On Uniqueness of Facial Recognition Templates

Michelle Chibba and Alex Stoianov
Information and Privacy Commissioner's Office of Ontario, Canada
March 2014

The following information attempts to respond to some questions about facial recognition technologies and their privacy impact.

1. If a biometric template is stored without other identifying information (e.g., name, metadata), is it still considered a unique identifier?

Information is considered personally identifiable (PII) if an individual may be uniquely identified either from this information only or in combination with any other information.

It is important to recognize that any information, whether it be numbers or alphanumerics, is rendered PII when linked to personal identifiers. One only needs to consider other examples of seemingly arbitrary but unique numbers (i.e. credit cards, passports, social security numbers, etc.), where misuse and theft have resulted in considerable anguish for the victims, to understand the harm that can result when this information is not secured.

Biometric systems function on the basis that templates can be linked to the identity of a person; without this data linkage, the biometric system is rendered useless. Therefore, the templates that are generated serve as a surrogate of a person's identity and are sensitive PII by virtue of the fact that they are linked to an identifiable individual.

The answer to the question of whether an individual may be identified based on a biometric template depends on what other information is stored with, or referenced by, the facial template. All that is needed to identify an individual is the submission of a tagged digital image (or another tagged template) of his or her face into the system. The biometric sample does not necessarily have to be captured by the deployed application sensor. It may be captured elsewhere and/or retrieved from another biometric database, be it government (e.g., DMV), proprietary, or public (e.g., Facebook). Therefore, the physical presence at the deployment site and/or the consent of the individual are not necessarily needed to perform the matching.

The uniqueness of biometric information (or PII strength) can be estimated by the decrease in uncertainty about the identity from a biometric measurement. For example, if the false acceptance rate (FAR) is set to 0.0001, the uncertainty decreases by a factor of 10,000.

For comparison, if age is used for identification, the uncertainty would decrease by a factor of about 80 (the average lifespan). Note that age is considered personal information (or PII) in all

jurisdictions. The important difference is that the age is usually verified based on documents (which can be forged) while biometrics is an inherent biological characteristic of individuals.

Therefore, it can be concluded that a face recognition template is PII, like any other biometric information.[1, 2]

2. Can a facial image be reconstructed from the template especially if the template generating algorithm is not known?

Sometimes it is claimed that template information cannot be reverse engineered or reconstructed into an image. The validity of this claim is very doubtful. In the past, the view of non-reconstruction was dominant in the biometrics community, especially if the template size was relatively small. However, over the last ten years, a number of scientific works were published[3,4] that showed that a fingerprint and face can, in fact, be reconstructed from the corresponding templates. This reconstruction is approximate yet the reconstructed image is sufficient to obtain a positive match in high percentage (often more than 90%) of cases.

For fingerprints, most templates comply with a fingerprint minutiae standard, so that the structure of the template, or at least a part of it, is known. For face recognition, there is no such standard yet. This gives some (false) grounds to the non-reconstruction claims. However, it should be noted that even though there is no facial template standard, many algorithms follow the same or similar approaches. Therefore, if the structure of the template becomes known (which will eventually happen), it will help to reconstruct the image.

However, there exist quite effective algorithms that do not even require the knowledge of the template structure. They test the template as a black box. All that is needed is the output matching score, even if it is quantized by the biometric system.

The examples of such reconstruction algorithms include:

- Hill Climbing Attack[5]: The attack starts with any impostor image. It is run against the template in question. By making small changes in the impostor's image, the attacker watches how the score changes. If it increases, the change is retained; if not, the attacker

---

[1] "By definition, a reference template created from an image of an individual is also personal data as it contains a set of distinctive features of an individual's face which is then linked to a specific individual and stored for reference for future comparison in identification and authentication/verification." . Opinion 02/2012 on facial recognition in online and mobile services, Article 29 Data Protection Working Party, 00727/12/EN WP 192, 22 March 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

[2] For fingerprint-based biometrics, see IPC publication: Ann Cavoukian, "Fingerprint Biometrics: Address Privacy Before Deployment". IPC, 2008. http://www.ipc.on.ca/images/Resources/fingerprint-biosys-priv.pdf

[3] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates", IEEE Trans. Pattern Anal. Mach. Intell. 29(9):1489–1503, 2007.

[4] Jianjiang Feng and Anil K. Jain, "Fingerprint Reconstruction: From Minutiae to Phase". IEEE Transactions on Pattern Analysis and Machine Intelligence, VOL. 33, NO. 2, 2011.

[5] A. Adler, "Sample images can be independently restored from face recognition templates". In Proceedings of the Canadian Conference on Electronic and Computer Engineering, 2003, pp. 1163–1166.

tries a different change. After a number of iterations (usually a few thousand), the attacker may be able to pass the threshold. The resulting modified impostor's image resembles the original image from which the template was generated.

- Break-in Set Attack[6]: An independent break-in set (usually a few hundred) of face images is chosen from a database compatible with the target biometric system. Then an affine transformation of the images is applied to approximate the behavior of the face recognition system. The templates from the break-in set are matched only once with the target template and matching scores are recorded. These scores are then embedded in the approximating affine space along with break-in set templates to compute the co-ordinates of the target template. The inverse transformation is used to reconstruct the approximate target image.

The examples of the Break-in Set attack are shown below. The reconstructed images show striking resemblance with the originals. The attack against a commercial off-the-shelf face recognition system was successful (meaning that the matching score exceeded the threshold) in 93% of cases.

Adapted from P. Mohanty, S. Sarkar, and R. Kasturi, "Privacy and security issues related to match scores", in IEEE Workshop on Privacy Research In Vision, CVPRW, 2006.

[6] P. Mohanty, S. Sarkar, and R. Kasturi, "Privacy and security issues related to match scores", in IEEE Workshop on Privacy Research In Vision, CVPRW, 2006.

3. **Can two facial templates created for the same person but by different algorithms be linked?**

The answer is Yes, based on the above-noted results of the image reconstruction from the template. If, in addition, the structure of both templates is known, they often can be made compatible with each other. In the future, a standardization of facial templates can be expected.
In general, counting on the proprietary nature of the facial algorithms is a notorious "security by obscurity" practice.

4. **Does breaking into the template, image reconstruction, and template linking require a sophisticated attacker with a Ph.D.?**

This argument is sometimes used by attorneys representing biometric proponents in judicial and quasi-judicial (e.g., labor tribunals) hearings. As seen from the previous subsections, the (indeed) sophisticated algorithms have already been developed, peer reviewed and published. All is needed is to create a software application and make it available. This task can be performed by many programmers or computer science students. Then virtually anyone will be able to use the application.

IPC/March 2014