EUROPOL

The Hague, 30 July 2020

Joint Parliamentary Scrutiny Group Secretariat

To the attention of the JPSG Co-Chairs

By email only:
jpsg.libesecretariat@europarl.europa.eu

Europol reply to written questions from MEP Chinnici and MEP Breyer to the Joint Parliamentary Scrutiny Group (JPSG)

Dear Co-Chairs,

In accordance with Article 4.2 of the JPSG Rules of Procedure and Article 51 of the Europol Regulation, Europol would like to respond to the questions raised by JPSG members, Mr Breyer and Ms Chinnici, received by Europol on 18 June 2020 as follows:

Written question by MEP Caterina Chinnici

The use of facial recognition software systems. In the answers provided to Hon. Breyer, Mr Ebner, Deputy Executive Director Governance, states that Europol uses two semi-automatic facial recognition software systems to carry out its investigations and to facilitate the detection /cross-checking of suspicious people. A system developed internally at EUROPOL, and another Griffeye Analyze DI Pro, purchased through a Swedish company at and used in 2019 to support investigations relating to the sexual exploitation of minors online.

1. *With reference to the use of these systems, how is respect for privacy guaranteed, obviously for the citizens involved who are not involved in the investigations, established by the General Data Protection Regulation (GDPR)?*

Europol's reply:

Europol collects and processes data in the context of criminal investigations carried out by EU Member States, which provide the data in accordance with the national law of the Member State concerned and the Europol Regulation.

Europol has implemented the appropriate technical and organisational measures and procedures in such a way that the data processing complies with Article 28 of the Europol Regulation and protects the rights of the data

subjects concerned by introducing the necessary data protection safeguards for the processing of facial images which allow or confirm the unique identification of the natural persons. The application of data protection rules by Europol including to all operations performed is supervised on various levels and throughout the entire information life cycle. The Data Protection Officer (DPO) has the task to ensure, in an independent manner, lawfulness and compliance with the Europol Regulation (ER) and its implementing rules. The DPO is a member of staff and an integral part of the organisation. External supervision is carried out by the European Data Protection Supervisor (EDPS) including the authority to issue processing bans in case of detected non-compliances. The EDPS acts in close cooperation with national supervisory authorities.

The Europol Regulation establishes special provisions for certain categories of data subjects. Processing of personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences, or in respect of persons under the age of 18, shall be allowed if it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives.

Europol makes a distinction between personal data in respect of different categories of data subjects as clear as possible. Facial images concerning persons such as victims, witnesses and persons possessing relevant information, as well as facial images concerning minors are processed only if strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives. In addition, access to the database of Europol's Analysis Project (AP) Twins is restricted to members of that team and the data contained in the AP is retained within the rules of the Opening Decision for the analysis project, which specifically allows that project to retain data in respect of children and adults, sexual preference and victims.

2. *Imagining the existence of a database? How many profiles / faces does it contain?*

Europol's reply:

The facial recognition software developed internally by Europol (FACE) extracts facial biometric data from contributions to Europol's databases related to different crimes areas. The large majority comes from contributions from EU Member States and Third Parties with which Europol is mandated to exchange personal data; a smaller number of images comes from open sources, e.g. from online terrorist propaganda imagery. At the end of June 2020, almost 1 million (995,096) facial biometric entities were accessible through FACE. The large majority falls into the area of child sexual abuse (>75 %). Contributions from EU Member States and Third Parties to Europol's database of child sexual abuse material seized in investigations and referred from online service providers have increased significantly over the years. Currently more than 48 million images and video files are available in Europol's database. The high number is a reflection of the prevalence of this crime in society.

3. *Are these databases updated? If yes, how long is this data kept?*

Europol's reply:

The processing of facial biometric data falls under the Europol Regulation, which includes specific provisions for regular data review. Authorised staff in line with these provisions review the contributions of personal data regularly.

4. *Based on the experience gained, can the error rate of these facial recognition systems based on biometric data already be established?*

Europol's reply:

For the facial detection-comparison features, these two software are using machine-learning algorithms that can provide to the user, for a given face ("vector"), the similar faces existing in the database ("candidates"), based on a calculated threshold that may vary from 0 to 100%. The Europol internal procedure for facial comparison specifies that a human operator, trained in the field of face comparison, shall further compare the vector with the candidates resulted from the output provided by the software.

The result of the comparison made by the human operator would be an assessment of whether candidate(s) present a high degree of similarity with the vector, or which candidates present similar facial characteristics to those of the vector. This result is further communicated to the relevant law enforcement partner who can further conduct specific enquiries to establish if the persons depicted in the vector and the candidate(s) images are either the same or the different person(s).

5. *How is the balance between the needs of the investigation and the respect of the involved child's right to be forgotten, i.e. the possibility of obtaining the immediate removal of content that could jeopardize his dignity?*

Europol's reply:

The removal of child sexual abuse material (CSAM) from the internet is a necessary step to prevent the re-victimization of the victim. It is very often one of the initial steps of the investigative process aiming at the identification of the victim and the arrest of the offender. Europol is not directly involved in the removal process, as it falls under the competence of the national authorities. Nevertheless, the processing of the CSAM contributed by the Member States in the frame of their investigations follows the procedures

established in Article 28 of the Europol Regulation, protecting the rights of the data subjects concerned by introducing the necessary data protection safeguards.

The removal of personal data from Europol systems, including facial-biometric, is specifically controlled by the Europol Regulation. The possibility to review personal data or to request to know what personal data is held by Europol in regard to any individual is open to the individual citizens themselves, subject to certain conditions, through the Europol Regulation[1]. Child sexual abuse material involves special categories of personal data including sex life information, which is particularly sensitive and has direct impact on the dignity of those victims. CSAM often continues to be shared amongst paedophiles via online environments also as regards cases that were already investigated by law enforcement authorities. The re-sharing of already known CSAM leads to the re-victimisation of concerned data subjects but also to additional investigations in order to identify those redistributing incriminated material. Furthermore, law enforcement operations may attempt to rescue minors from on-going sexual abuse while the reality might be that the same child has in fact already been identified (and ideally rescued) during an earlier law enforcement operation. Against this background, in some cases, CSAM is not being directly deleted from Europol databases after closure of a certain judicial case but being retained in order to enable building on already existing related criminal intelligence and to prevent later investment of law enforcement efforts into cases which may already (partly) have been solved, within the limits of Europol legal framework.

The purpose of the database storing the images extracted from the contributions to Europol is to enable the identification of children and their abusers.

The database was created and is maintained in a separated environment without access to the internet or linking to other databases. The right of the child to be forgotten, where necessary, is assured through the existing Europol regulation and the provisions in it regarding the retention of personal data on individuals. Special data retention rules apply to data related to victims of a criminal offence or persons under the age of 18. Furthermore, CSAM is subject to regular data retention related reviews in order to determine the continued necessity of processing at least every three years. Any potential data subject access request and any potential subsequent request for erasure of personal data by a concerned data subject would be duly scrutinised taking into account the operational interest and – very importantly – the interest of the individual concerned.

---

[1] Article 37(2) of the Europol Regulation stipulates that any data subject having accessed personal data concerning him or her processed by Europol in accordance with Article 36 shall have the right to request Europol, through the authority appointed for that purpose in the Member State of his or her choice, to erase personal data relating to him or her held by Europol if they are no longer required for the purposes for which they are collected or are further processed. That authority shall refer the request to Europol without delay and in any case within one month of receipt.

Written question by MEP Patrick Breyer

1. *How many and which hosting service providers (please list names) are systematically or mostly refusing to remove terrorist content referred to them by or via Europol?*

Europol's reply:

The role of Europol's EU Internet Referral Unit (EU IRU) is to support companies in reducing accessibility to terrorist content online, in voluntary cooperation with the tech industry. Since 2015, the EU IRU has detected terrorist content on around 360 platforms globally. The first outreach to the affected Online Service Providers (OSPs) is launched in the context of the referral process. The referral activity (meaning the reporting of terrorist and extremist online content to the concerned online service provider) does not constitute an enforceable act. Thus, the decision and removal of referred/identified terrorist and extremist online content is taken by the concerned service provider under its own responsibility and accountability based on the companies' terms of reference.

Whilst Europol is not in a position to provide operational details on OSPs' responses to referrals, it should be stressed that the EU IRU enhances its support to the affected OSPs with a combination of actions that go beyond the referral process. The EU IRU engages with OSPs to share best practices on the pro-active detection of terrorist content and informs OSPs how their services are being abused and by whom. It also provides law enforcement expertise on trends and methods used by terrorist organisations or examples of pro-active measures that could be implemented to improve resilience.

The combination of referral requests and the above mentioned actions is tailored to the type of services that each online platform offers and the degree of their capability for cooperation. The companies' responses vary, depending on their size, financial and human resources, extent of abuse by terrorists or technical capabilities. Whilst some companies would implement technical solutions to optimise the referral process or invest in moderation teams, others would focus mostly on pro-active detection or apply a combination of techniques, such as geo-blocking of terrorist content or "login pages.

Based on the measures set out above, the EU IRU has an excellent track record of building, over time, trust-based and sustainable relationships with relevant online platforms. In the EU IRU's experience, it is vital to understand the culture, set-up and limits of OSPs to ensure law enforcement's outreach is appropriately measured. Through its work as a key stakeholder in the EU Internet Forum and outreach efforts with NGOs like Tech Against Terrorism and co-chairing Global Internet Forum to Counter Terrorism Working Groups, EU IRU aims to continue to be an approachable and effective resource to facilitate Member State investigations and referrals.

2. *For each year since 2015, how many pieces of terrorist content did the Europol Internet Referral Unit refer to online platforms for removal (please answer separately for each year)?*

Europol's reply:

	Contributed number of items for referral
20162	20059
2017	24247
2018	37835
2019	25086
2020 (Q1)	5514

3. *For each year since 2015, how often did national authorities refer terrorist content to online platforms via the EU IRU technical solution (please answer separately for each year and each participating Member State)?*

Europol's reply:

	number of MS	number of items for referral via the EU IRU technical solution
2015	1	119
2016	8	2011
2017	7	3647
2018	9	71352
2019	11	137046
2020	7	15496

[2]The figure represents the number from Jul 2015 (establishment of EU IRU) until Dec 2016.

I hope that these answers will prove satisfactory. Europol remains available for further clarifications.

Yours sincerely,

Jürgen Ebner
Deputy Executive Director of Governance