PHYS.ORG

Ethically designed databases can help police without reducing privacy

October 16 2017, by Paul Henman

Credit: AI-generated image (disclaimer)

Governments seem to think that the only way to protect national security is to own as much data about the public as possible, but this is not the case.

The push in Australia to create a national registry of driving licence photographs has been criticised for breaching privacy principles and creating data security risks.

By truly adopting "privacy by design" principles, it could still achieve its aims while addressing some of these concerns. Instead of creating a new mega-database, matching algorithms in each of the federal, state and territory's existing databases could be used to provide a similar function.

Computer design principles exist to protect individual privacy and enhance data protection. This can be designed into the system itself, rather than being treated as an afterthought.

The "Capability"

In early October, the Council of Australian Governments agreed to establish a National Facial Biometric Matching Capability, claiming: "This will help to protect Australians by making it easier for security and law enforcement agencies to identify people who are suspects or victims of terrorist or other criminal activity."

The aim is to create a new national driving licence registry that sits alongside similar sources for passport and immigration photos and documents.

Its Face Verification Service (FVS) allows law enforcement or other agencies to supply the image and name of a person and check if they match data held in the federal government's databases. It already operates with passport, visa and citizenship images, but driving licence images would now be included.

The government will also create a new Facial Identification Service (FIS): a user submits an image of an unknown person (say, a terrorism suspect), and if there's a match, the system will return their name and identifying information.

FIS will become operational with passport, immigration and citizenship images in early 2018, and driver's licenses afterwards.

Concerns about the system

The proposed extension of Facial Matching Services to driver's licenses has been met with wide political support, but also concerns about the erosion of privacy, increased risks of data hacking and mission creep.

The creation of a large database of personal biometric information has Orwellian connotations, and the wide-scale sharing of driving licence data would breach a key privacy principle: not using data that was collected for one particular use for another without consent.

DERMALOG
THE BIOMETRICS INNOVATION LEADER
3D Face with Live Check
Lorena Rivas
fication successful! Welcome Lorena Rivas

The National Facial Biometric Matching Capability will include driver’s license images. Credit: EPA/OLE SPATA

However, according to a spokesperson from the Attorney-General's Department, the government has addressed concerns by creating a segmented database "hosted by the Commonwealth" and "replicated" from state and territory road agencies.

Driver's license images will be stored in "a federated database providing each state and territory Road Agency with its own partitioned data store, with individual Agency-based access controls…and common facial biometric matching software, managed centrally by the Commonwealth Data Hosting Agency."

In other words, each collection of images will be controlled by the relevant state or territory, and provided to the federal government under data sharing agreements.

But while the Commonwealth can't automatically see the data, it's still creating a new copy and larger database that could be hacked. That's a key risk: as the database grows with more "valuable" personal information, it becomes a more attractive "honey pot" for hackers to target.

Privacy by design using distributed databases

There are design alternatives to creating a large central database that reduce the scope of data-sharing, infringements on privacy, and attractiveness to hackers.

By installing matching algorithms in each of the eight state and territory's existing driver's license databases, the government could achieve the functionality it requires.

In other words, instead of searching one large database, it would search multiple databases at once: the driver's license databases of each state and territory, the passport database and the immigration database.

A safer design?

A truly distributed would mean that if a state or territory's database was hacked, the scope of the data leak would be smaller.

While the federal government might argue that its centralised approach is faster and more efficient, this is unlikely to be true. Searching smaller databases simultaneously can be faster than one larger database.

Not to mention, under the federal government's approach, keeping the centralised database up to date would require regular transfers of new images, changes of address and so on.

A distributed database design would be more accurate and timely. When someone gets a driver's license for the first time, or updates their image, this is immediately installed onto the state or territory's existing system.

Building better computer systems is a necessary part of 21st century policing and national security, but it does not need to come at the expense of privacy and data protection.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Ethically designed databases can help police without reducing privacy (2017, October 16) retrieved 18 April 2024 from https://phys.org/news/2017-10-ethically-databases-police-privacy.html