EU police departments preparing massive international facial recognition database

Kevin Reed
25 February 2020

Internal documents leaked to The Intercept show that the European Union (EU) is creating the legislative framework for implementing an international facial recognition database that will likely be integrated with a similar system already in place in the US.

The Intercept reported on Friday that an unnamed European official "who is concerned about the network's development" leaked information revealing that Austria is leading 10 EU police departments "to introduce and interconnect such databases in every member state." The Austria-led report states that face recognition is a "highly suitable" method for identifying suspects and should be implemented "as quickly as possible."

The report was circulated in November 2019 among EU officials and representatives from individual countries as part of ongoing discussions about the development of a continent-wide biometric data repository. Known as the Prüm system, the database enables DNA, fingerprint and vehicle registration data to be mutually searched by law enforcement and EU intelligence services across all 27 member countries.

The Intercept report states that the preparations for the legislation have included an investment of €700,000 (US$750,000) in a study by the consulting firm Deloitte "on possible changes to the Prüm system, with one part of the work looking at facial recognition technology" and €500,000 paid to a consortium of agencies to "map the current situation of facial recognition in criminal investigations in all EU Member States."

One of the leaked documents was a project presentation that was sent to national representatives in Brussels that outlined the goal of the initiative as moving "towards the possible exchange of facial data" among EU countries.

The Intercept report explains that legislation was passed by the EU last April that "established a database that will hold the fingerprints, facial images, and other personal data of up to 300 million non-EU nationals, merging data from five separate systems." When Deloitte initially proposed to the 10 police forces that facial images be integrated into this system, "the idea was met with unanimous opposition from law enforcement officials."

However, the police organizations recognize the value of having all European facial recognition systems linked with each other and with the US. The Intercept writes that as early as 2004, the US Embassy in Brussels was calling for "expansive exchanges and sharing all forms of data, including personal data." Since 2015, the Department of Homeland Security has demanded data sharing agreements with countries participating in the Visa Waiver Program.

Other US biometric databases have been integrated with Europeans more recently. According to Reinhard Schmid, a senior official in the Austrian criminal intelligence service who spoke to The Intercept, Austria began running fingerprints against the FBI's criminal fingerprint databases in October 2017. Since then, about 12,000 prints have been checked, leading to 150 matches. Schmid said, "Around 20 of these identified persons were under investigation and suspected of membership of terrorist organizations," while in 56 cases individuals had attempted to use a false identity.

According to a report in RT News, beginning in 2001 the US negotiated agreements to share both analytical and personal data between Europol and US law enforcement. "However, Europol's inability to collect the data itself meant it was dependent on what was supplied by member states. A facial recognition database in every nation, hooked into a central data-sharing network, creates an enviable transatlantic

© World Socialist Web Site

trough at which everyone's law enforcement can feed."

It is clear that facial recognition data is being gathered by local, national and international law enforcement organizations from states throughout the world and that the ability to link and integrate this information on globally searchable networks is becoming the norm. In the US, the mass surveillance of the population with facial recognition software is combined with scrubbing of social media accounts for facial images and other identity details.

There are no US laws governing this unconstitutional activity, which is a violation of at least the First and Fourth Amendments. A face image gathered by security services at an airport or at a highway toll booth can be combined with travel details and license plate information and stored into a federal criminal database without the permission or knowledge of the individual being photographed.

Discussing the EU moves to consolidate and share face profiles among states, Neema Singh Guliani, senior legislative counsel at the American Civil Liberties Union, told The Intercept that once the information sharing agreements are in place, there is nothing stopping data collected by the local police from being "shared with additional levels of U.S. law enforcement," such as the FBI, Homeland Security, the Central Intelligence Agency or the National Security Agency.

Guliani went on, "Their logic here is, 'When I have a serious crime and I want to run someone's photo against a database, why shouldn't I have this?'" Yet, she added, the privacy implications are enormous. "Once you have the access, you ultimately have the ability to identify almost anyone, anywhere."

The Intercept also spoke with Edin Omanovic, advocacy director for Privacy International, who said, "This is concerning on a national level and on a European level, especially as some EU countries veer towards more authoritarian governments." Omanovic also said he worries about a pan-European face database being used for "politically motivated surveillance."

With the growth of class conflict rising as well as the refugee crisis intensifying on every continent, the use of advanced artificial intelligence systems by the state to monitor the movement of every single person by way of biometric data is a serious threat. The use of authoritarian methods against individuals who have spoken up against injustice or anyone who has been labeled an "enemy of the state" will be on the rise.

At the center of these changes is US imperialism, where facial recognition tools are being perfected as part of a global system of perpetual surveillance, harassment, imprisonment, rendition, torture and assassination of its enemies. The working class can place no confidence in the bourgeois political order of any country to defend basic democratic rights. All talk of creating legislative frameworks for the use of facial recognition systems is both a cover-up of the advanced stage of their use today and the legitimization of their use tomorrow.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site