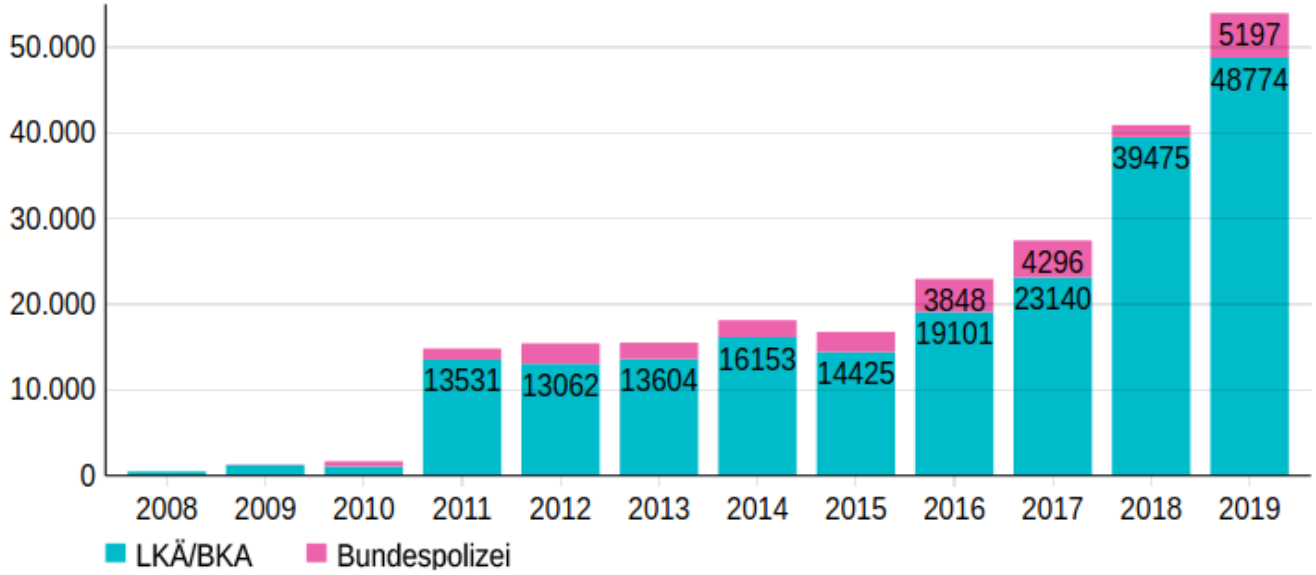
Security Dialogue on police information exchange and in particular the future developments regarding Prüm and the API Council Directive – experts meeting

LIBE Committee meeting on Tuesday 22 September 2020

On the occasion of the tenth anniversary of the Prüm Decision, the Council had proposed in 2018 Conclusions to extend this cooperation to facial images.[1] For the envisaged "Next generation Prüm" (Prüm.ng), the Commission ordered a feasibility study from the consulting firm Deloitte. On the basis of the study, a "focus group on face recognition" with ten European criminal police offices chaired by the Federal Criminal Police Office from Austria defined a technical framework for the comparison.[2]

The German Federal Criminal Police (BKA), which has lots of experience in facial recognition for criminal investigations, was part of the "Prüm focus group on face recognition". In Germany, the queries for biometric photographs increased drastically since 2008. Images are stored in the INPOL-Z file, which is operated by the BKA for police investigations together with the state criminal investigation offices (Landeskriminalämter, LKÄ). In total, German police forces (including Federal Police, Bundespolizei) launched about 54,000 facial recognition searches last year:



Also the number of photographs stored with personal data in INPOL has once again risen significantly, with around 5.8 million portrait photographs of 3.65 million people. Compared to 2018, the increase is about five percent (310,000 more photos).

After the G20 summit in 2017, the Hamburg police for the first time ever used facial recognition against (in that case left-wing) protestors. The Hamburg Data Protection Commissioner Johannes Caspar prohibited the police from further use of the system, but the administrative court finally overturned an order to that effect.[3]

Also in Austria, the Federal Criminal Police Office uses its new facial recognition software after demonstrations that took place in Vienna this summer. when Turkish right-wing extremists had attacked and injured feminist and anti-fascist activists for several days.[4] According to the newspaper

1 https://data.consilium.europa.eu/doc/document/ST-10550-2018-INIT/en/pdf
2 https://www.statewatch.org/media/documents/news/2020/mar/eu-council-prum-facial-recognition-13356-19.pdf
3 https://digit.site36.net/2019/09/19/face-recognition-after-g20-police-in-hamburg-laughs-at-data-protection-commissioner
4 https://digit.site36.net/2020/09/16/police-in-austria-use-facial-recognition-for-demonstrations

"Standard", the facial recognition was used to identify the antifascists involved, the magazine did not find out whether the photos of the right-wing attackers were also examined with the technology.

Under the abbreviation "FACE", the EU Police Agency Europol has also been operating a self-developed facial recognition system for investigations since 2016.[5] Europol also receives biometric evidence from international military and secret service missions.

Also Interpol offers facial recognition in its databases. The organisation is currently developing its own system and launched the two-year DTECH project[6], which processes photos and videos from social media. It is based on facial images provided by "national authorities, regional monitoring platforms, industry and commercial OSINT". The new database can be searched by the authorities of all Interpol member states with "MorphoFace Investigate" software from the French company Safran. Interpol also tested a system from the US company Clearview AI, which has collected around three billion personal images from the Internet and used them to create a facial recognition database.

There might be an increase of facial recognition searches in EURODAC as well, after the the European Commission enhanced its capabilities to store and compare facial images. As with fingerprints, EURODAC was the "pre-cursor" of the introduction of facial recognition in other EU databases. The database can be used not only for asylum prodecures, but for investigations in serious crime and terrorism.

Conclusions

Hamburg's Data Protection Commissioner Johannes Caspar described facial recognition technology as a "new dimension of state investigation and control options". I suggest to carefully reflect the proposals for a "Next generation Prüm" and not enhance it to facial images. I assume, that under a "Next generation Prüm" the use of facial images will drastically increase. Member States might use it for political purpose to repress dissent movements or organisations. An upgraded Prüm system with facial images will create more pressure by police authorities to process images from public surveillance cameras. Police will want to process images found in the Internet, which will lead to more dubious services offered by companies like Clearview AI. This will affect many more persons not involved in any crime acts. "False hits" will occur due to queries with lower quality images. They cannot be analysed by authorities, as the algorithms of the software are kept secret by companies like Cognitech (Germany) or Morpho (France). After the G20, when Hamburg's Data Protection Commissioner tried to enclose illegal police methods, the Hamburg Senate stripped his power of instructing the police (which he used for the first and only time after the G20 summit). This shows that oversight about new functions as facial recognition is very weak and always depending of political majorities.

Matthias Monroy
digit@so36.net
twitter.com/matthimon

5 https://digit.site36.net/2019/03/26/interpol-and-europol-extend-facial-recognition
6 https://digit.site36.net/2020/03/09/clearview-ai-what-does-interpol-use-face-recognition-for