statewatch

International police facial recognition system: Parliament must ensure democratic debate

accessnow

BIG BROTHER WATCH

digitalcourage

Fair Trials

EDRi

European Digital Rights

IT-Politisk Forening

LIBERTY

EFN Elektronisk Forpost Norge

NETPOL The Network for Police Monitoring

ORG OPEN RIGHTS GROUP

politiscope

STOPWATCH

Key points

- The EU plans to expand the 'Prüm' police data exchange system, in which the UK participates, to enable the cross-border searching and exchange of facial images, police records and potentially driving licences
- The necessity and proportionality of these changes have not been demonstrated
- The UK joining the expanded system could lead to millions of custody images and police records being made available for searches by police forces in the EU, and recent announcements suggest passport photos may also be made available via Prüm
- The government has previously ignored Parliament's wishes regarding UK participation in the system
- An open, thorough, democratic debate must be held to ensure that this does not happen again

Background

The Prüm system is a European framework for cross-border police cooperation and information exchange. Under the Trade and Cooperation Agreement, the UK still participates in the system. The current legislation dates from 2008, and in 2021 the European Commission published a proposal to update and expand the system.

The rules currently deal with cross-border searching and exchange of vehicle registration, fingerprint and DNA data by law enforcement agencies. The updated system ('Prüm II') would make it mandatory for participating states to interconnect databases of facial images for cross-border law enforcement searches. It would also provide the option of participating states interconnecting their databases of "police records."[1]

As the European Scrutiny Committee has noted,[2] civil society organisations – including a number of the signatories to this letter – have expressed serious concerns about the Prüm II proposal, arguing that it "fails to demonstrate the necessity and proportionality of its measures, in particular its vastly expanded categories of personal data."[3]

Parliamentary scrutiny

Parliament has historically shown deep concern for the civil liberties and human rights implications of the Prüm system. Due to concerns raised by Parliament in 2015 about the transnational searching and exchange of sensitive biometric and other personal data by police forces, the government agreed:

- to exclude from Prüm searches biometric data held by UK authorities on those suspected of committing a criminal offence;
- to only permit searches of data concerning recordable offences; and

[1] This is defined in the European Commission's proposal as "any information available in the national register or registers recording data of competent authorities, for the prevention, detection and investigation of criminal offences". See: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:784:FIN
[2] https://publications.parliament.uk/pa/cm5803/cmselect/cmeuleg/119-xiv/report.html
[3] https://www.statewatch.org/news/2022/september/european-police-facial-recognition-system-must-be-halted-warns-new-paper/

- to apply higher forensic science standards in the course of determining matches of DNA and fingerprint data.

Parliament subsequently supported the opt-in.[4]

However, EU institutions and member states continued to seek access to UK data on both convicts and suspects, and in June 2020 the government unilaterally reversed its previous position. Parliament was informed by ministers that its decision was being overturned, and that suspects' data – specifically, the DNA data of 5.7 million people – would now be made available for Prüm searches.

In response, the European Scrutiny Select Committee said it was "deeply concerned at the Government's lack of engagement with Parliament during the review process or involvement of Parliament in evaluating and endorsing the outcome of the review and the change in the Government's policy."[5] The Committee highlighted in a letter to the then-Security Minister that "more data, with fewer safeguards, will be shared with EU Member States now that the UK has left the EU than was the case when the UK itself was a Member State."[6]

Prüm II: expanding the system

The Prüm II proposal does little to alleviate such concerns. It substantially expands the types of data that can be searched and exchanged by law enforcement agencies. As noted, the Commission's proposal covers databases of facial images and gives participating states the option of including "police records," while the Council of the EU would like to include driving licence databases in the system.[7]

UK custody image retention

The use of facial recognition technology by the police has been repeatedly questioned and criticised by civil society organisations and human rights experts - for example, regarding necessity and proportionality, transparency and accountability, and (in)accuracy and discrimination. The potential establishment of a Europe-wide network of police facial recognition databases only multiplies these concerns. As far as the UK is concerned, the unlawful retention of millions of "custody images" (photos of arrested individuals) further compounds the problem.

The Home Office's 2017 review of custody images noted:

> *"As of July 2016, there were over 19 million custody images on PND [the Police National Database], over 16 million of which had been enrolled in the facial recognition gallery making them searchable using facial recognition software."*[8]

---

[4] Hansard, 8 December 2015, https://publications.parliament.uk/pa/cm201516/cmhansrd/cm151208/debtext/151208-0004.htm

[5] House of Commons European Scrutiny Select Committee, 'Cross-border police cooperation: the automated exchange of DNA and fingerprint data under Prüm', 9 September 2020, https://publications.parliament.uk/pa/cm5801/cmselect/cmeuleg/229-xv/22911.htm

[6] House of Commons European Scrutiny Select Committee, 'Cross-border police cooperation: the automated exchange of DNA and fingerprint data under Prüm', 9 September 2020, https://publications.parliament.uk/pa/cm5801/cmselect/cmeuleg/229-xv/22911.htm

[7] https://www.statewatch.org/news/2022/may/eu-police-to-be-granted-cross-border-access-to-driving-licence-photos/

[8] Home Office, 'Review of the Use and Retention of Custody Images', February 2017, p.19, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/594463/2017-02-23_Custody_Image_Review.pdf

The same review made clear that images of individuals who have been arrested but not convicted of any offence should not be in the database. However, due to the PND's technical limitations, they cannot be removed automatically, and individuals must instead apply to have their image(s) removed. The Biometrics Commissioner noted in his annual report for 2020 that "there have been very few applications requesting deletion and therefore few deletions."[9] It is self-evident that, at a minimum, these images should not be made available for Prüm II searches, should a decision be made for the UK to participate in the system.

Live facial recognition

The Prüm II proposal also raises concerns over the opportunities it may offer for the expansion of facial recognition deployments in public spaces. While the proposal does not mandate the deployment of facial recognition technology in public, interconnecting police databases of facial images lays the foundations for future abilities to feed live CCTV into those databases, creating the possibility of pervasive, pan-European biometric surveillance on a mass scale. Given this, we do not believe that the system as proposed, nor the possibilities that it lays the groundwork for, are necessary, proportionate or desirable in a democratic society.

Inclusion of driving licences

The Council's proposal to include driving licence databases in the Prüm network raises further concerns. While the ability to easily access the data stored in driving licences may well be useful to law enforcement agencies, that data is not collected for policing purposes, and it should not be possible to make routine use of that data for policing purposes.

The same point may be raised with regard to other UK government databases that hold facial images of citizens, residents or visitors to the UK, such as the passport database and the Immigration and Asylum Biometrics System.[10] The recent announcement by the policing minister that police officers should be able to "press one button" and "search it all" – including, for example, civil systems such as the passport database[11] – make these concerns even more urgent.

Police records

The option for states to interconnect their police records systems, while optional under the proposal, is being financially encouraged by the European Commission.[12] A "police record" is defined in the proposal as "any information available in the national register or registers recording data of competent authorities, for the prevention, detection and investigation of criminal offences." This broad definition could encompass vast quantities of files, including on people who have never been charged nor convicted of an offence, and including police

[9] 'Commissioner for the Use and Retention of Biometric Material, 'Annual Report 2020, November 2021, p.20, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1036487/E02669527_Biometrics_Commissioner_ARA_2020_Text_Elay.pdf

[10] TELEFI, 'Summary Report of the project "Towards the European Level Exchange of Facial Images"', January 2021, pp.146-7, https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf

[11] Tom Singleton, 'Police access to passport photos 'risks public trust'', *BBC News*, 5 October 2023, https://www.bbc.com/news/technology-67004576

[12] '"If you build it, the law will come": bypassing democracy to boost police powers', *Statewatch*, 8 September 2022, https://www.statewatch.org/news/2022/september/eu-if-you-build-it-the-law-will-come-bypassing-democracy-to-boost-police-powers/

records in the system would make troves of potentially incorrect, unwarranted or unverified data available for cross-border searches.

For example, with regard to the Metropolitan Police's 'Gangs Matrix', the Information Commissioner's Office found that the Met had set no data retention period, failed to erase data that it should have, processed excessive amounts of personal data, and that its processing of data was not "fair, lawful, or in accordance with [the law]." In and of itself, this has potentially extremely serious implications for the individuals concerned, a problem that would only be worsened were such a system opened up to searches by foreign police forces.

Ensure democratic debate and parliamentary scrutiny

The government's track record has shown that it is willing to override, without debate, Parliament's decisions regarding the Prüm system. We do not believe this should be allowed to happen again. Ultimately, we are of the view that the proposed changes to the Prüm system are not necessary, proportionate or desirable. We recognise that others will hold different views – but in any case, it is imperative that Parliament and the public are able to have a full and frank debate about the proposed changes to the system and the UK's participation in it prior to any decision being made. To do otherwise would be an affront to democratic procedure and endanger the rights and liberties of millions of people.

Signed

Statewatch (Europe)

Access Now (international)

Angela Daly, Professor of Law and Technology, University of Dundee

Big Brother Watch (UK)

Digitalcourage (Germany)

Elektronisk Forpost Norge (Norway)

Ella Jakubowska, Senior EU policy advisor on Prüm II at European Digital Rights network and alumna of LSE Human Rights

European Digital Rights (EDRi)

Fair Trials (international)

Habib Kadiri, executive director, StopWatch (UK)

IT-Pol Denmark

Liberty (UK)

Network for Police Monitoring (UK)

Open Rights Group (UK)

Politiscope (Croatia)

TechnopoliceBXL (Brussels, Belgium)