Facial images in Prüm

French Gendarmerie Criminal Databases Division

PRUM Workshop – 20th Apr. 2021
General overview

● In France, there is no live/real-time facial recognition but only post-event use by law enforcement agencies.

● By-design, a tool directly available to local investigators in the police records database which means:
  – Basic knowledge needed on how to use this tool;
  – No identification but just likely candidates to be considered as potential avenues of investigation.

● The police records database is comprised of +6 millions facial images. It is used by the National Gendarmerie and National Police.

I. How do we use it?

1st option: Running a search

- Running a search using an image of the unknown suspect (CCTV, social network, victims’ phone, etc.);

- Parsing the list of facial images ranked by computer-evaluated similarity;

- Determining whether a possible candidate is part of the list;
1. How do we use it?

2nd option: Inserting unknown suspects

- If investigators have a facial image of a suspect but no ID, it still can be stored in the database as an « anonymous » suspect (i.e.: facial images used in fraud cases or ID theft, CCTV...);

- When the tool is used in other investigations, the facial image of the « anonymous » suspect could appear as a likely candidate.

- Several cases could then be linked.
II. « Real life » examples

• Case #1: Rape, abduction and illegal confinement;

– Leaving a night-club, a young woman was abducted and raped. The victim didn’t know the perpetrator.

– The only clue: pictures taken during the night in the club.
II. « Real life » examples

Case #1: The investigation confirmed the likelihood and the identification of the suspect.

- The suspect used to live in the night-club’s neighborhood;
- He was known for fraud, violence and procuring.
- 4 days after the event, the suspect was charged and on remand.
II. « Real life » examples

- Case #2: sexual assault on minor
  - An old man got on a packed bus and tried to sexually assault a 12-years-old boy. A friend of the victim took a picture of the suspect.
Case #3: Burglary

- Two individuals break into a house and steal jewelry, luxury leather goods, and a car.
- Images of the suspects are extracted from CCTV.
III. Facial images exchanges in Prüm ?

• Conclusion of the TELEFI project

• In a significant number of cases, a facial image of a suspect is available
  – From a videosurveillance system ;
  – From the smartphone of a witness or victim ;
  – From a false identity document ;
  – From social networks ;
  – …

• The existing Prüm framework already showed the benefits of cross-border cooperation
III. Facial images exchanges in Prüm?

- Different state of play between Member States
- Facial images exchanges between MS should be allowed for those using a FR system
- A FR system should not be mandatory for MS
- Prüm FR searches by a MS without a FR system is an open question
III. Facial images exchanges in Prüm?

- Due to large databases involved and FR technology limits, processes similar to latent fingerprints seem appropriate (candidate list…)

- Multiple MS searches need to be streamlined due to candidate list size

- Relevance of searches in uncontrolled images databases?

- A FR positive result will be different from a fingerprint positive result

- Step 2 data exchange will allow further investigation to confirm it... or not…

    … Like for biographic data
So, in Prüm, Face Recognition:

- Would be another tool available to investigators, in addition to fingerprints and DNA;
- Should be used only in retrospective use case (no live-FR);
- Would not lead to identification but possible candidates (avenues of investigation), allowing links between cases;
- Should involve human check before requesting the personal data linked to the facial image in a second step;
- Should not be mandatory for MS.
Thank you