription holder
- Type of service, including identifier (phone number, IP address, SIM-card number, MAC address) and associated device(s)
- Profile information (user name)
- Data on the validation of the use of service, such as an alternative email address provided by the user/subscription holder
- Debit or credit card information (provided by the user for billing purposes) including other means of payment
- The Internet Protocol (IP) address used by the user to register the account or otherwise initiate service;
- All IP addresses used by the user to log into the account;
- Session times, dates and durations; and
- Any other information pertaining to the identity of the user, including, but not limited to billing information (including type and number of credit cards, student identification number, or other identifying information)

IMPORTANT NOTE: When requesting BSI, always provide a specific email address [e.g. Akan007@me.com] or IP address [e.g. IP address 80.42.104.81], or the URL for a web page [e.g. http://www.youtube.com/user/Victory4Mujahideen] or user name as well as the relevant date, time and time zone)

Types of traffic data available

1.45. The following are types of **Traffic Data** that may be available to be produced:

- For internet SPs
  - Connection destination or source of connection
  - Connection time and date
  - Disconnect time and date
  - Method of connection to system (e.g., telnet, ftp, http)
  - Data transfer volume (e.g., bytes) and
  - Routing information (source IP address, destination IP address(es), port number(s), browser, email header information, message-ID)
  - IP connection records / logs for identification purposes
  - Information pertaining to any image(s) or other documents uploaded to the account including the dates and times of uploading, and the sizes of the files but not including the contents of such files;
  - Name and other identifying details of individuals that accessed a specific image/file/web page between a specified period of time, on a specified date
  - Volume of data

- For web hosting SPs:
  - Logfiles
  - Tickets
  - Purchase history
  - Prepaid balance charging history

Types of content available

1.46. The following are types of **Content Data** that may be available to be produced:

- Any content of emails/messages available in the user's mail account including the IP address of the computer used to send the mail/message;
- Any attachments, photos, videos and audio recordings;
- Contact lists;
- Any draft emails;
- Any available deleted emails;
- (Web)mailbox dump
- Online storage dump (user generated data)
- Pagedump
- Message log/backup
- Server contents
- Any backups
- Any other records and other evidence relating to the requested account or server for example correspondence and other records of contact by any person or entity about the account or server

PRACTICAL NOTE

If the server contents are required, a forensic image maybe requested. This will be an exact copy of the entire server and the MLAR must include reference to the relevant IP Address, Domain Name and Owner of the server

Real-Time Collection of Traffic Data

PRACTICAL NOTE

Consideration should also be given to requesting historic **Traffic Data** (including netflow data) if there is a delay executing an MLAR for real-time collection of **Traffic Data**

1.47. Real-time collection of non-content information refers to obtaining routing information (e.g. data that identifies who is sending an email or connecting to a SP) while the communication is still en route to its destination by producing the log-in IP address.

IMPORTANT NOTE: This information will not include the content of the email, any attachments that may accompany it, or the subject line.

1.48. In the U.S. the term '*Pen Register*' is used interchangeably with '*trap and trace*' to describe the real-time collection of **Traffic Data** in U.S. Law

PRACTICAL NOTE

This technique is particularly useful to track the locations of suspects who use encrypted social media accounts where they are unable to request the content or move between devices. An investigator who has the IP address a suspect used and the time when it was used may be able to identify the location of the individual.

Use of evidence obtained

1.49. It is very important to state clearly the purposes for which the assistance is sought and to cover all reasonably foreseeable purposes. The following paragraph, adapted to the circumstances of the case, should be included in this section:

'*Unless you indicate otherwise, any evidence obtained pursuant to this request may be used in any criminal prosecution and related ancillary proceedings (including trials, restraint, confiscation and enforcement hearings) arising in whole or in part from the above noted investigation / prosecution, whether relating to the above-named subject(s) or to any other persons who may become a subject of this investigation / prosecution.*'

IMPORTANT NOTE: The clear purpose of any speciality provision is to prevent the party obtaining assistance from getting around any restrictions that an arrangement would otherwise impose by, for example, identifying a clearly non-political offence and then using the material obtained to prosecute a political offence.

1.50. If, having received the electronic evidence, the SPC wants to use it for an additional purpose to that stated in the original MLAR then it will be necessary to obtain the consent of the Requested State. Failure to do so may lead to the evidence being unable to be used in a trial in the SPC. An attempt to use evidence obtained without the requisite consent of the Requested State may also jeopardise future co-operation.

1.51. A request to obtain consent to use material already in the SPC's possession can usually be made by any means acceptable to the Requested State, including email and telephone. A written record of the request and the consent should be kept. An MLAR purely for this purpose would be inappropriate.

1.52. In order to clarify what happens to the evidence at the conclusion of a prosecution, it is advisable to include a paragraph in the MLAR to the effect that, '*unless otherwise informed we understand that you have no objection to the evidence obtained being kept at the conclusion of proceedings*'.

Preferred form of evidence

1.53. It is good practice to include this information under the heading '*Assistance requested and preferred (or required) form of evidence*' as this is often the first section of the request that the Central or Competent Authority of the Requested State looks at. If the '*preferred (or required) form of evidence*' is not listed in the same section as the '*assistance requested*', then requirements may be overlooked.

1.54. If alternative forms in which the electronic evidence might be provided may be acceptable to the Requesting State, such as there are alternative forms capable of meeting admissibility requirements, these alternative acceptable forms might be communicated to the Requested State, together with an indication prioritising which of those different forms of evidence is most preferable.

1.55. Executing Competent Authorities will generally do what they can to provide the assistance sought, in the format requested. Some international MLA arrangements require the executing Competent Authority to execute the request in the manner requested, provided that to do so is not inconsistent with the law of the Requested State.

Confidentiality

1.56. In some States, the judicial authorities may have an obligation to inform the affected person after intrusive measures have been taken against that person. In these circumstances, the Requesting State must address this issue in the MLAR and determine if confidentiality, to protect sensitive sources or intelligence, is required.

1.57. In many Requesting States, it seems obvious that law enforcement work is confidential and that investigative actions or requests will remain secret. This is not the case in the U.S. where transparency is the rule. Not only do most SPs, as a policy, notify their users when some authority asks to see their data but judges are very reticent to impose non-disclosure obligations which are called, '*gag orders*' or '*non-disclosure orders*'. Hence non-disclosure has to be specifically requested in the MLAR with a strong rationale (or '*good cause*') – for example disclosure could result in:

- Endangering the life or physical safety of an individual
- Flight from prosecution
- Destruction of or tampering with evidence
- Intimidation of potential witnesses, or
- Otherwise seriously prejudicing an investigation or unduly delaying a trial

1.58. If a suspect knows that he is being investigated, it is more difficult to have a strong rationale for confidentiality and specific explanation why these reasons may still apply is required (e.g., there are still other accomplices who do not know they are targets).

1.59. In the U.S., non-disclosure orders are limited in duration, which is something to bear in mind if an investigation is lengthy. In such cases, it is important to keep track of the expiration date of a non-dis-

closure order, and, if needed, to request that the U.S. Central Authority assist in obtaining an extension of the non-disclosure. The request to extend must be made prior to the original non-disclosure order's expiration.

1.60. In the U.S., requests may also be kept confidential through use of a '*sealing*' order. When the magistrate judge grants an order, he or she also may also order that the matter be '*sealed*', meaning that all court filings pertaining to the matter (including information about the MLAR) would not be accessible to the public. Sealing may be limited in duration, and it is important to contact the U.S. Central Authority if an additional sealing period is required.

1.61. Always include information in the MLAR as to whether confidentiality (i.e., a non-disclosure order and/or sealing) is needed or not so the question is not asked, which could delay execution of the MLAR.

PRACTICAL NOTE

Sealing can be done for a number of reasons including to prevent disruption to an on-going investigation or if personal details of a witness or victim are disclosed. Documents may be unsealed, for example, once the named person is arrested. Ordinarily documents will become unsealed after a specified time period unless grounds are provided to the U.S. Central Authority not to unseal.

Transmission of electronic evidence

1.62. This will usually be via a Central Authority in the SPC. Where documents are sensitive, a method of delivery that requires a signature on receipt should be requested. Where appropriate a request should be made for the material to be protectively marked by the Requested State or sent on an encrypted medium. In all cases, request in the MLAR that the Requested State email the SPC's Central Authority when they dispatch the evidence. For example: '*When you send the evidence, please also email firstname.surname@gov to confirm that the evidence has been sent. This will enable me to make enquiries to locate the evidence if it is not received within a few days.*'

IMPORTANT NOTE: In the U.S. a government agent will filter the produced Content Data to ensure that only electronic evidence that is requested in the MLAR is transmitted to the Requesting State. For certain complex or serious investigations, the U.S. Central Authority has sometimes allowed a law enforcement officer from the Requesting State to attend and assist in this process. If the attendance of a law enforcement officer from the Requesting State is required, the request for permission to travel should be included in the MLAR.

ReciprocAL procedural laws of a Requesting and Requested States

1.63. Some Requested States will only provide MLA if the Requesting State would be able to undertake the requested enquiries itself under its domestic law. In this case, the MLAR should include an appropriate assurance to this effect. If a Requesting State is unable to provide this assurance it is essential they contact the Requested State's Central Authority to confirm if the request can still be executed. This should be completed as a priority before sending the MLAR so time and effort is not wasted in both States.

1.64. This will be of particular importance if the MLAR is based on treaties which have no specific provisions for securing electronic evidence from SPs such as, for example, all UN conventions as well as all regional and sub-regional treaties on MLA in criminal matters. Requesting States will have to confirm in the MLAR that they have reciprocal legislation that would enable a SP in their State to be compelled to produce electronic evidence.

Contacts

1.65. Full contact details of the MLAR writer, and of investigators whom the Requested State is invited to contact must be included if any issues arise or further supporting information is required to fulfil the execution of an MLAR. This should include addresses, personal telephone numbers and emails, and where appropriate details of languages spoken.

Translation

1.66. Once the MLAR is completed it may be necessary to obtain a translation into an official language or one of the official languages of the Requested State). Only suitably qualified translators should be used. A poorly translated MLAR may lead to problems in the execution of the MLAR. It is preferable either to send the MLAR translated or obtain prior confirmation from the Requested State that the proposed request can be actioned fully if sent in the language of the Requesting State.

PRACTICAL NOTE

Some States have different dialects and it is important to confirm with a Requested State's Central Authority the specific translation required.

CASE STUDY

An MLAR is drafted by a Counter-terrorist investigative judge on 2 March 2017 and transmitted by the Central Authority of Newcountry on 7 March 2017 to the U.S. Central Authority

Office of International Affairs
U.S. Department of Justice
Washington DC

Your Ref: CT1/3/2017
Our Ref: CT1/MLAR1/2017
Date: 2 March 2017

Dear Sir or Madam

MUTUAL LEGAL ASSISTANCE REQUEST:

Suspect name: John Doe

Operation Improve

My name is Investigative Judge X, from the Newcountry High Court of Cassation & Justice and I have the honour to request your assistance in relation to a criminal investigation being conducted by the Counter-Terrorism Police of Newcountry (CTPN).

URGENT

We request that this matter is dealt with urgently in view of the threat to life posed by members of the terrorist network yet to be identified. The electronic evidence requested from Twitter will assist CTPN to identify other participants in the terrorist network and prevent further terrorist acts.

BASIS OF THE REQUEST

I have the honour to request your assistance under the provisions of the Treaty of Mutual Legal Assistance in Criminal Matters (2017) between the United States of America and Newcountry.

CONFIDENTIALITY

In order not to prejudice the investigation, I request that no person (including the subject John Doe) is notified by the competent authorities in your country of the existence and contents of this Request and any action taken in response to it. I further request that action is taken to ensure that any person from whom evidence is sought does not so notify any other person.

PURPOSE OF THE REQUEST

This is a request for evidence from Twitter (content evidence) in the USA for use in the investigation into and any subsequent prosecution of (including any related freezing, confiscation and enforcement proceedings and any ancillary proceedings related thereto) the following:

SUBJECT	DATE of BIRTH	PLACE of BIRTH	NATIONALITY	ADDRESS
John Doe	1st July 1980	Newtown	Newcountry	1st District Newtown

CTPN are investigating the following offences:

1. Material support to a terrorist organization contrary to Article 256 Criminal Code 2017

   Sentence: Life Imprisonment

2. Directing the terrorist organization contrary to Article 257 Criminal Code 2017

   Sentence: Life Imprisonment

THE RELEVANT LAW

Please find the applicable Newcountry Law at Annex A.

SUMMARY OF FACTS

1. John Doe left Newcountry in September 2011 to join the ranks of a well-known terrorist organization in Oldcountry B. Once in site, he opened several accounts on social media, notably Facebook and Twitter and became very active in terms of propaganda.

2. He specifically encouraged, on October 2012, his fellow-believers to commit attack on the soldiers of Newcountry by publishing for instance: "go get your knife and kill the first soldier you see".

3. John Doe was arrested in Oldcountry and deported back to Newcountry where he was incarcerated.

4. Processing his iPhone 5, switched off, without a Sim Card, IMEI number xxxx, showed its entire content had been deleted but there was one message he send to an unknown addressee, using his twitter app: "*I deleted your number- they cannot lock me up for ever- They will see when I come out*"

ASSISTANCE REQUESTED AND REQUESTED FORMAT OF EVIDENCE

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Twitter, Inc.

c/o Trust & Safety - Legal Policy 1355 Market Street, Suite 900 San Francisco, CA 94103 (attn: Trust & Safety - Legal Policy)

all of the Content Data held by them relating to the account #johndoe for the period commencing 1 September 2011 to the date of this request including, but not limited to:

1. Copy of the entire private and public Twitter exchanges of the account

2. Basic subscriber information: provided when the account was created: surname, name, first name, alias, nickname, username, date and place of birth, address, telephone

3. The date, time and IP address of account creation

4. The recording of the sessions and their length (date and time for the beginning and end of sessions, IP addresses used)

5. The list of followers and the list of accounts followed by the account holder

6. All other information available on this account in possession of the provider: its user and its contents.

It is further requested that:

1. Such other enquiries are made, persons interviewed and exhibits secured as appear to be necessary in the course of the investigation

2. Any records are produced as exhibits in any statements together with an explanation of the technical terms used in the records

3. Any information held on computer in any form be preserved and secured from unauthorised interference and made available to the investigating officers and the Newcountry High Court of Cassation & Justice for use at any subsequent trial

4. Any material provided to me pursuant to this request may be used in any criminal prosecution or other judicial proceedings connected with this matter, including any other freezing or confiscation proceedings and ancillary proceedings relating thereto including proceedings relating to any breaches of, variation of, reassessment of, or enforcement of Newcountry court orders

5. The above enquiries are made and that permission be given for the original or signed and certified copies of any statements made and documents or other items secured during the course of the enquiries to be removed to Newcountry for use in any criminal proceedings, trial, confiscation and enforcement proceedings.

RECIPROCAL PROCEDURAL LAWS

I confirm that the assistance requested above may be obtained under current Newcountry law if in a like case a request for such assistance were made to the authorities in Newcountry.

TRANSMISSION OF EVIDENCE

Please send any evidence to the Newcountry Central Authority and advise if you wish to have any part of the evidence returned to you at the conclusion of the proceedings in Newcountry.

When you send the evidence, I would be grateful if you would also me to confirm that the evidence has been dispatched. This will enable enquiries to be made to locate the evidence if it is not received within a few days.

The content of the email account and associated storage should be stored on a computer disk and should be encrypted to protect the content.

CONTACTS

Investigating Judge: Judge X

Email: JX@HCCJ.nc

Contact Number: 23142 676257

Address: The High Court of Cassation & Justice

I extend my thanks in anticipation of your valued co-operation and assistance in this matter.

Yours faithfully,

Judge X

The Following Problems are identified with the above MLAR:

1. How is it known this is a well-known terrorist organization?
2. How do law enforcement officers in Newcountry know the subject became very active on social media?
3. How is the conversation from October 2012 revealed?
4. What is the date range for the electronic evidence requested?
5. What is the rationale for not notifying the subject?
6. Is there sufficient probable cause to link the subject to
    a. The terrorist organization?
    b. The subject to a specific crime?
    c. The subject to the iPhone?
    d. The Tweet to a specific crime?
7. Has the Twitter account been preserved?
8. No reference to reciprocity

The U.S. Central Authority send an email with a query about Preservation

From: Attorney Y U.S. Central Authority
To: Newcountry Central Authority
Date: 8 June 2017
Subject: John Doe MLAR 3 March 2017

Dear Sirs,

We received your MLAR on June 8th 2017

In order to progress we will require confirmation the Twitter account has been preserved and the reference number from Twitter please

Thanks,
Attorney Y

The Newcountry Central Authority send an email to Judge X asking about preservation. Later that same day another email is received from the U.S. Central Authority detailing more issues with the MLAR

From: Attorney Y U.S. Central Authority
To: Newcountry Central Authority
Date: 30 June 2017
Subject: John Doe MLAR 3 March 2017

Dear Sirs,

Further to our earlier email we also require the following information please:

How did authorities from Newcountry learn that John Doe joined the terrorist organization in 2011? For example, did he publicly (or otherwise) acknowledge his affiliation with the organization?

What facts indicate that the Twitter account XXX belongs to him?

The request quotes the text of a message that John Doe posted on social media on October 2012, encouraging an attack on the military of country A and others. Did he post it to that Twitter account?

Did John Doe use the Twitter account xxx on other occasions, particularly around the time of his arrest, to commit, further, or discuss the criminal activity under investigation? If yes, how was he using Twitter account XXXX to commit, further, or discuss the criminal activity under investigation and when (a date range is fine)?

The request indicates that analysis of John Doe's phone revealed the contents had been deleted except for one message to an unknown person. The message stated, in part, that John Doe was "deleting your number and the others so they won't find anything" and that he will "act" when he is released.

Was this message sent via Twitter account xxx
When was the message sent?

What were the facts and circumstances around him sending this message that suggest he plans to take violent action on behalf of a terrorist organization?

Finally, we had inquired about whether your authorities requested preservation of the target Twitter account. If you have, we ask that you please maintain the preservation until resolution of this request. If you encounter any issues doing so, please let us know.

Attorney Y

The Newcountry Central Authority send a reply by email to the U.S. Central Authority on 15 September 2017

From: Newcountry Central Authority
To: Attorney Y U.S. Central Authority
Date: 15 September 2017
Subject: John Doe MLAR 3 March 2017

Dear Sirs,

Further to your earlier email of 30 June 2017 we confirm the following:

1. What facts indicate that the Twitter account XXX belongs to him?

    - Open source research reveals several account (Facebook and Twitter) with the same associated avatar (a monkey), same email and same user name.
    - John Doe is known by intelligence services to use this user name as his alias.
    - What is said on Facebook about the account user's whereabouts match what is said by John Doe in his interviews to the judge.
    - The public part of the Twitter account was also helpful.
    - In his hearings, he admitted to the use of the social media accounts for which data are requested.

2. How did Newcountry authorities learn that John Doe joined the terrorist organization? For example, did he publicly (or otherwise) acknowledge his affiliation with the organization?

    - This knowledge comes from the analysis of his social media accounts and was confirmed by his own admission during his interviews by the investigative judge. (again, copy translated of his hearing transmitted)

3. The use of his Twitter account:

    - Transcripts of conversations directly showing conversations to recruit or encourage terrorist acts - attached

4. What were the facts and circumstances around him sending this message that suggest he plans to take violent action on behalf of a terrorist organization?

    - See attached John Doe's travel documents showing when he joined the terrorist organization

- Elements from his hearings in front of the judge in which he describes his involvement, his role and responsibilities
- His links to well-known terrorists, for instance he traveled with one of them and the dates were close to major attacks in Europe

Regards,
Attorney Z

The U.S. Central Authority send a response by email to the Newcountry Central Authority on 19 September 2017

From: Attorney Y U.S. Central Authority
To: Newcountry Central Authority
Date: 19 September 2017
Subject: John Doe MLAR 3 March 2017

Dear Sirs,

Further to your earlier email of 15 September 2017 we respond with the following further queries:

1. On the link between John Doe and the Twitter account: he admitted to the possession of which social media account?

2. On the use of the Twitter account: despite transmission of very explicit transcripts of Tweets, we require more examples and date ranges for the posts please.

3. An important issue is confidentiality

The request asks that we treat this matter with confidentiality. This would mean for any application to the court that may result, we would request that the court issue a sealing order and a nondisclosure order, if appropriate. If we are in a position to file an application with the court, we will plan to seek a sealing order, which will prevent public disclosure of any application to the court and any resulting order (sometimes for a specific period of time).

A nondisclosure order would prevent Twitter from notifying the Twitter accountholder of the application and order

Given that John Doe is aware of the investigation, our typical justification in support of a nondisclosure order —letting a suspect discover he is under investigation— is weaker.

To obtain a nondisclosure order, we generally must show the court that disclosure could result in

a. Endangering the life or physical safety of an individual
b. Flight from prosecution,
c. Destruction of or tampering with evidence
d. Intimidation of potential witnesses
e. Otherwise seriously jeopardizing an investigation or unduly delaying a trial

If your authorities seek a nondisclosure order, please provide details explaining why one or more those criteria have been met here so that we may further evaluate this option.

We ask that you please provide supplemental information within 90 days. Should we not receive supplemental information by then, we will assume that Newcountry authorities no longer require the execution of this request, close our file, and cease efforts to preserve the Twitter account at issue.

Regards,
Attorney Y
U.S. Central Authority

The Newcountry Central Authority reply to the U.S. Central Authority on 22 September 2017 and request the General Prosecutor meets to discuss the MLAR

From: Newcountry Central Authority
To: Attorney Y U.S. Central Authority
Date: 22 September 2017
Subject: John Doe MLAR 3 March 2017

Dear Sirs,

Further to your earlier email of 19 September 2017

Confidentiality was not requested

All the Twitter transcripts relevant to the case have already been sent

The preservation reference from Twitter is #432123 and was extended for a further 90 days on 5 September 2017.

We reiterate the significant public interest in this matter and its importance to our national security.

We confirm that our General Prosecutor Madam G will be making an official visit to the U.S. and would be obliged to meet to discuss progress.

Regards,
Attorney Z
Newcountry Central Authority

October 2017: Twitter says there is a problem with the account URL and mails go back and forth between the two Central Authorities to make sure this is solved.

November 2017: the case moves from the U.S. Central Authority to a Federal Attorney in California.

Although Newcountry requested content, the Attorney in California confirms that he plans to ask the Magistrate Judge in San Jose for a d-order for Traffic Data to be served on Twitter i.e. dates of the tweets, who sent it and who read it.

A d-order is served on Twitter on 29 November 2017

December 2017: No news

3 January 2018: Newcountry requests an update and receives 2 days later from the U.S. Central Authority an advance copy by email of the d-order results provided by Twitter.

The Newcountry Central Authority Twitter review the d-order results which only confirm BSI that the Newcountry Counter-Terrorism Police (NCTP) already had. There is no login information nor any IP - yet the NCTP know the account has been used by the subject. The Newcountry Central Authority send an email on 8 January 2018 complaining that they have not received the evidence requested.

From: Newcountry Central Authority
To: Attorney Y U.S. Central Authority
Date: 8 January 2018
Subject: John Doe MLAR 3 March 2017

Dear Sirs,

Further to receipt of the d-order results on 5 January 2018 only basic subscriber information was attached – which we already have.

We, as you know, need the traffic data to support probable cause for content. I know you asked for the traffic data. Can you please tell me if other results are coming? As you know this is our most sensitive case and very urgent.

Thank you for your help.

Attorney Z
Newcountry Central Authority

Attorney Y from the U.S. Central Authority calls Attorney Y at the Newcountry Central Authority and asks whether John Doe is still in custody and what are the deadlines for the case to go to court.

Later in January Twitter produces additional records, which are sent by the U.S. Central Authority to Country A both by advanced email copy and by Fedex on a CD.

The Newcountry Central Authority now has relevant traffic data that supports probable cause for content and sends an email to the U.S. Central Authority confirming this additional information

February 2018: Finally, after some pressure from the General Prosecutor from Newcountry, a search warrant is served on Twitter for content data.

March 2018: The results of the search warrant are collected from Twitter by the FBI who sift through the contents and 5 days later the results are transmitted to the Newcountry Central Authority. The electronic evidence is received by the General Prosecutor's office and finally to the judge, **one year after the MLAR was drafted**.

Five Important Issues:

1. **The MLAR had insufficient information to support a search warrant for content data**
2. **Contact should have been made with the U.S. Central Authority to discuss the MLAR and a draft sent for review before formal transmission**
3. **Preservation information should have been included from the outset**
4. **Time was wasted clarifying information that should not have been in the MLAR for example confidentiality**
5. **Any supporting documentary evidence (such as tweets) should be attached to support probable cause**

The cloud act

1.67. On 23 March 2018, the "Cloud Act" (Clarifying Lawful Overseas Use of Data Act) became public law in the U.S.. This legislation is intended to allow authorities to legally compel SPs to provide electronic evidence stored on foreign servers under their control.

1.68. Additionally, the Cloud Act allows the U.S. to enter executive agreements with foreign governments that will enable the latter to get content and real-time interceptions directly from SPs and on a voluntary basis.

1.69. To reach such an agreement, different conditions, expressed within the legislation, need to be met, and reciprocity must be ensured. The sufficiency of any agreement needs to be certified by the Attorney General, and there is a final review by Congress. Once enacted, those agreements are subjected to periodical review every five years. Only the United Kingdom has such an executive agreement in place to date.

1.70. From the perspective of SPCs, the Cloud Act can provide significant advantages regarding swiftness when it comes to access to electronic evidence in the U.S., provided the SPC has reached an agreement, and the SP accepts to disclose on a voluntary basis. If this is not the case, the traditional avenues for requesting electronic evidence are to be used.

Proposed European Rules

1.71.  The European Commission has published proposed new rules to make it easier and faster for law enforcement and judicial authorities to obtain electronic evidence on the cloud through the following (also see **Annex I**):

- **European Preservation Order: This will allow a judicial authority in one Member State to oblige a service provider offering services in the Union and established or represented in another Member State to preserve specific data to enable the authority to request this information later via mutual legal assistance, a European Investigation Order or a European Production Order**
- **European Production Order:** This will allow a judicial authority in one Member State to request electronic evidence directly from a service provider offering services in the Union and established or represented in another Member State, regardless of the location of data, which will be obliged to respond within **10 days**, and within **6 hours** in cases of emergency

GLOSSARY

Account (or user) Identifier

This can be a username, email address, URL, or other method used to uniquely identify a user or account of a Service Provider.

Backup

A copy of a file or other data created in case of deletion or damage.

Basic Subscriber Information (BSI)

Information stored by a Service Provider confirming the name of the subscriber/user and may include how long the subscriber has used that specific service and the IP address of the first login.

Cloud Backup (or Managed Backup Service or Backup-as-a-Service)

A service that provides users with a system for the backup storage and recovery of computer files. Such backup services are considered a form of Cloud Computing.[42]

Cloud Computing

The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Cloud Storage Service (or File Hosting Service, Online File Storage Provider or Cyberlocker)

An internet hosting service specifically designed to host user files. It allows files to be uploaded that can be accessed over the internet after a password or other authentication is provided.

Comity

This refers to situations where MLA is granted despite a lack of a treaty or application of an international convention, on the basis of courtesy.

Competent Authority

This refers to the authority that will execute the MLAR in the Requested State.

Cross-platform Application

Computer software that can operate on multiple computer platforms such as Microsoft Windows and MacOS.

42. https://en.wikipedia.org/wiki/Remote_backup_service

D-Order

Named after section 2703(d) of the Electronic Communications Privacy Act (ECPA), a d-order will be granted if a U.S. Court is satisfied that there are, *"specific and articulable facts showing that there are reasonable grounds to believe that (the information) is relevant and material to an ongoing investigation."*

Data

The quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

Data retention

Retaining data in accordance with regulatory or legal requirements for a specified period.

Distributed Denial of Service

Denial of service (DOS) attacks are attempts to render a computer system unavailable to users through a variety of means. These may include saturating the target computers or networks with external communication requests, thereby hindering service to legitimate users. Distributed denial of service (DDOS) attacks are denial of service attacks executed by many computers at the same time. There are currently a number of common ways by which DOS and DDOS attacks may be conducted. They include, for example, sending malformed queries to a computer system; exceeding the capacity limit for users; and sending more e-mails to e-mail servers than the system can receive and handle.[43]

Domain Name

Domain names are used in uniform resource locators (URL) to identify web pages. Each domain name has a suffix for example .com **for each service provider.**

Dual Criminality

Requires that the particular acts alleged are a crime in both the Requesting and Requested State. The elements of the analogous offences need not be the same, but they must be sufficiently familiar that the conduct is criminal in both States.

Dynamic IP Address

A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it's connected to a network.[44]

43. T-CY Guidance Notes – 1 March 2017 p 18
44. https://www.techopedia.com/definition/28504/dynamic-internet-protocol-address-dynamic-ip-address

Electronic Evidence

Includes BSI, Traffic Data and Content Data.

Encryption

The process of encoding a message or information in such a way that only authorized parties can access it.

End-to-end Encryption (E2EE)

E2EE is a system of communication where only the communicating users can read the messages. E2EE prevents third parties deciphering the data being communicated or stored in servers. This means that Service Providers using end-to-end encryption, are unable to hand over content of Users' messages to law enforcement.

Freeware

Freeware is software that is available for use at no monetary cost.[45]

File Synchronization

Is the computer process of ensuring that computer files in two or more locations are updated via agreed rules.

File Transfer Protocol (FTP)

A network protocol used for the transfer of files between computers.

Forensic Image

Imaging is a phrase that is commonly used for copying or cloning the contents of a hard drive or server.

Good Cause

This means adequate or substantial grounds, or reason to take a certain action, or to fail to take an action, and is always dependent on the circumstances.

Good Faith

This means a general presumption that relevant will deal with each other honestly and fairly.

45. https://en.wikipedia.org/wiki/Freeware

Hypertext Transfer Protocol (HTTP)

The foundation of data communication for the World Wide Web that allows for the exchange of hyperlinks.

IP Address

An internet protocol address (IP address) is a numerical label assigned to each device (e.g. Computer) participating in a computer network that uses the internet protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing

Instant Messaging

Online chat that offers real-time text transmission over the internet.

Joint Investigation Team

An agreement between competent authorities – both judicial (judges, prosecutors, investigative judges) and law enforcement – of two or more States, established for a limited duration and for a specific purpose, to carry out criminal investigations in one or more of the involved States.

Log Files

A log file is a file that records events that occur in a computer system

Login

A login is a set of credentials used to authenticate a User or Subscriber of a website, computer application or mobile app. Logins may include a username and password or a PIN number, passcode, or passphrase. Some logins may also require a biometric identifier, such as a fingerprint or retina scan.

Media Access Control (MAC) Address

A unique identifier for a device connected to a network.

Metadata

Is data providing information about one or more aspects of the data, such as:

- **Means of creation of the data.**
- **Purpose of the data.**
- **Time and date of creation.**
- **Creator or author of the data.**
- **Location on a computer network where the data was created.**

- **Standards used (i.e. uniform engineering or technical criteria, methods, processes and practices).**

Mutual Legal Assistance

The provision of assistance, usually in the gathering and transmission of evidence by a competent authority of one country to that of another, in response to a written request for assistance.

Mutual Legal Assistance Request (MLAR)

Term used for the formal written document by which an MLA can be made (in French, a '*commission rogatoire*' or a Letter Rogatory) – also known as a Letter of Request.

Netflow Data

NetFlow data covers IP network traffic, comprising details of which other IP addresses are contacting servers and which they are contacting.

Parallel Investigation

Where two States have independent but simultaneous investigations (that are not subject to a Joint Investigation Team Agreement). These can be subject to informal coordination and communication to determine strategy and how to share evidence.

Pen Register

In U.S. Law a Pen Register is defined as

"A device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business".

Police-to-Police Cooperation

This includes law enforcement officers from a one State directly contacting counterparts for assistance in another.

Port Number

A *port number* is part of the addressing information used to identify the senders and receivers of messages. Port numbers are most commonly used with IP connections. These port numbers

allow different applications on the same computer to share network resources simultaneously and can assist to identify a specific user.

Probable Cause

A higher legal standard of proof than, *"reasonable grounds to believe"* but not as high as, *"more likely than not"*. Probable cause requires credible evidence, which can include hearsay or intelligence provided that it is demonstrably reliable.

Purge

An SP removing all data from its server

Raw Message Format

A message sent as an entire message in a single field.

Reciprocity

Also known as mutuality, reciprocity in this context means a requested state recognizes the same investigative and court processes that the requesting state can use in its domestic proceedings.

Requested State

Refers to a State executing a Mutual Legal Assistance request from a Requesting State.

Requesting State

Refers to a State requesting Mutual Legal Assistance in the gathering and transmission of evidence by a competent authority of one State.

Reasonable Grounds to Believe

This legal standard of proof relies upon there being enough credible evidence to lead a person of ordinary and prudent judgement to the suspicion and belief that the applicant holds.

Routing Information

Routing is the process of selecting a path for traffic in a network, or between or across multiple networks. Information provided by routing includes: Source IP address, destination IP address(es), port number(s), browser, email header information, message-ID.

Sign on Logs

Logging in (or logging on or signing in or signing on) is the process by which an individual gains access to a computer system by identifying and authenticating themselves the logs show when a user logged in.

Source IP Address

Source IP is the IP address of the device sending data transfer.

Service Provider (SP)

A service provider transports information electronically, and encompasses companies in the internet, cable, satellite, and social media services.

Static IP Address

A static Internet Protocol (IP) address is a permanent number assigned to a computer by a Service provider. Static IP addresses are useful for gaming, website hosting or Voice over Internet Protocol (VoIP) services.[46]

Telnet

A protocol used on the internet (or a local area network) that allows for text to be communicated between computers.

Touchpoint

A touchpoint describes the connection of a service provider with its users. Therefore, if a subscriber's registration information or ip address resolves to a specific state – this means that state is the touchpoint.

Traffic data or Transactional Information/data

Information that includes records identifying with whom a subscriber communicated, what websites a subscriber visited, and similar information about a user's online activity.

URL

A URL is one type of uniform resource identifier (URL); the generic term for all types of names and addresses that refer to objects on the world wide web. The term "web address" is a synonym for a URL that uses the http or https protocol.

46. https://www.techopedia.com/definition/9544/static-internet-protocol-ip-address-static-ip-address

User

The term used interchangeably with subscriber, refers to the person who is registered to use a social media or other online messaging service, such as email.

Virtual Private Network

A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.[47]

Voice Over IP

Technology that delivers voice messages over Internet Protocol (IP) networks such as the internet.

Web Hosting

A web hosting service is a type of Internet hosting service that allows individuals and organizations to make their website accessible via the World Wide Web.

Website Defacement

An attack on a website that changes the visual appearance of the site or webpage.[48]

24/7 Networks

Point to point network for urgent assistance in cybercrime matters – each State has a single point of contact available 24 hours a day, 7 days a week.

47. https://en.wikipedia.org/wiki/Virtual_private_network
48. https://en.wikipedia.org/wiki/Website_defacement

ANNEXES

ANNEX A: Links to Service Provider Law Enforcement Guidelines

The following law enforcement guides (or transparency reports or privacy policies) are available online (also see: http://www.search.org/resources/isp-list/) - please refer to the most recent online documents:

Adobe For users in U.S.	http://www.adobe.com/legal/lawenforcementrequests/law- enforcement.html
For users outsider of the U.S.	https://www.adobe.com/legal/lawenforcementrequests/law-enforcement-intl.html
Airbnb	https://www.airbnb.co.uk/help/article/960/how-does-airbnb-respond-to-data-requests-from-law-enforcement
Amazon	https://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf
Ask.FM	http://safety.ask.fm/ask-fm-guide-for-law-enforcement-requests/
Atlassian	https://www.atlassian.com/legal/guidelines-for-law-enforcement
Apple	http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf
Baaz	https://www.baaz.com/privacy
Comcast	https://www.xfinity.com/law-enforcement-handbook
DropBox	https://www.dropbox.com/transparencyhttps://www.dropbox.com/transparency
Facebook	www.facebook.com/safety/groups/law/guidelines
GoDaddy	https://uk.godaddy.com/agreements/ShowDoc.aspx?pageid=civil_subpoena
Google	https://support.google.com/transparencyreport/answer/7381738?hl=en
Hidemyass	https://www.hidemyass.com/legal/privacy
IVPN	https://www.ivpn.net/privacy
Instagram	https://help.instagram.com/494561080557017/
Kik	https://lawenforcement.kik.com/hc/en-us
Linkedin	https://help.linkedin.com/ci/fattach/get/7890851/0/filename/Law_Enforcement_Guidelines_January%202018.pdf
Pinterest	https://help.pinterest.com/en/articles/law-enforcement-guidelines
Snapchat	www.snapchat.com/static_files/lawenforcement.pdf
Surespot	https://www.surespot.me/documents/surespot_law_enforcement_guidelines.html
Tumblr	https://www.tumblr.com/docs/law_enforcement
Twitter	https://support.twitter.com/articles/41949-guidelines-for-law-enforcement#

Uber For law enforcement in the U.S.	https://www.uber.com/en-GH/legal/data-requests/guidelines-for-law-enforcement-united-states/en-US/
For Law enforcement outside of the U.S.	https://www.uber.com/en-GH/legal/data-requests/guidelines-for-law-enforcement-outside-the-united-states/en/
WhatsApp	https://faq.whatsapp.com/en/general/26000050
Wikr	https://www.wickr.com/legal-process-guidelines/
Verizon	https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_irvine7_irvi neca.pdf
Viber (Privacy Policy)	https://www.viber.com/terms/viber-privacy-policy/
Yahoo	https://transparency.yahoo.com/law-enforcement- guidelines/us/index.htm?soc_src=mail&soc_trk=ma

ANNEX Bi: Model MLAR for Stored Electronic Evidence

Address of Central Authority

Dear Sir or Madam

MUTUAL LEGAL ASSISTANCE REQUEST:

[insert Operation name]

[insert Name of Accused/s or Suspect/s]

URGENCY

[Please consider if the request is truly urgent – over use can cause difficulties and delays other cases – if so confirm reasons e.g. threat to life or serious physical harm]

I am **[insert name]** a **[insert title]** of the **[insert name of Agency]** and I am empowered to make this request for evidence pursuant to **[insert relevant domestic law]**

Basis of the Request

I have the honour to request your assistance under the provisions of **[insert relevant Treaty of Mutual Legal Assistance in Criminal Matters]**

CONFIDENTIALITY

In order not to prejudice the investigation, I request that no person (including any of the subjects) is notified by the competent authorities in your country of the existence and contents of this Mutual Legal Assistance Request and any action taken in response to it. I further request that action is taken to ensure that any person from whom evidence is sought does not so notify any other person.

If the above subjects or an associated party became aware of the existence of this request **[or]** sensitive material, namely **[identify the sensitive material – either the entire request or confirm the relevant part] [or]** of action taken in response to it, it is reasonably justifiable to believe that disclosure of the fact of an investigation to the subjects will result in **[insert as appropriate for example destruction of evidence]** as supported by **[describe conduct in support i.e. deletion of accounts]**

If it is not possible to preserve confidentiality in the above manner, please notify me prior to executing this Mutual Legal Assistance Request.

PURPOSE OF THE REQUEST

This is a request for evidence **[insert type of evidence e.g. content of emails – and the service provider. Be explicit if required for real-time collection of non-content]** for use in the prosecution (including any related restraint, confiscation and enforcement proceedings and any related ancillary proceedings) of the following

[insert if suspects/accused known]

SUBJECT	DATE of BIRTH	PLACE of BIRTH	NATIONALITY	ADDRESS

The above are the subject of a criminal investigation being conducted by **[insert name of investigating Law Enforcement Agency]** and a criminal prosecution being conducted by the **[Insert relevant Agency]** for offences of **[insert offences, relevant statute and maximum sentences].**

[insert if only IP address of a server known]

This is a request for the competent authorities in **[insert Requested State]** to provide a forensic image of the servers listed below for use in Court Proceedings within the jurisdiction of **[insert Requesting State]**

IP ADDRESS	HOSTING COMPANY (name and address)

OR

The **[insert name of investigating Law Enforcement Agency]** is attempting to identify individuals involved in **[insert criminality]**. This evidence will be used in any subsequent prosecution of these individuals (including restraint, confiscation and enforcement proceedings and any related ancillary proceedings) who are committing offences associated with the **[insert name of software]** and its variants namely: **[insert offences, relevant statute and maximum sentences]**

[insert if only email address or social media username known]

This is a request for the competent authorities in the **[insert Requested State]** to provide evidence related to the email address listed below for use in Court Proceedings within the jurisdiction of **[insert Requesting State]**

USERNAME	Service Provider (name and address)

The **[insert name of investigating Law Enforcement Agency]** is attempting to identify the user of the **[insert Service Provider]** and obtain the material more particularly detailed in the

Assistance Required paragraph below. This evidence will be used in any subsequent prosecution of the individual/s (including restraint, confiscation and enforcement proceedings and any related Ancillary proceedings) who are committing offences associated with the **[insert email address]**: **[insert offences, relevant statute and maximum sentences]**

THE RELEVANT LAW

Please find appended to this Mutual Legal Assistance Request the applicable Law at Annex A.

SUMMARY OF FACTS AND HISTORY OF PROCEEDINGS

Include a chronology of the investigation and a brief summary of the offences investigated/ prosecuted against each subject

IMPORTANT NOTE: Provide nexus between the offences investigated and the electronic evidence requested

PRESERVATION

A preservation request in relation to the relevant account was made by the **[insert relevant Law Enforcement Agency]** and was granted on **[insert date]** and will expire on **[insert date]** and has reference number **[insert reference number]**

IMPORTANT NOTE: Confirm preservation information for each account preserved

ASSISTANCE REQUESTED AND REQUIRED FORMAT OF EVIDENCE

Apple

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Apple Inc.

Attention: Privacy and Law Enforcement Compliance 1 Infinite Loop, Cupertino, CA 95014

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the email addresses **[insert email address]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: ***It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B***

Ask.fm

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

ASKfm

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the email addresses **[insert account identifier]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

ATlassian

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Atlassian Inc.

Attn: Legal Department
1098 Harrison Street
San Francisco, CA, 94103
USA

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the email addresses **[insert email address]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Dropbox

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Dropbox, Inc.

Attn: Legal Department 185 Berry Street,
4th Floor
San Francisco, CA
94107

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to **[insert email address associated with a Dropbox account or a Dropbox user ID]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Facebook

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Facebook,Inc.

1601 California
Avenue Palo Alto, CA
94304

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the account **[insert account identifier]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

GoDaddy

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Compliance Department GoDaddy.com, LLC
14455
North Hayden Rd., Suite 219 Scottsdale, AZ
85260

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the **[insert URLs where the hosted content is located]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Google

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Google

1600 Amphitheatre Parkway, Mountain View,
CA 94043
USA

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the email addresses **[insert email address]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Grindr

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Grindr, LLC

6725 Sunset Blvd, Suite
110 Los Angeles CA 90028-7163
facsimile: 1-310-919-1228
email: legal@grindr.com

all of the **[insert if BSI or Traffic Data and/or Content Data]** held by them relating to the email addresses **[insert email address registered to Grindr account]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Instagram

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Attn: Instagram Law Enforcement
Response Team 1601 Willow Road
Menlo Park, CA 94025

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the email addresses **[insert account identifier]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Linkedin

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

For all non-U.S. requests:

LinkedIn Ireland U.C.

ATTN: Legal Department Wilton Plaza
Wilton Place,
Dublin 2
Ireland

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the account **[insert LinkedIn public profile URL]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Microsoft

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Microsoft Corporation
1065 La Avenida, Mountain View,
CALIFORNIA 09043

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the email addresses **[insert identifier: Email Address/Microsoft Account (MSA) Phone Number ,CID or PUID, Credit Card Number, XBOX Gamertag or Serial Number]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Pinterest

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Pinterest

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the account **[insert Pin URL]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Skype

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Skype Communications SARL
23-29 Rives de Clausen
L-2165 Luxembourg

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the account **[insert identifier: Skype username/ID Skype Number, Dialed PSTN Number, 16-digit credit card number, Skype Order Number]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Snapchat

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Snapchat Inc.

Custodian of Records
Snapchat Inc.
PO BOX 1784
Pacific Palisades, CA 90272
USA

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the account **[insert account]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Surespot

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Surespot, llc.

2995 55th Street #18034
Boulder
CO 80308

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the account **[insert associated email account, account name or URL]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Tumblr

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Tumblr, Inc.

Attn: Trust & Safety
35 East 21st Street, Ground Floor
New York, NY 10010

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the account **[insert associated email account, account name or URL]** for the period commencing [**insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Twitter

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Twitter, Inc.

c/o Trust & Safety - Legal
Policy 1355 Market Street,
Suite 900 San Francisco, CA 94103
(attn: Trust & Safety - Legal Policy)

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the account **[insert username and URL]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Whatsapp

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

WhatsApp Inc.

1601 Willow Road
Menlo Park, California 94025 United States of America
Attention: WhatsApp Inc., Law Enforcement Response Team

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to [**insert WhatsApp identifier]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Wikr

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Wickr Inc.

Attn: Legal Department
20 California street
#250
San Francisco, CA 94111

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the email addresses **[insert Wikr identifier]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Wordpress

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Automattic Inc.

132 Hawthorn St
San Francisco,
CA 94107
Attn: General Counsel

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the article **[insert article name and URL]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B

Yahoo

After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain from an administrator at:

Yahoo Inc.!

Compliance Team
01 First Avenue
Sunnyvale, Mountain View,
CALIFORNIA 94089

all of the **[insert if BSI, Traffic Data and/or Content Data]** held by them relating to the email addresses **[insert Yahoo identifier]** for the period commencing **[insert date]** to **[insert date]**

Confirm the format of the electronic evidence – for example: It is requested that these records be produced as exhibits in a statement together with an explanation of the technical terms used in the records. A blank statement is attached in Annex B.

INSERT FOR ALL REQUESTS

It is further requested that:

1. Such other enquiries are made, persons interviewed and exhibits secured as appear to be necessary in the course of the investigation.

2. Any records are produced as exhibits in any statements together with an explanation of the technical terms used in the records.
3. Any information held on computer in any form be preserved and secured from unauthorised interference and made available to the investigating officers and the [Insert Agency Prosecuting/Investigating Judge/Examining Magistrate] for use at any subsequent trial.
4. Any material provided to me pursuant to this request may be used in any criminal prosecution or other judicial proceedings connected with this matter, including any other restraint or confiscation proceedings and ancillary proceedings relating thereto including proceedings relating to any breaches of, variation of, reassessment of, or enforcement of court orders.
5. The above enquiries are made and that permission be given for the original or signed and certified copies of any statements made and documents or other items secured during the course of the enquiries to be removed to the [Insert Requesting State] for use in any criminal proceedings, trial, confiscation and enforcement proceedings.
6. Insert if required: The investigator is granted permission to travel and attend the sift of the evidence obtained from the Service Provider and before transmission.

Reciprocal Procedural Laws (only include if there are reciprocal laws)

I confirm that the assistance requested above may be obtained under current **[Insert Requesting State]** law if in a like case a request for such assistance were made to the authorities in **[Insert Requesting State]**

Transmission of Electronic Evidence

It is requested that any electronic evidence or other correspondence are sent to me at the above address and that you notify me as to any need to return any documents at the conclusion of the proceedings in **[Insert Requesting State]**

Contacts

The appropriate person to contact in the event of any query about this request is the **[insert case lawyer/investigative/examining judge as appropriate]**

Name: **[insert name]**

Address: **[insert]**

Email: **[insert]**

Direct telephone number: + **[insert]**

Fax number: + **[insert**]

or the Investigator **[insert name]**

on telephone number: + **[insert]** or by e-mail at **[insert].**

I would be grateful if you would keep the [Insert prosecutor/investigating or examining magistrate name] and Investigator generally informed as to the progress of this request.

I extend my thanks in anticipation of your valued co-operation and assistance in this matter.

Yours faithfully,

ANNEX Bii: Model MLAR for real-time collection of traffic data or content

Address of Central Authority

Dear Sir or Madam

MUTUAL LEGAL ASSISTANCE REQUEST:

[insert Operation name]

[insert Name of Accused/s or Suspect/s]

URGENCY

[Please consider if the request is truly urgent – over use can cause difficulties and delays other cases – if so confirm reasons e.g. threat to life or serious physical harm]

I am **[insert name]** a **[insert title]** of the **[insert name of Agency]** and I am empowered to make this request for evidence pursuant to **[insert relevant domestic law]**

BASIS OF THE REQUEST

I have the honour to request your assistance under the provisions of **[insert relevant Treaty of Mutual Legal Assistance in Criminal Matters]**

CONFIDENTIALITY

In order not to prejudice the investigation, I request that no person (including any of the subjects) is notified by the competent authorities in your country of the existence and contents of this Mutual Legal Assistance Request and any action taken in response to it. I further request that action is taken to ensure that any person from whom evidence is sought does not so notify any other person.

If the above subjects or an associated party became aware of the existence of this request **[or]** sensitive material, namely **[identify the sensitive material – either the entire request or confirm the relevant part] [or]** of action taken in response to it, it is reasonably justifiable to believe that disclosure of the fact of an investigation to the subjects will result in **[insert as appropriate for example destruction of evidence]** as supported by **[describe conduct in support i.e. deletion of accounts]**

If it is not possible to preserve confidentiality in the above manner, please notify me prior to executing this Mutual Legal Assistance Request.

PURPOSE OF THE REQUEST

This is a request for real-time collection of traffic data OR real-time collection of content **[Important Note: Real-time collection of content not available through MLA in the U.S.]** and the evidence will be used in the prosecution (including any related restraint, confiscation and enforcement proceedings and any related ancillary proceedings) of the following

[insert if suspects/accused known]

SUBJECT	DATE of BIRTH	PLACE of BIRTH	NATIONALITY	ADDRESS

The above are the subject of a criminal investigation being conducted by **[insert name of investigating Law Enforcement Agency]** and a criminal prosecution being conducted by the **[Insert relevant Agency]** for offences of **[insert offences, relevant statute and maximum sentences].**

OR

The **[insert name of investigating Law Enforcement Agency]** is attempting to identify individuals involved in **[insert criminality]**. This evidence will be used in any subsequent prosecution of these individuals (including restraint, confiscation and enforcement proceedings and any related ancillary proceedings) who are committing offences associated with the **[insert name of software]** and its variants namely: **[insert offences, relevant statute and maximum sentences]**

[insert if only email address or social media username known]

This is a request for the competent authorities in the **[insert Requested State]** to provide evidence related to the email address listed below for use in Court Proceedings within the jurisdiction of **[insert Requesting State]**

EMAIL ADDRESS or SOCIAL MEDIA USERNAME	SERVICE PROVIDER (name and address)

The **[insert name of investigating Law Enforcement Agency]** is attempting to identify the user of the **[insert Service Provider]** and obtain the material more particularly detailed in the Assistance Required paragraph below. This evidence will be used in any subsequent prosecution of the individual/s (including restraint, confiscation and enforcement proceedings and any related Ancillary proceedings) who are committing offences associated with the **[insert email address]**: **[insert offences, relevant statute and maximum sentences]**

THE RELEVANT LAW

Please find appended to this Mutual Legal Assistance Request the applicable Law at Annex A.

SUMMARY OF FACTS AND HISTORY OF PROCEEDINGS

Example:

Mr X has created a false identity in the name of "Mr Z" and is believed to be part of a proscribed organisation "War on All". It can also be shown (see statement of Officer X at Annex A) that Mr X, in the name of "Mr Z", has set up three websites on the Internet, which contain Jihadi Videos from the war in Syria.

Mr X has been using a laptop computer, which is owned by a company for whom he used to work. The Police have discovered an email account (X@SP.com) on the computer that is linked to Mr X through service of domestic legal process and receipt of the following basic subscriber information: [name and address]

The email has been used as a contact, which was used to create the websites referred to above as detailed in the statement of Officer X in Annex B.

A recipient of an email from Mr X reported to the police that he had sent her an email to encourage her to fight in Syria and to "bring Jihad home" (see statement of Miss S at Annex C and copy emails from Mr X at X@SP.com)

Mr X is known to use the Web and Coffee Cybercafe in Madeuptown under surveillance by Madeuptown Police. Observation by officers of the screens show Mr X accessing jihadi videos (see statements of Officer K and J at Annex D) and this is supported by the owner of the Web and Coffee Cybercafe (see Statement of Mr G in Annex E).

It is believed that monitoring the live traffic data on X@SP.com from Mr X will assist the enquiry and reveal who Mr X is sending links to of the jihadi websites that are being used to promote the war in Syria, encourage persons to travel to fight for proscribed organisations and to "bring jihad home" to Madeuptown.

OR The live monitoring of the content of the communications in x@SP.com will also show who Mr X is working with and whether he and others have had any discussions about their plans in relation to bring Jihad to their home.

ASSISTANCE REQUESTED AND REQUIRED FORMAT OF EVIDENCE

After obtaining any appropriate warrant, court order or other order monitor the following account **[insert account identifier i.e. x@SP.com]** registered with [**confirm name and address of SP for service of any warrant or other court order]** and collect all traffic or

content data to and from the account from **[insert date]** to **[insert date]**

Also include the following:

1. **Confirmation that a lawful interception order or warrant has been issued domestically in connection with a criminal investigation, if such an order or warrant is required by law**
2. **If possible, the provision of sufficient technical data, in particular the relevant network connection number, communications address or service identifier to ensure that the request can be met**
3. **Confirmation if a live feed required or recordings provided with supporting statements/affidavits**
4. **Consider if a request should also be made for historical data as well (using model paragraphs from MLAR in Annex E for Stored Electronic Evidence)**

It is further requested that:

1. Such other enquiries are made, persons interviewed and exhibits secured as appear to be necessary in the course of the investigation.
2. Any records are produced as exhibits in any statements together with an explanation of the technical terms used in the records.
3. Any information held on computer in any form be preserved and secured from unauthorised interference and made available to the investigating officers and the **[Insert Agency Prosecuting]** for use at any subsequent trial.
4. Any material provided to me pursuant to this request may be used in any criminal prosecution or other judicial proceedings connected with this matter, including any other restraint or confiscation proceedings and ancillary proceedings relating thereto including proceedings relating to any breaches of, variation of, reassessment of, or enforcement of court orders.
5. The above enquiries are made and that permission be given for the original or signed and certified copies of any statements made and documents or other items secured during the course of the enquiries to be removed to the **[Insert Requesting State]** for use in any criminal proceedings, trial, confiscation and enforcement proceedings.
6. Insert if required: The investigator is granted permission to travel and attend during the real-time collection.

Reciprocal Procedural Laws (only include if there are reciprocal laws)

I confirm that the assistance requested above may be obtained under current **[Insert Requesting State]** law if in a like case a request for such assistance were made to the authorities in **[Insert Requesting State]**

Transmission of Documents

It is requested that any documents or other correspondence are sent to me at the above address and that you notify me as to any need to return any documents at the conclusion of the proceedings in **[Insert Requesting State]**

Contacts

The appropriate person to contact in the event of any query about this request is the **[insert case lawyer/investigative/examining judge as appropriate]**

Name: **[insert name]**

Address: **[insert]**

Email: **[insert]**

Direct telephone number: + **[insert]**

Fax number: + **[insert**]

or the Investigator **[insert name]**

on telephone number: + **[insert]** or by e-mail at **[insert].**

I would be grateful if you would keep the [Insert prosecutor/investigating or examining magistrate name] and Investigator generally informed as to the progress of this request.

I extend my thanks in anticipation of your valued co-operation and assistance in this matter.

Yours faithfully,

ANNEX C: MLAR checklist

Operation Name:	
Subjects: 1. 2. 3. 4.	
Reference:	
Have alternatives to an MLA been assessed by the prosecutor	Can the electronic evidence requested be obtained through a Direct Request to the SP ☐ Yes ☐ No Is there or has there been an investigation in the Requested State allowing sharing of evidence on a *police-to-police* basis ☐ Yes ☐ No Can the electronic evidence be obtained through user consent ☐ Yes ☐ No Can relevant user download own content ☐ Yes ☐ No
Correct Opening Paragraph I am **[insert name]** of the, **[insert name of Agency]** a designated authority, and I am empowered to make this request for evidence pursuant to section **[insert section]** of the **[insert name of Act]**	☐ Yes ☐ No
Correct Treaty Reference **For example**: I make this request pursuant to Article 18 of the UN Convention against Transnational Organized Crime, and the Protocols thereto done at Palermo in 2000 and ratified by x on x **Or insert relevant bilateral or multilateral Treaty**	☐ Yes ☐ No
Urgency If an urgent request provide details of why (e.g. imminent trial date, facts included to support serious risk of harm) and any dates when the evidence is required by.	Is this an Urgent MLAR ☐ Yes ☐ No **If Yes** are there sufficient reasons stated in the MLAR ☐ Yes ☐ No Confirm further detail required if insufficient reasons:

Confidentiality If notification to the account holder and/or disclosure (i.e. sealing) of the application to the public would prejudice the investigation – include this section and reasons why notification or disclosure to the public would hamper the investigation e.g. destruction of evidence or suspect would flee. **Please note** that if the application is sealed in the U.S. this will be limited to 2 years and further grounds will have to be provided to extend.	Required ☐ Yes ☐ No Are reasons clearly included to justify confidentiality ☐ Yes ☐ No Is the correct paragraph used: In order not to prejudice the investigation, I request that no person (including any of the above subjects) is notified by the competent authorities in your country of the existence and contents of this MLAR and any action taken in response to it. I further request that action is taken to ensure that any person from whom evidence is sought does not so notify any other person. If the above subjects or an associated party became aware of the existence of this request **[or]** sensitive material, namely **[identify the sensitive material – either the entire request or confirm the relevant part] [or]** of action taken in response to it, it is reasonably justifiable to believe that disclosure of the fact of an investigation to the subjects will result in **[insert as appropriate** destruction of evidence as supported by **[describe conduct in support i.e. deletion of accounts]**; disclosure of the identity of the confidential informant has the potential to place his life in danger or risk of serious injury **[describe conduct in support i.e. if informant close to subject and subject has a history of violence]** If it is not possible to preserve confidentiality in the above manner, please notify me prior to executing this MLAR. ☐ Yes ☐ No
Purpose of the Request	Is this set out clearly i.e. insert type of evidence e.g. content of emails from Google or real-time collection of traffic data from Yahoo! ☐ Yes ☐ No Does the MLAR state that the evidence will be for use in the prosecution (including any related freezing, confiscation and enforcement proceedings and any related ancillary proceedings) ☐ Yes ☐ No Are all subjects listed: ☐ Yes ☐ No With: Full name ☐ Yes ☐ No Date of Birth ☐ Yes ☐ No Place of Birth ☐ Yes ☐ No Nationality ☐ Yes ☐ No If subject details not known is there sufficient information provided (for example IP address, hosting company, email address, username) ☐ Yes ☐ No Confirm further details required:

Law	Are the offences each suspect/defendant has been charged with listed ☐ Yes ☐ No N/A If pre-charge are the offences being investigated listed ☐ Yes ☐ No N/A Is the relevant section and legislation listed for each offence ☐ Yes ☐ No Is the maximum sentence for each offence provided ☐ Yes ☐ No Is the relevant legislation for each offence provided in an annex to the MLAR ☐ Yes ☐ No Do the offences have a maximum sentence to satisfy a Requested State's de minimis requirements where relevant (e.g. U.S.) ☐ Yes ☐ No If an offence related to terrorism is the terrorist organisation proscribed under law ☐ Yes ☐ No
Factual Summary The summary of facts must be relevant to the required assistance. Therefore, provide facts to show a crime has been committed but **not** a summary of the complete investigation. Include those facts that are relevant to the evidence required. Also confirm the source of any supporting facts e.g. if attribution determined through admission or consent confirm the source	Is there a brief chronology of the investigation/proceedings to date (i.e. insert when arrested, charged, and when any trial date is fixed if known) ☐ Yes ☐ No If a counter-terrorism investigation/prosecution reference to proscribed organisation contrary to national law or a sanctions list ☐ Yes ☐ No If only Basic Subscriber Information (BSI) requested has a Direct Request been attempted to obtain the evidence from the SP ☐ Yes ☐ No N/A If No confirm reasons: If MLAR required is there sufficient supporting information to show that BSI is relevant and related to the offences being investigated/ prosecuted ☐ Yes ☐ No N/A If only traffic data requested has a direct request been attempted to obtain the evidence from the SP ☐ Yes ☐ No N/A If No confirm reasons: If MLAR required is there sufficient supporting information to show that traffic data is relevant and material (specify date range – with justification why relevant and material to investigation) ☐ Yes ☐ No N/A **If an MLAR is required for content data, traffic data or real-time collection has the author:** Provided facts to attribute each account to the user ☐ Yes ☐ No If answered No - list accounts where attribution is still required: **MLARs to the U.S. for stored Content Data** **Probable Cause** **Note:** *If multiple accounts requested confirm for each account*

	Detailed the type of content to be seized (e.g., an email communication) ☐ Yes ☐ No Provide the reason why the content data is relevant to the criminal offence being investigated. ☐ Yes ☐ No Provide specific facts of the types of communications or specific examples supporting the belief that the content data sought will be found among the records of the Service Provider ☐ Yes ☐ No Provide specific facts and their source to support the belief that the content data relates to a crime. ☐ Yes ☐ No If source of information has a criminal record or is anonymous – has further information been provided to show credibility and reliability ☐ Yes ☐ No N/A Has the date range for content data been provided and justified on the facts (i.e. probable cause for the time-span requested) ☐ Yes ☐ No **MLARs to other States for Stored Content Data** **If Legal Standard Reasonable Grounds to Believe** **Note:** *If multiple accounts requested confirm for each account* Detailed the type of content data to be seized (e.g., an email communication) ☐ Yes ☐ No Provide supporting information of the types of communications or specific examples supporting the belief that the content data sought is stored by the Service Provider ☐ Yes ☐ No Provide the reason why the content data is relevant and material to the criminal offence being investigated. ☐ Yes ☐ No Provide information to support the belief that the information in support is credible ☐ Yes ☐ No Has the date range for content data been provided and the time-span justified on the facts ☐ Yes ☐ No **For real-time collection** **Note:** *If multiple accounts requested confirm for each account* Does the law in the Requested State allow for real-time collection? (e.g. U.S. law does **not** allow for an MLAR for real-time collection of content data) ☐ Yes ☐ No

	Sufficient supporting information to show the real-time collection is relevant to the investigation (e.g. will show the location of an offender or disclose incriminating messages) ☐ Yes ☐ No Provide information to support the belief that the information in support is credible ☐ Yes ☐ No Why other investigative methods have not and/or will not secure the evidence requested ☐ Yes ☐ No How collateral intrusion (i.e. invasion of privacy of persons not connected to the investigation) will be avoided ☐ Yes ☐ No Specific date range for the real-time collection – with justification why that time-span is relevant and material to investigation) ☐ Yes ☐ No
Preservation If an account isn't preserved there will be no certainty there is stored electronic evidence to seize and the MLAR will not be executed. The preservation reference is needed so the relevant court process matches the SP account and the evidence required.	Are all relevant accounts preserved ☐ Yes ☐ No Is the date of preservation included ☐ Yes ☐ No Is the expiry date of preservation included ☐ Yes ☐ No Is the reference number of preservation included ☐ Yes ☐ No

Assistance Requested	Is a paragraph included to confirm the following: After obtaining any appropriate subpoena, search warrant, court order or other order, to obtain a witness statement in writing from an administrator at **[insert SP]** ☐ Yes ☐ No Is the correct address of the SP included ☐ Yes ☐ No Is the username/URL/email account/social media account identifier confirmed ☐ Yes ☐ No **For stored Content Data** Is the required date range confirmed ☐ Yes ☐ No Is the required date range correct? ☐ Yes ☐ No If no confirm reasons: Does the MLAR confirm what type of stored electronic evidence is required for each account (i.e. BSI and/or traffic data and/or content data)? ☐ Yes ☐ No Does the list of required evidence list the electronic evidence required for each account according to what is available from each SP ☐ Yes ☐ No If No confirm evidence that still needs to be requested: **For real-time collection** Does the MLAR provide sufficient technical data, (i.e. the relevant network connection number) to ensure that the real-time collection is possible? ☐ Yes ☐ No Does the MLAR confirm that a lawful interception order or warrant has been issued domestically in connection with a criminal investigation, if such an order or warrant is required by law ☐ Yes ☐ No Does the MLAR confirm the date range for the real-time collection ☐ Yes ☐ No Does the MLAR confirm if live transmission and/or recordings are requested ☐ Yes ☐ No **General** Is there a catchall paragraph re any other enquiries arising from the MLAR ☐ Yes ☐ No
Form in which electronic evidence is requested	Does the MLAR have a request for the electronic evidence to be produced according to the procedure of the Requesting State ☐ Yes ☐ No Is a model format attached to the MLAR ☐ Yes ☐ No

Reciprocity	Is reciprocity a requirement for MLA with the Requested State ☐ Yes ☐ No **If Yes** is the following standard paragraph included: I confirm that the assistance requested above may be obtained under current law of **[insert name of Requesting State]** if in a like case a request for such assistance were made to the authorities in **[insert name of Requesting State]** ☐ Yes ☐ No
Transmission of Evidence	Is the following standard paragraph included: It is requested that any documents or other correspondence are sent to me at the above address and that you notify me as to any need to return any documents at the conclusion of the proceedings in **[insert name of Requesting State]** ☐ Yes ☐ No
Confirmation of Approval	Can this MLAR be approved ☐ Yes ☐ No If no - detail further action required *(Use a separate sheet if necessary)*: 1. 2. 3. 4. 5. Additional sheet required ☐ Yes ☐ No Date to re-submit Signature: Date Print Name: Grade:

ANNEX D: Legal Instruments

Budapest Convention on Cybercrime (ETS No.185)

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

As of August 2018, 58 States have ratified the convention, while a further four states had signed the convention but not ratified it.[49]

The Budapest Convention Parties maintain a 24/7 Network[50] to enable effective investigation and preservation of evidence.[51]

Relevant provisions for MLA include:

Article 25 provides that the Parties shall co-operate with each other to the widest extent possible for the purposes 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

Article 31 allows a Requesting State to request another Party to search, access, seize, secure and disclose electronic evidence stored there

Article 33 provides for the real-time collection of traffic data

Article 34 provides for the real-time collection of content data

Official texts in English and French

(Also available in German, Russian and Arabic)

Additional Protocol

Signatures and Ratifications

49. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Sv9dObc4
50. Article 35
51. See Explanatory Report to the Convention on Cybercrime, No. 298

Reservations and Declarations

Explanatory Report

The League of Arab States Convention on Combating Information Technology Offences

The Arab Treaty on Countering Information Technology Offences ('CITO') was adopted in December 2010 and entered into force in February 2014. To date Algeria, Jordan, UAE, Sudan, Iraq, PA, Qatar, Kuwait and Egypt have ratified CITO.

Dual criminality is an essential prerequisite to the provision of any mutual legal assistance under Article 32(5) between CITO member states.

Significant provisions include the disclosure of information under Article 33[52] by law enforcement to another party to CITO that can be used proactively by a Requested State.

There are no provisions for the real-time collection of traffic data or content through MLA.[53]

There is also provision under Article 43 for a, "…*specialized body dedicated 24 hours a day to ensure the provision of prompt assistance for the purposes of investigation, procedures related to information technology offences or gather evidence in electronic form regarding a specific offence.*"

African Union Convention on Cyber Security and Personal Data Protection

In July 2014 the African Union adopted the Convention on Cybersecurity and Personal Data Protection.

The Convention does not provide for the full set of procedural powers for investigating and prosecuting cybercrime and securing electronic evidence in domestic investigations – for example production orders, which are crucial to obtain data from SPs are not included.[54] Further, the AUC does not constitute a legal basis for international cooperation to secure electronic evidence.[55]

Official texts in English, French, Arabic and Portuguese

Status Table

52. Consistent with Article 26 of the Budapest Convention
53. Articles 33 and 34 of the Budapest Convention
54. Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime 20 November 2016
55. Ibid

ANNEX E: Model direct request form for voluntary disclosure

Text in black precedent wording

Text in red guidance notes

Insert name of person making the request Insert name of agency/judicial authority : Insert telephone number with international codes : Insert official email address	

DIRECT REQUEST to INSERT SP For VOLUNTARY DISCLOSURE	
1. Introduction	I, insert name, rank, any badge or other identifying reference of officer, prosecutor or judicial authority making the request am investigating the following offences: List criminal offences and confirm contrary to which law
2. Authorisation	Acting with the authorisation of insert name and title (e.g. Prosecutor/ Investigating Judge or Senior Officer) OR Attach domestic legal order to produce BSI and/or traffic data (**Check SP Law Enforcement Guidelines to confirm if domestic legal order must be attached)**
3. Name and contact details of the SP	Make a Direct Request to insert name of Service Provider
4. Confirm account data requested for	For voluntary disclosure of data for insert identifier for account The information below is made available to you to assist with disclosing the required data IP address…… Telephonenumber…… Email address…… IMEI number…… MAC address…… Person(s) whose data is being requested…… Name of the service: …… Please note that (tick and complete if applicable): ☐ The requested data was preserved in accordance with an earlier request for preservation issued by …… (indicate the authority, and, if available, the date of transmission of request and reference number) and transmitted to ……..…… (indicate the service provider/ legal representative/ public authority to which it was transmitted and, if available, the reference number given by the addressee)

5. Confirm specific data requested and date range	**Basic Subscriber Information**, including but not limited to (tick and complete if applicable): ☐ Name, address, date of birth, contact information (email address, phone number) and other information pertaining to the identity of the user/ subscription holder ☐ Date and time of first registration, type of registration, copy of a contract, means of verification of identity at the moment of registration, copies of documents provided by the subscriber ☐ Type of service, including identifier (phone number, IP address, SIM-card number, MAC address) and associated device(s) ☐ Profile information (user name, profile photo) ☐ Data on the validation of the use of service, such as an alternative email address provided by the user/subscription holder ☐ Debit or credit card information (provided by the user for billing purposes) including other means of payment **Traffic Data**, including but not limited to: For internet (tick and complete if applicable): ☐ IP connection records / logs for identification purposes ☐ Routing information (source IP address, destination IP address(es), port number(s), browser, email header information, message-ID) ☐ Base station ID, including geographical information (X/Y coordinates), at the time of initiation and termination of the connection ☐ Volume of data For web hosting (tick and complete if applicable): ☐ Logfiles ☐ Tickets ☐ Purchase history ☐ Other traffic data, including but not limited to: ☐ Prepaid balance charging history ☐ Contacts list Date Range: Insert date range requested – be realistic!
6. Confirm contact details for digital data transmission and due date	Replies must be sent by email to : Insert email address for transmitting the requested electronic evidence to and due date
7. Confirm User NOT to be notified of request	DO NOT INFORM THE ACCOUNT USER OF OUR REQUEST. If specific reasons for not notifying confirm here (i.e on-going investigation that could alert the suspect leading to destruction of evidence or avoiding possible arrest) Also confirm that there will be no prejudice caused to the suspect through this request Also confirm any law enforcement requirements imposing confidentiality if relevant
8. Confirm if a statement or affidavit is required to authenticate the requested data (if not self authenticating)	We request that a statement or affidavit is provided authenticating the electronic evidence requested to confirm that you are the custodian
9. Closing	I confirm I have the required legal authority to submit this request – please contact my telephone number or email address if any further information is required Insert Name, date and any official stamp of the agency requesting and authorising officer/prosecutor or judicial officer

ANNEX Ei: APPLE Government / Law Enforcement Information Request

Apple's Legal Process Guidelines for Government & Law Enforcement outside the United States are available at:

https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf

Government / Law Enforcement Officers should transmit requests to the relevant email address for their geographical region, which may be found in the above-mentioned guidelines.

Apple will not process a Government or Law Enforcement Information Request unless it is received from the requesting officer's official government or law enforcement email address.

Government or Law Enforcement Agency	**Country** ..... **City/State/Province** ..... **Agency Name** .....
Requesting Officer	**Name & Title/Rank** ..... **Official Government or Law Enforcement Email Address** ..... **Phone** .....
Case Context	**Case Date & Location** ..... **Case Type & Overview** .....

Information Context

- **Information Supporting Request** (Examples: Apple Device Serial/IMEI Number; Apple ID; Email Address; Phone Number; Physical Address; Person Name):
- **Information Requested from Apple** (Note: Information requested should be as narrow as possible relative to the case context):
- **Legal Basis & Purpose** (please provide the legal basis for your request and the purpose for which any information provided by Apple will be used):

ANNEX F: Simplified uniform request for preservation and emergency: disclosure requests

For a copy of the PDF form please contact EuroMed Police

Date

Requête urgente / emergency request

Requête de gel / preservation request

Pays / Country

Service / Service

Unité / Unit

Numéro de téléphone / Telephone number

Réseau social / Social Media

Adresse de la société / Company's address

Tribunal / Court

Numéro de dossier / Legal proceedings

Identifiant de l'usager (ID) / Identification number

Type de délit / Type of crime

Localisation de l'objectif / Target location

Type d'information sollicitée / Type of information request

Avis de Confidentialité / Confidentiality notice

Pour les requêtes urgentes

Explication de l'urgence / Description of the emergency (danger de mort ou danger physique / death or physical injury threat)

Type de données nécessaires pour éviter le danger / Type of data needed to prevent the emergency

Identifier un individu inconnu / Identify an unknown individual

Localiser un individu connu / Locate a known individual

Autres / other

Pourquoi le processus normal de requête est insuffisant et qu'une procédure d'urgence est nécessaire?/ Why is the normal disclosure process to obtain the information insufficient?

Comment le profil de notre société est relié à l'enquête? / How is the company's identifier listed above connected to the emergency?

Publication directe sur un profil appartenant à notre société. / Did the subject under investigation made the statement using a product of another company?

Présence d'un profil sur une publication d'une autre société. / Insert any statement related to the emergency originated from another company

URL

Screenshots :

ANNEX Fi: GOOGLE emergency disclosure request form

This form is to assist Google in determining whether there is sufficient justification to establish a good faith belief that disclosing data without delay is necessary to avert a threat of death or serious physical injury to a person, as set forth in 18 U.S. C. § 2702(b)(8) & (c)(4). This form must be completed by an authorized law enforcement official.

Please be sure to: (a) specify the user by the appropriate product identifier (e.g., Gmail address, YouTube URL or Google Voice number), (b) answer all questions, (c) sign as indicated below (initial any additional pages submitted), and (d) return the completed signed form and supporting materials either by email from an official email address of your agency to EDRLawEnforcement@google.com, or by fax with a cover letter on your agency's official letterhead to +1-650-469-0276.

1. Provide a detailed explanation of the emergency, including how the threat involves the risk of death or serious physical injury to a person and when the harm may occur:
2. What type of data do you need to help prevent the emergency?
   Information to help identify an unknown individual (e.g., name, phone number) information to help locate a known individual (e.g., recent IP activity, location coordinates) Other *(please explain)*:
3. What is the Google identifier (e.g., Gmail address, YouTube URL, Voice number) that you are investigating?
4. Why is the normal disclosure process to obtain the information insufficient to address the emergency you described above?
5. How is the Google identifier listed above connected to the emergency? Please **check** the most appropriate box:

   The subject under investigation made the statement using a Google product (e.g., the subject sent a threatening Gmail message).

   - If the subject sent a Gmail email message, please provide the email text and expanded headers (see #7 below)
   - If the subject made the statement on another Google product please provide the URL of the blog post, YouTube video URL, etc.

   A statement related to the emergency originated from another company (e.g. Twitter, Facebook, askFM), but there is a link to a Google user (e.g., the subject made a threat on Twitter, and provided a Gmail address when creating a Twitter account). Please provide supporting documentation (see #7 below).

   You believe that a person related to the emergency is using a Google product. Please explain this person's connection to the emergency and how you obtained the identifier:

   Other (*please explain*):

6. Specify the exact information you are requesting from Google Inc. (e.g. subscriber information, IP login address, etc.)

7. Provide supporting documentation (as described in #5):

   If the emergency relates to an email or message, please provide a copy of the email (with full headers if available) or message, or a URL to the message if it was posted on a public forum. You may find the following Gmail Help pages useful in obtaining and reading email headers: https://support.google.com/mail/answer/22454

   https://support.google.com/mail/answer/29436

   If you identified the Google Account based on information provided by another company (e.g., Facebook, Twitter), please list any other user information from the company's records (for example, name, phone number, IP address) and/or provide us with a copy of the production from the other company. Because many companies allow users to provide unverified email addresses during account creation, this additional information will help us determine whether the information from Google is related to your emergency.

If you are submitting this form outside of normal business hours (9am-5pm Pacific Time Monday through Friday) and you have not already spoken to Google Legal Support regarding this matter, you may call +1-650-417-9011 and leave a message, as faxes and emails are only reviewed during normal business hours.

Printed Name: .....

Designation/Title: .....

Agency: .....

Email: .....

Phone: .....

Fax: .....

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that I am a sworn government official.

_____ _____

Signature Date of Execution

ANNEX Fii: APPLE emergency government / law enforcement information request

Apple considers a request to be an emergency request when it relates to circumstance(s) involving imminent and serious threat(s) to:

8. the life/safety of individual(s);

9. the security of a State;

10. the security of critical infrastructure/installation(s).

Apple will not process a request on an emergency basis unless it relates to circumstance(s) as outlined above and this form is fully completed by the requesting officer and transmitted from the officer's official government or law enforcement email address to the mailbox: exigent@apple.com with the subject line: "Emergency Request".

Government or Law Enforcement Agency	**Country** ..... **City/State/Province** ..... **Agency Name** ..... **Agency Phone:** .....
Requesting Officer	**Name & Title/Rank:** ..... **Official Government or Law Enforcement Email Address:** ..... **Office Phone:** ..... **Mobile Phone:** .....

Supervisory Officer	As requesting officer, I acknowledge and understand that if Apple produces responsive information to this Emergency Government & Law Enforcement Information Request, my supervisor, whose name and contact details I have provided below, may be contacted and asked to confirm to Apple that the request relates to a legitimate emergency circumstance. **Supervisor's Name & Title/Rank**: ..... **Supervisor's Official Government or Law Enforcement Email Address**: ..... **Supervisor's Office Phone**: .....
Requesting Officer Confirmation	By providing electronic initials here_____, I, the requesting officer, confirm I completed this form in my capacity as an authorized government/law enforcement official and the information provided in it is true and correct to the best of my knowledge and belief.
Case Context	**Emergency Incident Date & Location**: ..... **Emergency Incident Overview** .....
Information Context	**Information Supporting Request** (Examples: Apple Device Serial/IMEI Number; Apple ID; Email Address; Phone Number; Physical Address; Person Name): ..... **Information Requested from Apple** (Note: Information requested should be as narrow as possible; the more information requested, the longer it will take to search for and produce relevant responsive information): ....

ANNEX G: Law and procedure in SPCs

Algeria

Algeria has ratified CITO - Article 32 ensures that it can be used as an instrument to facilitate MLA and provides for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and disclosure of stored data and traffic data to States that have also ratified CITO.

Procedural Power	National Legislation	Comments
Search and Seizure	**Law No. 09-04 of 14 Chaâbane 1430 corresponding to 5 August 2009 laying down specific rules on the prevention and the fight against infringements related to information and communication technologies** **Articles 3, 4, 5 and 6**	Article 3 allows for search and seizure of content data in a computer system or computer storage system Article 4 restricts the search and seizure provisions to certain categories of offence (that include terrorism offences) – this means that many cybercrimes that are not crimes against national security or terrorist related will not have relevant procedural powers to search and seize content data. Article 6 ensures the copying and integrity of any evidence seized. Article 5 refers to the '*requisition*' of an individual to assist with information regarding the operation of the computer system or protection of the data.
Real-time collection of content and traffic data	**Law No. 09-04 of 14 Chaâbane 1430 corresponding to 5 August 2009** **Article 3** **Act n°09-04 of 05-08-2009** **Article 10** **Presidential Decree 15-261 of 08-10-2015**	Content and traffic data can be intercepted pursuant to Article 3 for all offences using a computer. Article 10 of Act n°09-04 of 05-08-2009 allows for SPs to be compelled to collect or record content data in real-time for all offences. This measure must be ordered in compliance with the provisions of the Code of Criminal Procedure upon authorization by the public prosecutor or examining magistrate. The authorization must include all the elements allowing the identification of the communications to be intercepted, the offence justifying the resort to this measure, as well as its length (4 months, renewable). This measure cannot undermine professional secrecy. There is a specific and independent power to collect traffic data real-time as provided by the provisions of Presidential Decree 15-261 of 08-10-2015 on the composition, organization and functioning of the national body for the prevention and the fight against ICT-related offences (Official journal n°53 of 08-10-2015)
Data retention obligations		SPs in Algeria have such an obligation

Procedural Power	National Legislation	Comments
Article 37 CITO: Expeditious Safeguarding of Information Stored on Information Systems	**No equivalent**	CITO allows for preservation for 60 days. Dual criminality is required unless an offence outlined in CITO Chapter II[56]
Article 40 CITO: Access to Information Technology Information Across Borders	**No equivalent**	This provision can be used to access a computer in another State with consent of the person who has legal authority to disclose the data (Article 40(2)) This procedural power is an exception to the principle of territoriality and permits unilateral trans-border access without the need for MLA where there is consent or the information is publicly available.
Preservation Requests		The standard route is for an MLAR for preservation of electronic evidence stored by SPs in Algeria through the Ministry of Justice. A country could also contact through the Interpol NCB to preserve
Voluntary Disclosure		There are no domestic provisions to allow direct requests to SPs in Algeria
Emergency Requests		Emergency Disclosure Requests can be sent via the Ministry of Justice in an urgent MLAR

Egypt

Egypt has ratified CITO and can be used as the basis for cooperation with other States that have ratified. Article 32 ensures that it can be used as an instrument to facilitate MLA and provides for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and disclosure of stored data to States that have ratified CITO. On 14 August 2018 Egypt adopted the Law 175/2018 on Combating Information Technology Crimes. The Anti-Cybercrime Law regulates activities online, and, according to official statements, it aims to complement the new press and media laws, which penalize, inter alia, unlicensed online activity and content violations, such as fake news.

56. Article 6 Illicit Access, Article 7 Illicit Interception, Article 8 Offence Against Integrity of Data, Article 9 Misuse of ICT, Article 10 Computer-related Forgery, Article 11 Computer-related Fraud, Article 12 Pornography, Article 13 Gambling and Sexual Exploitation, Article 14 Breach of Privacy, Article 15 Offences related to Terrorism, Article 16 Offences related to Organized Crime, Article 17 Copyright Offences and Article 18 Illicit Use of Electronic Payment Tools

Procedural Power	National Legislation	Comments
Search and seizure of stored computer data	**Criminal Procedure Code no. 150/1950** **Articles 95, 206 and 206 bis** **Communications Act no. 10/2003** **Articles 19 and 64** **Article 6 of Cybercrime Law (2018) stipulates:** To the competent investigating authority, as the case may be, to issue an injunction to competent judicial officials, for a period not exceeding thirty days renewable for one time, when it is useful in the appearance of the truth to commit a crime punishable under the provisions of this law, one or more of the following: 1. To control, withdraw, collect or hold data or information or information systems in any place, system, program, electronic support or computer in which they are located. The digital evidence shall be delivered to the issuer of the order, provided that this does not affect the continuity of the systems and the provision of the service, if any. 2. Research, inspection, and access to computer programs, databases and other information systems and systems for the purpose of control. 3. To order the service provider to deliver its data or information relating to an information system or technical device under its control or stored in it, as well as the data of its service users and the communications traffic carried out on that system or technical device. In any case, the competent investigative authority must be responsible. The appeal of the advanced orders before the competent criminal court shall take place in the Chamber of Counsel, in accordance with the procedures established in the Code of Criminal Procedure.	The provisions in the Criminal Procedure Code and Communications Act do not refer to computers or computer systems or other computer storage mediums – but could be used for search and seizure.

Procedural Power	National Legislation	Comments
Production Order	**Criminal Procedure Code no. 150/1950** **Articles 95, 206 and 206 bis** **Communications Act no. 10/2003** **Articles 19 and 64** **Article 6 (3) of Cybercrime Law (2018) stipulates:** 3. To order the service provider to deliver its data or information relating to an information system or technical device under its control or stored in it, as well as the data of its service users and the data traffic carried out on that system or technical device. In any case, the competent investigative authority must be responsible.	As above the provisions in the Criminal Procedure Code and Communications Act do not refer to computers or computer systems or other computer storage mediums– but can be used for production orders.
Real-time collection of Traffic Data	**Criminal Procedure Code no. 150/1950** **Articles 95, 206 and 206 bis** **Telecommunications Act no. 10/2003** **Articles 19 and 64** **Article 2 of Cybercrime Law (2018) stipulates:** **First:** Without prejudice to the provisions of this law and the Telecommunications Regulatory Law promulgated by Law No. 10 of 2003, the service providers shall comply with the following: 1. The preservation and storage of the information system log or any means of information technology, for one hundred and eighty consecutive days. Data to be stored and stored are as follows: A. Data that enables the service to identify the user. B. Data relating to the content and content of the information system in which the customer is under the control of the service provider. C. Traffic Data. D. Data communications. E. Any other data to be determined by a decision of the Board of Directors of the Authority.	The Criminal Procedure Code does not refer to conversations made through the internet or computers and the issue has not been adjudicated upon by the Egyptian Court of Cassation. As Article 19 of the Communications Act requires all information subject to interception to be provided - this could include content and traffic data. The investigative judge/or the public prosecutor (through a judicial decree issued by a judge) can issue an order to record wired and unwired conversations in certain circumstances – pursuant to Articles 95, 206 and 206 bis of the Criminal Procedure Code. The Department of Computer and Network Crimes can carry out the interception of IP addresses. Once an MLAR is received by the central authority and it is approved by the Attorney General, it is sent to the Department of information and the Egyptian Ministry of Interior, which proceeds with interception through trained police officers at the Department of Computer and Network Crimes. These officers will prepare a report about the outcome - without giving any details about the steps and technicalities of the interception.

Procedural Power	National Legislation	Comments
Real-time collection of Traffic Data	2. Maintain the confidentiality of stored data and store it, and not to disclose it without a warrant issued by a competent judicial authority, including personal data of any of its users or any data or information relating to the sites and special accounts to which such users enter or the persons and contacts with whom they communicate. 3. Secure data and information in a manner that preserves its confidentiality, not to be hacked or damaged. **Second:** Subject to the inviolability of the right of privacy guaranteed by the Constitution, the service providers and their dependents shall, in the event of the request by the **National Security Authorities** and in accordance with their needs, provide all technical possibilities that enable them to exercise their powers in accordance with the law. **Third:** The IT service providers, their agents and distributors assigned to them to market these services are obliged to obtain user data, and others are prohibited from doing so.	
Encrypted devices	**Communications Act no. 10/2003** **Article 64** **Article 22 of Cybercrime Law (2018) stipulates:** Any person who obtained, possessed, brought, sold, made available, produced, imported, issued or traded in any form whatsoever any device, equipment, tools, software, developed, modified, pass codes, codes or other similar data, without the authorization of the device or a justification of fact or law, and proved that such conduct was for the purpose of using any of them in committing or facilitate the commission of any of the crimes provided for in this law, or conceal their effects shall be liable for not less than two years imprisonment and a fine not less than three hundred thousand pounds and not exceeding five hundred thousand pounds.	Article 64 prevents the use of encrypted equipment – such as pin locked devices -and also allows for the provision of software to access encrypted services.

Procedural Power	National Legislation	Comments
Article 37 CITO: Expeditious Safeguarding of Information Stored on Information Systems	**Article 2 of Cybercrime Law (2018) stipulates:** First: Without prejudice to the provisions of this law and the Telecommunications Regulatory Law promulgated by Law No. 10 of 2003, the service providers shall comply with the following: 1. The preservation and storage of the information system log or any means of information technology, for **one hundred and eighty consecutive days.** Data to be stored and stored are as follows: A. Data that enables the service to identify the user. B. Data relating to the content and content of the information system in which the customer is under the control of the service provider. C. Traffic Data. D. Data communications. E. Any other data to be determined by a decision of the Board of Directors of the Authority.	This expedited power to retain **BSI**, **Traffic Data** and stored content is essential as part of cybercrime investigations to ensure the evidence is available for search, access, seizure and review. CITO allows for preservation for 60 days. Dual criminality is required unless an offence outlined in CITO Chapter II.[57] For SPs in Egypt Requesting States should send an MLAR to the Ministry of Justice for preservation – a Public Prosecutor will confirm if lawful
Article 38 CITO: Expeditious Disclosure of Safeguarded Users Tracking Information	**Article 6 (3) of Cybercrime Law (2018) stipulates:** 3. To order the service provider to deliver its data or information relating to an information system or technical device under its control or stored in it, as well as the data of its service users and the data traffic carried out on that system or technical device. In any case, the competent investigative authority must be responsible.	This procedural power is especially important to ensure that SPs provide data to locate the perpetrator of a crime. CITO does not define *tracking information* and it is unclear if it includes the communication's origin, destination, route, time, date, size, duration, or type of underlying service (i.e. **Traffic Data**)
Article 39 CITO: Cooperation and Bilateral Assistance Regarding Access to Stored Information Technology Information	**Article 4 of Cybercrime Law (2018) stipulates** The competent Egyptian authorities shall facilitate cooperation with their counterparts in foreign countries within the framework of ratified international, regional and bilateral agreements / conventions, or in accordance with the principle of reciprocity, by exchanging information in order to ensure that cybercrimes are avoided, and to facilitate the investigation and prosecution of such crimes. **The National Center for Computer Emergency shall be the technical point in this regard.**	This is an essential provision for an effective cybercrime investigation to ensure SPs provide **BSI, Traffic Data** and stored content data. Further, this power will require individuals and others (such as corporate entities, financial institutions and other organizations) who hold data to produce it to law enforcement authorities.

57. *Ibid*

Article 40 CITO: Access to Information Technology Information Across Borders	**See article 6 of Cybercrime Law (2018)**	This provision can be used to access a computer in another State with consent of the person who has legal authority to disclose the data (Article 40(2))
Emergency Requests	**See article 6 of Cybercrime Law (2018)**	MLAR to the Ministry of Justice for an emergency request – a Public Prosecutor will confirm if lawful before a request is made by the Police to a SP in Egypt
Voluntary Disclosure	**See article 4 of Cybercrime Law (2018)**	There are no domestic provisions to allow direct requests to SPs in Egypt
The Admissibility of Digital Evidences before Egyptian Courts	**Article (11) of Cybercrime Law (2018) stipulates:** Evidence derived from or derived from hardware, equipment, media, electronic supports, information system, computer software, or any means of information technology should have the same value and authenticity of physical forensic evidence [before Egyptian courts] so far as the collection of such evidences satisfied the technical requirements contained in the executive regulations of this law.	

Israel

Israel has ratified the BC and Article 25 ensures that it can be used as an instrument to facilitate MLA. The International Legal Assistance Law 5758-1998 Section 8(b) provides that MLARs can only be executed in Israel if the investigative provision is permissible under Israeli Law. The National Cyber Center at Lahav 433 (NCC) operates as required by the BC as part of the 24/7 Network. The following table confirms the domestic law:

Procedural Power Pursuant to Budapest Convention	National Legislation	Comments
Article 19 BC - **Search and seizure of stored computer data**	**Criminal Procedure (Arrest and Search) Ordinance [New Version], 5729 – 1969** **Section 23A** **Penetration of computer material** **Section 32** **Power to seize objects**	Section 23A allows for the '*penetration of a computer material - within its meaning in section 4 of the Computers Law 5755-1995*' Section 32 provides that a policeman may seize an '*object*' that includes '*computer material*' Section 1 defines an *object* to include '*computer material as defined by the Computers Law 5755-1995*'

Procedural Power Pursuant to Budapest Convention	National Legislation	Comments
Article 29 BC – **Expedited preservation of stored content data**	**Criminal Procedure Law (Communication's Data) (2007)** **Article 3 and 4** **Criminal Procedure Ordinance (Arrest and Search) (1969)** **Article 43**	Article 3 and 4, of the Criminal Procedure Law (Communications Data) (2007) provides for preservation of communication's data Article 43 of the Criminal Procedure Ordinance (Arrest and Search) (1969) provides for preservation of any other computer data. Preservation requests are sent to the National Cyber Center at Lahav 433 (NCC) as part of the 24/7 Network. There must be a criminal offence at the basis of the investigation and confirmation the requested action is necessary and cannot be obtained via domestic investigative measures in the Requesting State
Article 30 BC **Expedited preservation and partial disclosure of traffic data**	**Procedure Law (Enforcement Powers - Communication Data), 5768-2007, article 4**	Article 4 provides the ground to request preservation in circumstances of emergency. In other circumstances the Israel police will base its request on the Budapest Convention.
Article 31 BC – **Disclosure of stored content data**		This should be requested via a formal Request for Mutual Legal Assistance
Article 33 BC – **Real time collection of traffic data**	**Criminal Procedure Law (Communication's Data) (2007)** **Article 3(g)** **Communications Law (1982)** **Article 13(b)(2)**	Article 3(g) to the Israeli Criminal Procedure Law (Communication's Data) (2007) and Article 13(b)(2) to the Israeli Communications Law (1982) can allow, under some circumstances the collection of **Traffic Data** in real-time.
Data retention obligations		The Israeli data protection and privacy laws do not include specific obligations regarding the period for which records must be retained. However, specific requirements do exist with regard to certain kinds of data, such as medical (especially in hospitals) and credit data, which provide that relevant data be retained for specific minimum periods.
Direct Requests to SPs for Voluntary Disclosure		In order to receive information from a service provider such as BSI and/or traffic data contact can be made with National Cyber Center – if a SP will not voluntarily disclose an MLAR must be submitted
Emergency Disclosure	**Criminal Procedure Law (Communication's Data) (2007)** **Article 4**	The Criminal Procedure (Communication's Data) Law, 2007 Article 4 provides that a SP with a Bezeq Licence shall provide **BSI**, **Traffic Data** or content data – when asked by an Israeli police chief superintendent to prevent immediate loss of life or to prevent a criminal act that endangers the safety of others. A Requesting State must send the Emergency Disclosure Request to the cyber fusion center of the Israeli national police to secure data from an Israeli SP.

Jordan

Jordan has ratified CITO - Article 32 ensures that it can be used as an instrument to facilitate MLA and provides for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and disclosure of stored data and traffic data to States that have ratified CITO. CITO does not provide for real-time content and traffic data interception and the Jordanian domestic legislation Cybercrimes Law No. 27 of 2015 does not provide for preservation of data – although – electronic evidence can be preserved when an MLAR is sent.

Procedural Power pursuant to CITO	National Legislation	Comments
Article 26 CITO - Inspecting Stored Information **Article 27 CITO - Seizure of Stored Information**	**Cybercrimes Law No. 27 of 2015** **Article 13**	This investigatory power includes searching for data.
Article 37 CITO: Expeditious Safeguarding of Information Stored on Information Systems	**No equivalent**	This expedited power to retain BSI, traffic data and stored content is essential as part of cybercrime investigations to ensure the evidence is available for search, access, seizure and review. CITO allows for preservation for 60 days. Dual criminality is required unless an offence outlined in CITO Chapter II.[58] Preservation requests will be sent via MLAR through the Ministry of Justice to the Attorney General's Department for a Prosecutor to confirm if legal to require a SP in Jordan to preserve electronic evidence
Article 38 CITO: Expeditious Disclosure of Safeguarded Users Tracking Information	**No equivalent**	This procedural power is especially important to ensure that SPs provide tracking information that could locate the perpetrator of a crime.
Article 39 CITO: Cooperation and Bilateral Assistance Regarding Access to Stored Information Technology Information	**No equivalent**	This is an essential provision for an effective cybercrime investigation to ensure SPs provide **BSI**, **Traffic Data** and stored **content** data. Further, this power will require individuals and others (such as corporate entities, financial institutions and other organizations) who hold data to produce it to law enforcement authorities.
Article 40 CITO: Access to Information Technology Information Across Borders	**No equivalent**	This provision can be used to access a computer in another state with consent of the person who has legal authority to disclose the data (Article 40(2))
Article 41 CITO: Cooperation and Bilateral Assistance regarding the Expeditious Gathering of User's Tracking Information		There is no procedural power in Jordan to collect **Traffic Data** real-time. CITO does not define *tracking information* and it is unclear if it includes the communication's origin, destination, route, time, date, size, duration, or type of underlying service (i.e. traffic data)

58. *Ibid*

Procedural Power pursuant to CITO	National Legislation	Comments
Article 42 CITO - Cooperation and Bilateral Assistance regarding Information related to Content	**Cybercrimes Law No. 27 of 2015** **Article 13**	Article 13 provides for interception of computers – but only for cybercrime offences contrary to the 2015 Law
Emergency Requests		Emergency requests will be sent via MLAR to the Ministry of Justice to the Attorney General's Department for a Prosecutor to confirm if legally correct to require a SP in Jordan to disclose. Any MLAR should be marked as URGENT
Voluntary Disclosure		There are no domestic provisions to allow for direct requests to SPs in Jordan

Lebanon

Lebanon is not a party to a Convention dedicated to cybercrime but has signed MLA bilateral Treaties with Syria, Jordan, Kuwait, Greece and Bulgaria.

Lebanon does not have any specific law on cybercrime at present (please note an Electronic Transactions and Personal Data Bill has been drafted)

There are no provisions in law that allow for the collection of electronic evidence. A data retention regulation was ordered by the General Prosecution Office (GPO) in 2013 requiring all SPs and internet cafés to retain **Traffic Data** for one year.

Public prosecutors and investigative judges may seek assistance of the Telecommunication Regulation Authority when gathering evidence from national SPs.

Law 140/99 (as amended by Law 158/99) allows for interception, listening, and surveillance of all means of communication - including e-mails.

IMPORTANT NOTE: There is no domestic legislation for preservation of data - these should be sent through the Central Authority (Ministry of Justice) who will transfer the request to the GPO or The Cybercrime and Intellectual Property Bureau. Emergency Requests can be sent to the Cybercrime and Intellectual Property Bureau (email cybercrime@isf.gov.lb)

Morocco

Morocco ratified the BC and this will be the basis for cooperation with other States that have ratified. Although, there is no national legislation outlining the proscribed procedures.

Procedural Power Pursuant to Budapest Convention	National Legislation	Comments
Article 19 BC - **Search and seizure of** **stored computer data**	**Code of Criminal Procedure** **Articles 57, 59, 60, 62 and 99**	Articles 57 and 59 of the Code of Criminal Procedure allow judicial police officers aware of a felony or *flagrante delicto* to immediately inform the public prosecutor's office, go to the place where it was committed, and note all the relevant facts. The public prosecutor ensures that the evidence at risk of disappearing and any other element useful in ascertaining the truth are preserved. This includes seizing the instruments used or intended to be used to commit the offence i.e. a computer. Articles 60 and 62 do not refer to '*data*' and is not computer specific. It can be essential in cybercrime investigations to access the computer and the data contained therein. The Code of Criminal Procedure does not make it clear if stored computer data per se will be considered as a tangible object and therefore seized in a parallel manner as tangible objects (such as computers) other than by securing the computer or data medium upon which it is stored.
Article 29 BC – **Expedited preservation of stored content data**	**No equivalent**	Preservation can be used by other States that ratified the BC to ensure that data which is vulnerable to deletion or loss is preserved. An MLAR must be sent for preservation through the Ministry of Justice for any SPs in Morocco – the Prosecutor General must confirm if a request is lawful There are three SPs and the Moroccan law requires them to cooperate with the authorities. Each has a special department to handle requests
Article 30 BC **Expedited preservation and partial disclosure of traffic data**	**No equivalent**	This procedural power can be used by other BC States to ensure that SPs provide **Traffic Data** to locate the perpetrator of a cybercrime
Article 31 BC – **Disclosure of stored content data**	**No equivalent**	Disclosure of content provides those States that have ratified the BC access to messages – for examples emails
Article 33 BC – **Real time collection of traffic data**	**No equivalent**	This procedural power is important to determine the location of a perpetrator of a crime using a computer.
Voluntary Disclosure		There are no domestic provisions to allow direct requests to SPs in Morocco

Procedural Power Pursuant to Budapest Convention	National Legislation	Comments
Emergency Requests		Police-to-police contact with the Judicial Police in Morocco can be made to secure data to save life in emergency requests. An MLAR can be sent for an emergency request through the Ministry of Justice for any SPs in Morocco – the Prosecutor General must confirm if a request is lawful

Palestine

Palestine has ratified CITO and on July 9 2017, Law No. 16 of 2017 on Electronic Crimes was issued. Article 32 CITO ensures that it can be used as an instrument to facilitate MLA with other States that have ratified and the national law now provides for expedited preservation of stored computer data, expedited preservation, partial disclosure of **Traffic Data**, disclosure of stored data and **Traffic Data**, interception of **content** data, real-time collection of **Traffic Data**, production orders and search and seizure.

Procedural Power pursuant to CITO	National Legislation	Comments
Article 26 CITO - Inspecting Stored Information **Article 27 CITO - Seizure of Stored Information**	**Decree Law No. 20 of 2015 on Combating Money Laundering and the Financing of Terrorism** **Article 33** **Law No.16 of 2017 on Electronic Crimes** **Articles 33 and 34**	Article 33 Decree Law No. 20 of 2015 relates to accessing computers and networks but is only available for money laundering and the financing of terrorism. Article 33 No. 16 of 2017 is more wide-ranging and applies to the cybercrime offences it criminalizes. Article 34(1) confirms access to computers and data relevant to crimes in law No. 16. Article 34(3) of law No. 16 enables copying of the relevant data if not seized. Article 34(4) of Law No. 16 prevents access if the data cannot be seized and Article 34(5) of the same law requires integrity of the seized data is maintained.
Article 37 CITO: Expeditious Safeguarding of Information Stored on Information Systems	**Law No.16 of 2017 on Electronic Crimes** **Article 34**	This expedited power in Article 34 of Law No. 16 to retain **BSI**, **Traffic Data** and stored **content** is essential to ensure the evidence is available for search, access, seizure and review. Preservation requests are sent to the Public Prosecutors Office to verify and then sent to the Police to request preservation CITO allows for preservation for 60 days.
Article 38 CITO: Expeditious Disclosure of Safeguarded Users Tracking Information	**Law No.16 of 2017 on Electronic Crimes** **Articles 34 and 35(2)**	Article 35(2) of Law No. 16 is especially important to ensure that SPs provide IP addresses to locate the perpetrator of a cybercrime

Procedural Power pursuant to CITO	National Legislation	Comments
Article 39 CITO: Cooperation and Bilateral Assistance Regarding Access to Stored Information Technology Information	**Law No.16 of 2017 on Electronic Crimes** **Articles 34, 35, 43 and 44**	Law No.16 will ensure SPs provide **BSI**, **Traffic Data** and stored **content** data. Further, this power will require individuals and others (such as corporate entities, financial institutions and other organizations) who hold data to produce it to law enforcement authorities.
Article 40 CITO: Access to Information Technology Information Across Borders	**Law No.16 of 2017 on Electronic Crimes** **Article 40**	Article 40 of Law No.16 permits unilateral trans-border access without the need for MLA where there is consent or the information is publicly available.
Article 41 CITO: Cooperation and Bilateral Assistance regarding the Expeditious Gathering of User's Tracking Information	**Law No.16 of 2017 on Electronic Crimes** **Articles 34, 35, 43 and 44**	There is no procedural power in Palestine to collect traffic data real-time. CITO only allows for tracking data which would not include the communication's origin, destination, route, time, date, size, duration, or type of underlying service
Article 42 CITO - Cooperation and Bilateral Assistance regarding Information related to Content	**Law No.16 of 2017 on Electronic Crimes** **Articles 34, 35, 43 and 44**	Domestic law allows interception under Law No.16 of 2017 on Electronic Crimes Article 35(2) and Decree Law No. 20 of 2015 on Combating Money Laundering and the Financing of Terrorism Article 33
Emergency Requests		Police-to-police contact with the police in Palestine can be made to secure data to save life in emergency requests – this must be judicially authorised. There are 24/7 contact points at the Office of the Public Prosecutor for such requests
Voluntary Disclosure		There are no provisions for direct requests to SPs in Palestine

Tunisia

Tunisia does not have legislation on cybercrime - although a bill is being prepared. Tunisia has acceded to Convention No. 108 of the Council of Europe for Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional protocol No 181 for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows.[59] Tunisia is not a party to the BC, CITO or AUC. This means that Tunisia is not a party to an international convention dedicated to cybercrime, and this will hinder international investigations as procedural powers will not have a legal basis. A Cybercrime Bill is presently before Parliament.

Preservation Requests		An MLAR must be sent for preservation through diplomatic channels and the decision to cooperate is the responsibility of the Directorate-General of Criminal Affairs at the Ministry of Justice
Emergency Requests		Police-to-police contact with the Judicial police in Tunisia can be made to secure data to save life in emergency requests. An MLAR can also be sent for an emergency request and the decision to cooperate is the responsibility of the Directorate-General of Criminal Affairs at the Ministry of Justice. MLATs may confirm that urgent MLARs do not need to be sent through diplomatic channels and can be sent directly to the Ministry of Justice
Voluntary Disclosure		There are no provisions for direct requests to SPs in Tunisia

59. Organic Law 2017-42 of 30 May 2017

ANNEX H: Law and Procedure in Selected States with SPs[60]

Canada

MAIN SPS IN CANADA

- Kik Interactive – law enforcement guidelines: https://lawenforcement.kik.com/hc/en-us/categories/200320809-Guide-for-Law-Enforcement
- TextNow – law enforcement guidelines: https://supportwireless.textnow.com/hc/en-us/articles/204231469-Law-Enforcement-Legal-Requests
- Hushmail – law enforcement guidelines https://www.hushmail.com/privacy/
- OVH Hosting – no law enforcement guidelines
- Blackberry – no law enforcement guidelines

PRESERVATION

See SP Mapping in **Part 4**

LAWS ON PRODUCTION OF ELECTRONIC EVIDENCE STORED BY SPS IN CANADA

BSI / Content Data

In general, a production order under Canada's Mutual Legal Assistance in Criminal Matters Act (MLACMA) is required in order to obtain **BSI or Content Data** from Canadian SPs. The legal threshold is reasonable grounds to believe that an offence has been committed and that evidence of the commission of the offence, or information that will reveal the whereabouts of the person suspected of having committed the offence, will be found in Canada. In other words, sourced evidence establishing the relevance of the **BSI or Content Data** to the foreign investigation or prosecution is necessary to justify such orders.

60. For more information on national law see the Council of Europe website, the UNODC Sherloc database https://www.unodc.org/cld/en/v3/sherloc/index.html or UNODC Cybercrime Repository

Traffic Data

A production order is required to obtain **Traffic Data** (or transmission data) in Canada. However, it is possible to gather these records on the lower legal threshold of reasonable grounds to suspect that an offence has been committed, the data is in the possession or control of the person in question, and the evidence will assist in the investigation of the offence.

Real-Time Content

Under Canadian law, real-time email/internet **Content Data** may not be intercepted on behalf of a foreign State. However, it is possible to obtain data transmission recorder warrants (DTRW), permitting the real-time, covert gathering of information for a foreign state about devices communicating with each other (e.g.)

This device called that device at this time and the communication lasted for x period of time). As well, it is possible to obtain a tracking warrant which allows a person or thing to be tracked in real-time and covertly. DTRWs and tracking warrants involving the tracking of a thing may be obtained on reasonable grounds to suspect that an offence has or will be committed and the evidence will assist in the investigation of the offence. Tracking warrants to track a person must satisfy the higher test of reasonable grounds to believe.

Other Court Orders for Electronic Evidence

Canada also has the ability to obtain production orders for historical tracking data and for tracing specified communications (tracing communications routed through multiple service providers to identify the originator). The legal threshold for these production orders is reasonable grounds to suspect that an offence has been, the data is in the possession or control of the person in question, and the evidence will assist in the investigation of the offence.

 The following MLA Guidelines are available:

Canadian eGuidance

NON-EMERGENCY DIRECT REQUESTS TO CANADIAN SPS

There is no express prohibition against direct contact. However, it is important to note that a Canadian SP is under no legal obligation to comply with such a request and any voluntary disclosure would need to comply with Canadian privacy laws. See SP Mapping in **Part 4**

EMERGENCY DISCLOSURE REQUESTS TO CANADIAN SPS

There is no express prohibition against direct contact. However, it is important to note that a Canadian SP is under no legal obligation to comply with such a request and any voluntary disclosure would need to comply with Canadian privacy laws. See SP Mapping in **Part 4**

Republic of Ireland

LAWS ON PRODUCTION OF ELECTRONIC EVIDENCE STORED BY SPS IN IRELAND

An MLAR for stored data (always for **Content Data**) must be sent in accordance with section 75 of the Criminal Justice (Mutual Legal Assistance) Act 2008

There is no Irish law for interception of email or other online communications.[61]

NON-EMERGENCY DIRECT REQUESTS TO IRISH SPS

The Republic of Ireland hosts data centres for a number of U.S. SPs (Facebook, Twitter, Microsoft and Yahoo) with European addresses for example @yahoo.fr

Disclosure of non-content data (i.e. **BSI and/or Traffic Data**) to Law Enforcement in Ireland is governed by the Data Protection Acts 1988 and 2003, the Criminal Justice Act 2011 and the Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012. Irish Law Enforcement.

Non-content can be obtained by the Garda Síochána and shared police-to-police – if there is an Irish nexus. Absent nexus an MLAR must be sent for non-content.

The following MLA Guidelines are available:

eGuidance

EMERGENCY DISCLOSURE REQUESTS TO IRISH SPS

Emergency requests can be sent to SPs in Ireland (if the data is stored there) when there is a:

- Risk of death or serious physical injury to a person or persons;
- The risk is imminent such that there is not sufficient time to obtain a valid and properly served Irish court order or send an MLAR that would normally be required to compel production of data;
- The data requested is relevant to the investigation of the imminent risk; and

There is sufficient information for the SP to form a good faith belief that producing the requested data will assist law enforcement in deterring or otherwise addressing the imminent risk.

61. The Irish Department of Justice and Equality have published a policy document on amending the law relating to the interception of communications.

Switzerland

MAIN SPS IN SWITZERLAND

- Proton Mail:
  https://protonmail.com/
  https://protonmail.com/blog/transparency-report/
- Threema
  https://threema.ch/en/transparencyreport

Servers hosted in Switzerland

- Chorus Call
  http://choruscall.com/
- Digital Suisse
  https://digitalsuisse.com/#!/
- Private Layer
  https://www.privatelayer.com/

PRESERVATION

Preservation Requests must be sent through the 24/7 contact point (the Federal Office of Police) or the Central Authority (the Federal Office of Justice). In cases where the Budapest Convention applies, police-to-police channels may be used for Preservation requests.

LAWS ON PRODUCTION OF ELECTRONIC EVIDENCE STORED BY SPS IN SWITZERLAND

Switzerland does not require a treaty basis for judicial cooperation and is able to assist on the basis of reciprocity.

Switzerland has received several requests to obtain electronic evidence from SPs hosted in Switzerland. Requests concerning providers hosted in Switzerland have been executed through an incidental decree and the voluntary disclosure of **BSI** (non-content data) others after a conclusive decree. Requests concerning servers hosted in Switzerland have been executed through an incidental and a conclusive decree (stored digital data).

 MLA Guidelines can be found at (not specific on accessing electronic evidence): https://www.rhf.admin.ch/dam/data/rhf/strafrecht/wegleitungen/wegleitung-strafsachen-e.pdf

NON-EMERGENCY DIRECT REQUESTS TO SWISS SPS

Actively contacting SPs as private parties might constitute a crime. Article 271 Swiss Penal Code prohibits the gathering or taking of evidence in Switzerland for use in a foreign proceeding without lawful authority (where such activities are the responsibility of a public authority or public official)

EMERGENCY DISCLOSURE REQUESTS TO SWISS SPS

Emergency Disclosure Requests must be sent through the 24/7 contact point (the Federal Office of Police) or the Central Authority (the Federal Office of Justice) at email address: irh@bj.admin.ch

In cases where the Budapest Convention applies, police-to-police channels may be used for Emergency Disclosure based on voluntary disclosure of the SP. It is also recommended to additionally send an MLA.

ANNEX I: European Union cooperation with third countries

Judicial cooperation in criminal matters between EU MS and third countries are governed by international law treaties and agreements, either bilateral or multilateral. For the Agreements that the EU MS has concluded with some third countries please go to the EuroMed CrimEx Legal and Gaps Analyses and the Judicial library that you can access via the homepage of the EJN - https://www.ejn-crimjust.europa.eu/ejn/libcategories.aspx

The model proposed by the EU for cross-border gathering of electronic evidences

On 17 April 2018 the European Commission presented two legislative proposals to enhance cross-border gathering of electronic evidence:

1. Proposal for a **Regulation**[62] on European Production and Preservation Orders for electronic evidence in criminal matters establishing:

    - The **European Preservation Order** allowing a judicial authority to request that **a SP or its legal representative in another EUMS** preserves specific data in view of a subsequent request to produce this data via mutual legal assistance, a European Investigation Order or a European Production Order
    - The **European Production Order** allowing a judicial authority to obtain electronic evidence (such as emails, text or messages in apps, information to identify a perpetrator) **directly from a SP or its legal representative in another EU Member State**, which will be obliged to respond within **10 days**, and within **6 hours** in cases of emergency (compared to up to 120 days for the existing European Investigation Order or an average of 10 months for a Mutual Legal Assistance procedure);
    - The **right to protection of personal data**: the service providers and persons whose data is being sought will benefit from various safeguards and be entitled to legal remedies;

2. Proposal for a **Directive** 63 on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, providing for

    - Mandatory designation by the service providers of a legal representative in the EU: for the receipt of, compliance with and enforcement of decisions and orders, even if their headquarters are in a third country
    - Legal certainty and clarity: applying the same rules for access to all SP.

62. https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF
63. https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

EU data protection reform package

1. **GDPR - General Data Protection Regulation (EU) 2016/679**[64], in force from 25 May 2018 lays down general rules to protect natural persons in relation to the processing of personal data.
   GDPR recital (19) stipulates that this Regulation **should not apply** to processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, which are the subject of a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council.

2. **DPDC - Directive (EU) 2016/68065** in force on 6 May 2018, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Subject-matter and objectives

DPDC lays down the special rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities in the areas of criminal matters and public security.

Transfers of personal data to third countries or international organisations, (DPDC art 35, 36, 37, 38, 39, 40).

Where personal data are transferred **from the EU to Interpol, and to 3rd countries** which have delegated members to Interpol, DPDC, in particular the provisions on international transfers, should apply. DPDC applies the specific rules laid down in Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61) and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

A transfer to a third country or to an international organisation takes place only if the controller in the third country or international organisation is an authority competent within the meaning of the Directive. Such a transfer may take place in cases:

- Where the Commission has decided - adequacy decision- that the third country or international organisation in question ensures an adequate level of protection,
- Where appropriate safeguards have been provided in a legally binding instrument such as bilateral agreements, or
- Where derogations for specific situations apply - to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject for the prevention of an immediate and serious threat to the public security of a EUMS or a third country; in an individual case for

64. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
65. https://publications.europa.eu/en/publication-detail/-/publication/182703d1-11bd-11e6-ba9a-01aa75ed71a1/language-en

the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or in an individual case for the establishment, exercise or defence of legal claims.

Where personal data are transferred from a EUMS to third countries or international organisations, such a transfer should, in principle, take place only after the EUMS from which the data were obtained has given its authorisation to the transfer.

Onward transfers of personal data should be subject to prior authorisation by the competent authority that carried out the original transfer.

Where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism - in specific individual cases, when the regular procedures requiring contacting such an authority in the third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards, - the competent authorities of EUMS could decide to transfer personal data directly to recipients established in those third countries.

Article 61. Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force **until amended, replaced or revoked.**

EU agencies cooperation with third countries

Eurojust - COUNCIL DECISION 2009/426/JHA[66] of 16 December 2008

In accordance with Article 26a of the Eurojust Decision, to exchange information, including personal data, to second liaison officers or magistrates, Eurojust may conclude agreements with third States and organisations such as:

- International organisations and their subordinate bodies governed by public law;
- Other bodies governed by public law which are based on an agreement between two or more States; and;
- The International Criminal Police Organisation (Interpol).

66. http://eurojust.europa.eu/about/Partners/Documents/article-26a-EJD-EN.pdf

EJN[67] - European Judicial Network in Criminal Maters[68] - Joint Action 98/428 JHA of 29 June 1998[69]

Cooperation through judicial networks and contacts to facilitate the practical implementation of the binding legal framework for judicial cooperation and speed up the procedures. In case a third country does not belong to any judicial network, the direct nomination of contact points can fulfil the same purpose. Such nominations may take place also in case there is a particular need, e.g. in relation to countries which the EU Member States cooperate with on a more regular basis.

Europol - Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol)70

On 4 June 2018 European Council approved the Commission's proposal to strengthen Europol's cooperation with third countries and fight terrorism and other serious transnational crime more effectively. The Council authorised the opening of negotiations for agreements between the EU and Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey on the transfer of personal data between Europol and these countries to prevent and combat terrorism and serious crimes.

Europol operates SIRIUS platform, a practical and innovative solution to address the current challenges faced by law enforcement in Internet-based investigations. SIRIUS is a capacity-building tool fostering knowledge exchange.

The EU Internet Referral Unit (EU IRU) at Europol launched the SIRIUS project in 2017 to provide a secure environment to facilitate cross-border access to electronic evidence in an operational context. SIRIUS is an innovative, interactive knowledge platform accessible to law enforcement authorities and members of the judiciary, and aims to improve EU-US cooperation on cross-border access to electronic evidence. The platform empowers a community of members from law enforcement and the judiciary to share knowledge, tools and methodology on Internet-based investigations.

The project is funded by the European Commission's Service for Foreign Policy Instruments (FPI) under grant agreement No PI/2017/391-896.

Euromed Police will use the **Euromed Threat Forum**, hosted in the same Europol Platform for Experts (EPE) as SIRIUS, which intends to be a similar platform where the sharing of information related to SPs and contact points takes place. **All the information related to the digital evidence manual would be updated in this platform.**

67. Presentation Brochure in Arabic https://www.ejn-crimjust.europa.eu/ejnupload/StaticPages/Leaflet_Arabic.pdf
68. https://www.ejnforum.eu/cp/network-atlas
69. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31998F0428&from=EN
70. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0794&from=EN