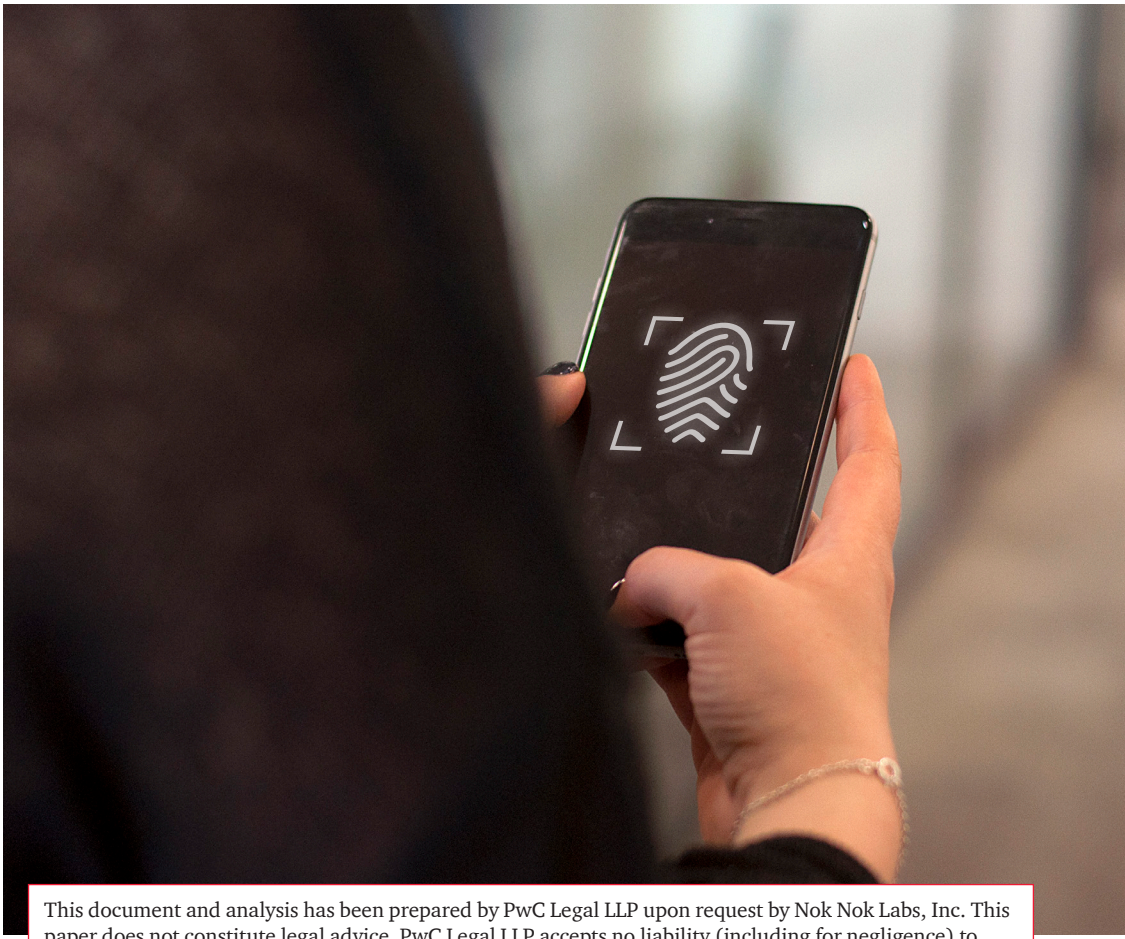
Biometrics and Privacy
On Device vs On Server matching

May 2016

Nok Nok LABS



This document and analysis has been prepared by PwC Legal LLP upon request by Nok Nok Labs, Inc. This paper does not constitute legal advice. PwC Legal LLP accepts no liability (including for negligence) to anyone else in connection with this document.

pwc

PricewaterhouseCoopers Legal LLP

Executive Summary

Biometric data processed for authentication and verification purposes is generally considered personal data, as it can be used to confirm the unique identification of an individual. As such, the processing of biometric data is subject to data protection and privacy laws.

Biometric authentication and verification can be one of the most secure ways to control access to restricted systems and information. Unlike authentication based on traditional passwords, authentication using biometric data, which is unique to an individual, is easier to use in practice, and can be far more secure. However, this is a double-edged sword. As a result of its uniqueness and how intrinsic it is to a specific individual, biometric data is particularly sensitive. As such, additional efforts must be made to keep this data secure and confidential including choosing a proper compliance system and infrastructure, which takes into account the particularly sensitive nature of biometric data.

Biometric systems generally fall into two categories. The first involves an individual's biometric data being compared against biometric data stored centrally on a system, to verify if there is a match. This is often described as a "one-to-many" system, or server-side biometric enablement. The second involves an individual's biometric data being compared against biometric templates stored locally on a device. This is called a "one-to-one" system, or device-side biometric enablement. This paper will highlight the main privacy consequences and differences between the two categories; matching biometric data on server vs. on device.

Although biometric data covers physiological, behavioural and psychological data, this paper considers the privacy implications of processing (including storage and transfer) of physiological and some behavioural biometric data. This includes: fingerprints, iris patterns, retina scans, facial recognition, voice recognition, gait analysis and even body odour detection, although it is important to note that this list is constantly evolving through technology innovations.

While some jurisdictions have already specifically referenced biometric data in privacy guidance and legislation, most countries have not yet developed specific laws that address the collection and use of biometric data. Despite the lack of express legal provisions covering biometric data, all jurisdictions covered by this paper consider biometric data to be personal data and in some countries, for example in Australia, biometric data is classified as sensitive personal data. The upcoming European General Data Protection Regulation expressly identifies biometric data as a category of sensitive personal data.

This paper sets out the key privacy implications of processing biometric data in the EU and Switzerland, Canada, USA and the Asia Pacific region (covering Japan, Singapore, Hong Kong and Australia). This paper will touch on legislation and best practice recommendations in these jurisdictions without going into the details of specific laws.

Stewart Room

PricewaterhouseCoopers Legal LLP | Partner
Direct: +44 (0) 20 7213 4306
Mobile: +44 (0) 7711 588 978
Email: stewart.room@pwclegal.co.uk

1 Embankment Place, London WC2N 6RH

Overview of privacy requirements when processing biometric data

There are a number of globally accepted privacy principles that apply to the processing of biometric data, notably, transparency, individual choice and control, security and confidentiality, cross-border transfers of data and data quality. The associated privacy requirements that organisations need to be aware of when processing biometric data are outlined in this section.

Note, as a preliminary consideration, prior to processing personal data (including biometric data), it is currently best practice for organisations in Europe and Canada to carry out privacy impact assessments to consider the impact new or materially different data processing has on affected individuals' privacy and the organisation's compliance with applicable privacy rules. The final draft of the General Data Protection Regulation in the EU expressly identifies biometric data as a special category of data, and states that a privacy impact assessment should be performed in cases where biometric data are processed.

Transparency

The gathering of fingerprints, iris scans and retina images usually requires the individual to be in close proximity to the reading device. However, advances in technology have allowed the collection of this type of data to be less intrusive, and as voice, facial and gait analyses becomes more prevalent, the risk of covert or incidental collection of biometric data significantly increases.

As biometric data is generally considered to be personal data it is crucial that all users, regardless of how their biometric data is stored, are notified of the collection of their data and provided with information about what the organisation is doing with it.

The EU and Australia, in particular, require the individuals to be informed of who is collecting their data, why their data is being collected, how their data will be used, where their data will be stored and who will have access to that data. This is often achieved through the use of an accessible privacy policy.

Individual choice and control

Freely given, informed consent is required before processing biometric data in almost every jurisdiction looked at in this paper. The protocols for how this consent is obtained vary but they generally require the consent to be specifically given once the data subject is made aware of all the uses for their biometric data. For consent to be valid, the EU requires it to be freely given, specific, informed and an indication of the data subject's wishes. "It must be clear that such consent cannot be obtained freely through mandatory acceptance of general terms and conditions, or through opt-out possibilities, furthermore, consent must be revocable."[1] In Switzerland the data subject must consent to each international transfer of their data and a generic consent covering multiple transfers is not permitted, which may be extremely burdensome for an on-server system that requires the constant transfer of biometric information to and from multiple locations.

In addition, it is a generally accepted privacy principle that individuals must be able to access their data and correct it where necessary. This means that organisations are required to ensure that individuals can access their biometric data as and when they request it. Further, organisations should have processes in place to allow individuals to correct, update and delete their data where necessary.

1 - Article 2(h) of the Data Protection Directive

Security and confidentiality

Security and confidentiality of data are fundamental privacy requirements. Biometric data is considered to be sensitive personal data in some of the jurisdictions covered by this paper, which means that enhanced levels of security are required. Organisations must establish technical and organisational measures to protect biometric data from unauthorised access and other unlawful processing operations. In addition, staff with access to biometric data must be trained on how to handle and protect such data. Staff and suppliers must also be vetted to ensure that they are reliable. The next section of this white paper compares the privacy implications in relation to matching biometric data on server vs. on device, and security is one of the key differences addressed.

Some jurisdictions also require data breaches to be notified to affected individuals and regulators and specific contractual provisions to be put in place when third party providers are used to process biometric data.

Cross-border transfers of personal data

There is a general prohibition on cross-border transfers of biometric data in most of the jurisdictions covered by this paper as biometrics are considered personal data. Therefore, when storing biometric data on a central server/in the cloud, organisations must be mindful of the restrictions on the transfer of biometric data across borders. Some exemptions to the general prohibition exist, such as obtaining consent from individuals or ensuring that the cross-border transfers are only to countries that ensure an adequate/similar level of protection for the rights of individuals.

Personal data quality

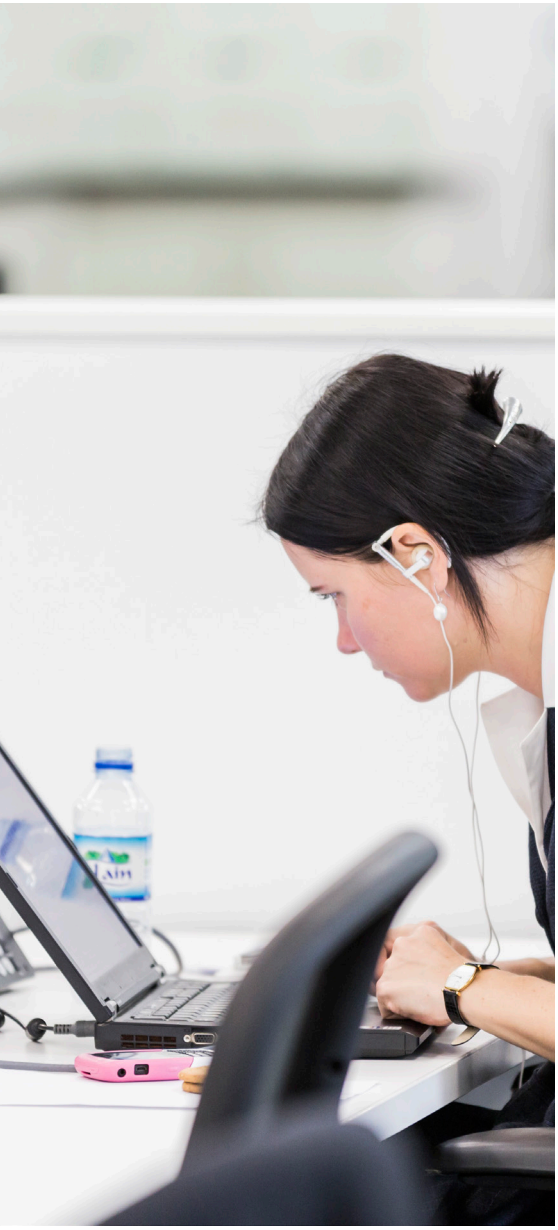
There are commonly accepted data quality principles in place in all jurisdictions covered by this white paper. This means that any biometric data must be adequate and accurate, be relevant and up-to-date, not be excessive and not be kept for longer than necessary to achieve the purpose for which it was collected. It is vital that biometric data collected is adequate and not excessive for the purpose of authentication and verification, and that retention periods are set determining how long such data is stored. Further, accuracy of the biometric data is key, particularly in relation to the "one to many" approach to authentication, which could potentially increase the risk of inaccurate matching of the data when such data is inaccurately recorded.

Summary table – the main privacy differences between matching biometric on server vs. on device

Privacy Issue	*On Device*	*On Server*
Individual choice and control	Individual choice and control means that the individual must be able to withdraw permission to use their data at any point; this is simpler where biometric data is stored on a local device as **the individual has far more control over the data** because they can just delete it. In addition, authentication systems such as those based on the FIDO™ authentication protocols[1] allow the user to revoke permission at any point by de-registering from the service.	Both the controller and processor will have to have in place **policies to ensure that once permission is revoked the data is adequately destroyed**. They must also be able to identify quickly what data they hold for each user and ensure it is disposed of when required to do so. This is especially important in the EU as the data subject will have the right to issue a subject access request under the Data Protection Directive.
Security and confidentiality	Each device will in principle only retain its own user's biometric data, as opposed to retaining the biometric data of a large number of individuals. As such, the volume of biometric data at **risk is lower** when compared to the volume of biometric data at risk on a server, which will typically store the biometric data of a multitude of individuals. This lowers the level of risk because a hacker is more likely to target a single database repository where they could access the data of that multitude of individuals, rather than a specific individual's device where they would only access that particular individual's data. It must be noted however, that in the event of a successful attack on a specific device, the data accessed is likely to provide a more detailed profile of the device's owner due to the wealth of personal data generally stored on an individual's device. There will generally be no involvement of 3rd parties to host the biometric data stored on device, unless the individual initiates and consents to such involvement, for example, by backing-up a device to the cloud or allowing a mobile application to access the biometric data.	Although not technically prohibited, the EU, Canada and Singapore advise strongly against the use of centralised biometric storage unless entirely necessary. The Art 29 working paper states biometric databases should be avoided if possible. With centralised storage of biometric data, the **potential for large-scale loss of data is increased dramatically** and, therefore, additional security measures must be put in place. Examples such as the 2015 biometric data loss in the USA and the 2011 loss in Israel show that there is a real risk for this type of database. The transfer to a 3rd party requires the original data collector to maintain control over the data and is legally responsible for the data at all times. Hong Kong specifically requires that consent to transfer the data to 3rd parties is obtained before the data is collected.
Cross-border transfers of personal data	As the data will remain on the device there will be **no transfers of the biometric data**, other than those instigated by the user such as back-ups to the cloud, or cross-border travel with the device storing the biometric data (see section on individual choice and control).	A global network of biometric authentication users will require **international transfers of biometric data**. The transfer of personal data out of a jurisdiction is generally restricted and most jurisdictions enforce stringent requirements. These are especially notable in the EU and Singapore. Hong Kong is also expected to introduce legislation banning certain international transfers in the near future.

1. The FIDO™ Alliance is a non-profit organisation that aims to develop specifications and certifies interoperable products for stronger, simpler online authentication, including through the use of biometric authenticators. The FIDO™ specification privacy principles are designed so that the individuals' credentials remain on device, and are not shared with the service provider. For further information on FIDO™ Alliance please check www.fidoalliance.org.

The main privacy differences between matching biometric on server vs. on device



User choice and control

As outlined in the table on the previous page, storage and matching of biometric data on device inherently gives users more control over their personal data when compared to storage and matching of biometric data on server and, as such, is consisent with privacy best practices to provide an individual control over his/her personal data.

It is also globally accepted that organisations must provide individuals with choice in relation to the collection, use, transfer and disclosure of their personal data. Specifically, the Asia-Pacific Economic Corporation privacy principles state that "individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information"[1]. Technologies that give users control over their biometric data by storing it on device, and therefore, allow users a choice over which (if any) biometric data are collected and shared are, therefore, preferable from a privacy perspective.

A key criterion in the EU, Hong Kong and Switzerland is that the consent is freely given; therefore the system must allow for the user to both refuse to give their consent and revoke their data if required. An automatic enrolment system or one where the user cannot access the system without giving their biometric data would not be allowable under EU data protection law. Both on device and on server systems would need to have protocols in place to ensure this could be complied with.

Security and confidentiality

The creation of large databases of personal data such as biometrics data is not a new concept. At one point due to the cost and speed of the technology only public bodies could justify systems to collect biometric data. However with the latest technological innovations, currently both public and private bodies collect and store vast quantities of biometric data. Often this is done in the name of public security, immigration control or consumer profiling. The USA for example retains the fingerprints of every visitor entering the country along with their name, address and passport number. India is in the process of building the world's largest biometric database of all its' 1.3 billion citizens data.

The collection and subsequent storage of biometric data brings significant security risks when conducted on such a large scale. The Office of the Privacy Commissioner of Canada states in its guidance that "centralised storage [of biometric data] heightens the risk of data loss or the inappropriate cross-linking of data across systems"[1]. A number of high profile attacks on

1 - APEC privacy framework (http://publications.apec.org/publication-detail.php?pub_id=390)
2 - Data at your fingertips – Biometrics and the challenges to privacy (Office of the Privacy Commissioner of Canada)

large biometric databases have already happened. In October 2015, over 5.6 million fingerprint records were stolen from the US Federal Government Office of Personnel Management in the USA and in 2011 the records of over 9 million citizens were lost in Israel. As biometric data, unlike other data such as passwords, cannot be changed, once biometric data is exposed, it is difficult to mitigate the breach by asking the user to change his or her authentication data because an individual's fingerprint or iris is permanent and cannot be changed. Losses such as this could be prevented by comparing an individual's biometric data to a template embedded in an official document (e.g. passport) or via an on device application, instead of retaining large databases of biometric data.

EU and Canada

Due to these serious security concerns, Canada and the EU privacy authorities strongly advise against the storage of biometric data on large databases unless it is absolutely necessary. This is especially the case when it comes to verification systems where alternative solutions can be just as effective, such as the use of RFID tags. The EU's Article 29 Working Party on biometric data "warns of the risks involved in the use of biometric data for identification in large centralised databases, given the potentially harmful consequences for the person connected" and further goes on to advise that "whenever it is permitted to process biometric data, it is preferable to avoid the centralised storage of the personal biometric information".

The Office of the Privacy Commissioner of Canada has published guidance on the storage of biometric data stating that companies should:

- Record a summary of the biometric data rather than the image itself to reduce the likelihood of biometric data being used for a different purpose that may be unauthorized;
- Store biometric information locally rather than in centrally located databases to minimize the risk of data loss or inappropriate cross-linking of data across systems; and
- Use biometric data to authenticate the identity of individuals, which involves the matching of one biometric sample to one sample on record. Avoid using biometric data to identify individuals, which involves matching one biometric sample against all records in a database. One-to-one matching reduces the risk of false matches and data breaches.

Cloud - supply chain

Although the collection of biometric data and subsequent storage of such data on a server could be done by the same company, in practice this would be highly unusual. Mass storage of biometric data on a server will, for many organisations, inevitably mean using a third party supplier to host the data in the cloud. There are privacy implications with using third parties to process personal data and the organisation in control of the collection and use of the data must ensure that the third party keeps that data secure and confidential. If there is a data breach, it is the organisation that collected the personal data that will be held responsible under data protection legislation, not the third party supplier. Organisations using third parties to host biometric data, therefore, need to carry out due diligence on the supplier, have appropriate contracts in place and carry out ongoing monitoring to ensure that the third party meets its contractual obligations.

Cross-border transfers of personal data

An 'on server' system necessitates the transfer of data from the device to a single database. Therefore, multinational 'on server' offerings are likely to require the transfer of the biometric data out of a jurisdiction to the single database (that may be hosted on one or across many servers). This is not a concern for an 'on device' system because the data stays on the device and there is no transfer of biometric data to an outside server unless so intended by the individual user.

Every jurisdiction covered by this white paper holds the transferor liable for the security of the personal data even when that data is outside of the jurisdiction.

Most jurisdictions covered by this paper have a non-absolute prohibition on the transfer of personal data (which includes biometric data) across national borders. Although the specific nature of the restrictions on transfers varies between the jurisdictions, there are commonalities in approaches to data transfers across the jurisdictions. For example, the prohibition can generally be subverted: (1) by obtaining the consent to the transfer from the individual; or (2) if the transfer is to a jurisdiction providing an adequate/similar level protection to the rights of individuals.

EU

The EU has set out specific criteria in the Data Protection Directive around transfers of data to ensure that transfers only take place:

- Where the recipient country has been considered by the EU Commission as affording an appropriate level of protection to the transferred personal data;
- If the sender and the recipient have entered into a personal data transfer agreement pursuant to the standard contractual clauses approved by the EU Commission;
- If the intended personal data transfer is covered by approved Binding Corporate Rules;
- In specific and legally defined circumstances such as if the data subject has given his or her consent to the personal data transfer; or
- When the transfer has been approved by the relevant supervisory authority for data protection.

The decision of the Court of Justice of the European Union in the landmark case of Maximilian Schrems v Data Protection Commissioner (C-362-14) ruled the transfer of data to the USA under the established safe harbour system was unlawful and has focused attention on international data transfers and reinforced how important it is to ascertain whether the data transfer is legitimate.

Switzerland and APAC

Switzerland and most Asia Pacific countries require a similar protection to that afforded in the Data Protection Directive above and specifically mention that the transfer of data must be to a jurisdiction that offers a substantially similar level of protection.

Canada

Under Principle 4.1.3, Schedule 1, Personal Information Protection and Electronic Documents Act (PIPEDA) Canadian companies must contractually ensure that the recipient country offers a similar level of protection.

USA and Hong Kong

The USA and Hong Kong do not generally restrict the transfer of biometric data outside of their borders; however there is legislation in development in Hong Kong that may limit these transfers in the future.

The restrictions on the cross-border transfer of personal data, outlined above, demonstrate the legal complexity faced by organisations that choose solutions that match biometric data on server as opposed to on device.

This legal complexity does not apply to matching of biometric data on device as any transfers of such data are under the control of the individual.

Conclusion

Biometric data is personal data (and some jurisdictions consider it to be sensitive personal data). There are common privacy requirements in place that govern the processing of personal data in the EU and Switzerland, Canada, the USA and the Asia Pacific Region. Compared to 'on server' storage of biometric data, the storage and matching of biometric data 'on device' for authentication purposes is a compelling and easier approach to satisfy global privacy requirements on cross-border personal data transfers, and individuals' choice and control around such personal data. The 'on device' storage of biometric information is gaining momentum, as evidenced by the growing support for solutions incorporating FIDO™ authentication protocols.