Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 480 - 487), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1086

Malaysian Journal of Social Sciences and Humanities (MJSSH)

Volume 6, Issue 10, October 2021

e-ISSN : 2504-8562

Journal home page:
www.msocialsciences.com

A Study on the Laws Governing Facial Recognition Technology and Data Privacy in Malaysia

Muhammad Ashraf Bin Mohd Nor [1], Mohammad Asyraf Bin Mohd Tasrib[1], Bryan Francis[1], Nurul Izzah Binti Hesham[1], Mohd Bahrin Bin Othman[1]
[1]Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia

Correspondence: Mohd Bahrin Bin Othman (mohdb916@uitm.edu.my)

Abstract

The advancement of technology in the past decade has led humans to achieve many great things. Among that is facial recognition technology that uses a combination of two techniques which is face detection and recognition that is capable of converting facial images of a person into readable data and connecting it with other data sets which enable it to identify, track or compare it. This study delves into the usage of facial recognition technology in Malaysia where its regulation is almost non-existent. As its usage increases, the invasive features of this technology to collect and connect its data posed a threat to the data privacy of Malaysian citizens. Due to this issue, other countries' laws and policies regarding this technology are examined and compared with Malaysia. This enables the loopholes of the current law and policies to be identified and restructured, which create a clear path on the proper regulations and changes that need to be made. Thus, this study aims to analyse the limitation of law governing data privacy and its concept in Malaysia along with changes that need to be made. This study's finding shows the shortcoming of Malaysia's law in governing data privacy especially when it involves complex technology that has great data collection capability like facial recognition.

Keywords: facial recognition technology, privacy, personal data privacy, Personal Data Protection Act 2010, General Data Protection Regulation 2018

Introduction

Facial Recognition Technology (FRT) has been acknowledged as a mechanism for better surveillance and crime deterrence purposes (Morris, 2019). The existing law in Malaysia is incomprehensive in regulating the biometric-based surveillance technology specifically to avoid violation of data privacy and the right to life. In the case of Sivarasa Rasiah v Badan Peguam Malaysia (2010), our legal system has formally recognised the right to privacy as part of the constitutional right. In this case, the right to privacy has been confirmed as one of the rights to personal liberty as stated in Article 5(1) of the Malaysia Federal Constitution. Salleh (2019), stated that the right to privacy has three aspects which are the right to be alone, to have control over one's personal information and the right to have a set of conditions necessary to safeguard one's self-dignity and independence (Buang, 2019).

The Personal Data Protection Act 2010 (PDPA) is the closest when it comes to the law on privacy in Malaysia. According to section 6 of PDPA, sensitive personal data cannot be used other than for the purpose it was lawfully taken for. Under section 4, 'sensitive personal data' means any personal data consisting of information about one's physical, mental health, body condition, political opinion,

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 480 - 487), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1086

religion or any other information of the same nature. Due to the express exception in Section 3 of PDPA, the federal and state government are not under the act's jurisdiction. The act is also silent upon procedures for a data breach, civil remedies and the right for data deletion.

The lack of comprehensive rules governing data protection in PDPA formed the major part of this study which seeks to investigate problems that may arise when protecting personal data privacy in FRT via this act. The rest of the study seeks to investigate the capability of FRT in causing the violation of data protection while also seeking the best methods available to mitigate the weaknesses of PDPA in such matters. The vague provisions and limited application of PDPA poses a great threat to Malaysian personal data privacy since this act is supposed to protect their data.

The PDPA is also criticised especially upon its narrow application which only restricts its applicability on commercial use of data inside Malaysia only. It is stated in section 2(1) that the act only applied in commercial transactions which greatly minimise its scope of jurisdiction such as the usage of data in social media, government's database and other non-commercial entities. Furthermore, in a recent development, Malaysia's Personal Data Protection Commissioner also reportedly wants an update on the current PDPA following the country's adoption of FRT into the surveillance system (Pascu, 2020). This developing scenario consequently discloses the need for more thorough policies and guidelines to be established before fully adopting this technology in Malaysia. Thus, form a reliable basis to doubt the safety of our personal data privacy upon the implementation of FRT in Malaysia.

Literature Review

In general, many studies have been written regarding the impact of FRT upon the privacy of the public at large. The majority of those studies have included breaches of data privacy among various concerns that they emphasized inside their studies and articles while also mentioning several complex features relating to this technology which make it difficult to tackle data-related issues.

The Notion of Data Privacy

People are often confused between the concept of privacy and data privacy. Nissenbaum (1998), explains the concept of data privacy using the term 'contextual integrity' where it forms part of the condition to privacy. When information governing norm is followed by using data given by the people for the purpose it was given, it would respect the contextual integrity. However, when that information is used in an inappropriate context, this norm is not followed thus, violating the contextual integrity. Nissenbaum (2010), in another study, clarified that the notion about data privacy is neither the right to secrecy nor the right to control but, a right to a suitable flow of information and personal data. Black, Setterfield and Warren (2018), explain data privacy using the definition used by Gormley which is the ability of citizens to regulate their information and the definition by Solove, which is the power to control one's personal information. For consistency, the notion of data privacy by Nissenbaum will be utilised in this study.

In Malaysia's context of law regarding data privacy, PDPA has provided for data privacy concerns. Munir and Mohd Yassin (2012) stated that PDPA has provided six rights which are the right to be informed, to access our personal data, to correct it, to retract consent, to prevent data processing likely to cause damage or distress and to prevent data processing for direct marketing. Balasingam and Qamar Siddique (2017) states although PDPA is not perfect to protect our personal data, it is seen as a good start and even if Malaysia's judiciary is yet to fully recognise data privacy as a right it is high hope that the judiciary is heading toward a right direction.

The Concept of Data Protection

Data protection and privacy are considered fundamental rights in the European Union (EU) and applicable in the law enforcement context. Their understanding of these rights begins in 1970 by the comprehensive case law of the European Court of Human Rights (ECHR) and was further developed in

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 480 - 487), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1086

recent years through some important EU instruments such as the Directive 95/46/EC, the Treaty on the Functioning of the European Union and the Charter of Fundamental Rights, as well as the EU courts' case law. Boehm (2015) states that data protection has been guaranteed to exist at the primary law level since 2009 when the Lisbon Treaty came into force. Additionally, Article 16 of the Treaty on the Functioning of the European Union (TFEU) explicitly refers to the individual right to data protection and lays down procedural rules for the legislative process in these matters. It reflects the right to data protection established in Article 8 of the Charter of Fundamental Rights and stipulates the competencies of the EU in data protection related matters. It also extends to substantive data protection guarantees, particularly the control of independent authorities. Apart from that, Articles 7 and 8 of CFR also provide a comprehensive right of protecting both personal data and life privacy which emphasized the significance of data protection as an important fundamental right within the framework of EU's law. For instance, Article 8 (2) of CFR requires the processing of data must be based on consent or another legitimate legal basis.

It also highlighted the rights of access and rectification regarding a person's right to get information whenever their data are processed and question its purpose. To summarize, the existence of the EU's perspective of privacy and data protection as comprehensive fundamental rights, there are several principles which formed the data protection in the EU, Boehm (2015). They include, rules on data quality standards, on sensitive data, independent supervision, the purpose limitation principle, rules on the inter-agency exchange or transfer of data to third states and other rules similar in nature.

In Malaysia, data protection is governed through the PDPA. Munir and Mohd Yassin (2012) stated that Malaysia has section 42 (1) of PDPA that allows a data subject, at any time by notice in writing to require the data user, to cease or not to begin the processing of, or processing for a specified purpose or in a specified manner, of any personal data on the certain grounds. However, this provision does not define the exact extent of the substantial damage or distress to an individual's right which makes the issues relating to it unclear and debatable.

The Conflict of Data Privacy in Facial Recognition

The conflict between the protection of data privacy and the FRT which utilise those data is inevitable. This issue has been discussed frequently in numerous studies. Brey (2004) focuses more on the ethical aspect of FRT in public places. He explains four problems of FRT via Smart CCTV in public have, which are errors from the system, function creep, lack of policies and privacy issues. According to Nissenbaum in Brey's (2004) study, the practice of data aggregation, which is the act of gathering different sources of information on people to produce databases, violating the public's privacy expectation. Another criticism was also being voiced out in a study by Andrejevic and Selwyn (2020) about facial recognition technology in school. Among the issues being raised are the problem of 'mission creep' and the overreaching of this technology such as by creating detailed databases on people's actions which raised serious concern regarding our personal information and its usage in FRT. This is quite similar to Brey's issue of data aggregation. Andrejevic and Selwin (2020) stated that this technology is altering the way people perceive what 'being out in public' is and under this technology, people cannot restrict what they share because the data is their face hence exposing people to constant surveillance.

Zorkadis and Donor (2004) suggested that to minimise the risk of non-compliant to privacy protection legislation and to increase data users acceptance, FRT must follow the data protection principles, purpose, proportionality and security, provided in international legislation. Their research has summarised the importance of complying with the principles of data protection legislation by the Biometric systems and data controllers since they create and process personal data. To find out whether a biometric system fulfils the legal obligations, the principles of purpose and proportionality of biometric-based identification should be applied when processing personal data.

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 480 - 487), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1086

In the United States (US), the majority of their states use FRT across all agencies. However, the first state to ban this technology after its implementation is the state of San Francisco via its legislators who have voted unanimously to ban the use of FRT for all local agencies especially for the law enforcement and transport authority. Among the reasons for the banning is to protect the public from possible bias, inaccuracy and to maintain their liberty and privacy. After San Francisco, Oakland and the city of Somerville also passed their ban upon their city's usage of FRT (Zeng et al. (2019).

In Malaysia, there are very limited studies and articles that touch upon the FRT in the local context due to its lack of interest until recent years. In one of the studies, the purpose of using FRT is for criminal identification as stated by Abdullah at al. (2017). The identification of criminals via thumbprint is outdated as criminals are cleverer and fully aware of this method of criminal identification. Hence, it creates problems for forensic to detect the existence of a thumbprint as criminals are very careful in not leaving it on the scene. FRT will indeed benefit criminal security in detecting criminals but lack of discussion regarding the consequences of using, storing or processing the personal data of the public would result in a breach of privacy of one's personal information. However, this study only focuses solely upon facial recognition systems on criminal identification whereas, our study seeks to investigate a wider area of this technology in terms of data privacy in Malaysia.

The literature review above has highlighted an undeniable number of studies conducted and written on legal research of data privacy around the world. However, it must be pointed out that there has been no study on laws of data privacy protection and FRT done in Malaysia yet. This study seeks to close the gaps of knowledge regarding FRT in Malaysia by carefully analysing its impact on data privacy in this country and finding out possible solutions to mitigate future conflicts.

Methodology

This is qualitative research and utilised the doctrinal approach and comparative research methodology. Firstly, the doctrinal approach is a method that focuses on analysing case-law, statutes and other legal resources as they are. This method is used because this study seeks to do an in-depth analysis of the law governing Malaysia's personal data and the effect of FRT on it. For example, PDPA, EU General Data Protection Regulation (GDPR), EU Charter of Fundamental Rights and other legal resources on personal data. To keep this study relevant, data and information of the most recent study were used for both the primary and secondary sources. The primary sources of law are obtained via a comprehensive analysis of the law governing personal data in Malaysia, the EU, the US and other countries which have long adopted facial recognition systems. The PDPA is the primary focus for this method as it is the sole law that directly governs personal data that are the focus of this study.

Secondly, the comparative approach is an important method used in this study which intended to compare the elements of similarities and differences between Malaysia's law and policy on data privacy in FRT with other EU and US stances upon similar matters. It enabled the data privacy issues in FRT to be viewed from various angles of laws and demographics which greatly increased this study's contents. The EU's policy on data privacy especially regarding its usage in FRT are compared with Malaysia's policy and law on the same issue. Aside from the EU, this study also compared with the position in the US. All of this comparison and analysis is done to carefully identified the loopholes regarding data privacy in Malaysia's context and explored possible improvements that can be made when using FRT.

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 480 - 487), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1086

Result

Inadequacy of PDPA in Ensuring Data Privacy

The PDPA is the sole law that governs data privacy in Malaysia. Although various other laws touch upon privacy or data privacy like the Computer Crime Act 1997 and Digital Signature Act 1997 but, these laws are only specified in limited areas and do not cover data privacy in general. In contrast, the PDPA is enacted specifically to cater to the need for personal data privacy regulation in Malaysia in light of progressive improvement of the internet where personal data is crucial. However, this act has its limitation when it comes to certain areas including FRT. This limitation can be observed in section 3 where this act does not apply to federal and state government and also any personal data processed outside Malaysia unless intended to do so in Malaysia. It also has a very limited definition of 'personal data' that are confined to data use in commercial transactions only. Additionally, this act does not provide a clear definition of 'consent' which enables improper collection of consent. Other than that, PDPA is also silent upon the matter of safety procedures in processing personal data including guidelines that must be followed when there is a data breach.

Privacy in Facial Recognition Technology in Malaysia

This study also finds that the principle of privacy or specifically, data privacy is almost non-existent under FRT in Malaysia. This is because data processed in FRT is not applicable under PDPA due to the limitation of personal data meaning under the act that is only applicable for data used for commercial transactions whereas, most FRT are used for surveillance and security. Moreover, FRT that are utilised by the government itself is also not applicable under PDPA due to section 3. These limits set by the act deny proper data protection rights upon FRT which raise serious concerns on privacy as the data used by this technology are highly sensitive data that per Nissenbaum (2010), are open to various abuse including data profiling and tracking which violate the general expectation of privacy. The capability of FRT also made it a highly intrusive technology because it can collect data without the data subject's awareness and proper consent. Adding the weak and limited law under PDPA into consideration, it can be concluded that personal data used by FRT in Malaysia are very prone to abuse due to a severe lack of data protection elements.

Discussion

There are a few recommendations that can be made to improve personal data privacy concerning the usages of FRT in Malaysia. It focuses on the PDPA as the sole law governing this matter where a few areas need immediate improvement with the GDPR as the gold standard. The role of the Ministry of Communication and Multimedia is important in amending the current PDPA by fixing and improving the right provisions. The recommendation will also touch upon some new laws that can be used to improve data privacy in FRT and also the role of the public in this matter.

Establishing a Clear and Precise Meaning of 'Personal Data' and 'Consent'

The recommendation that must be made is to widen the meaning of personal data and abolish the requirements for it to be for commercial transactions purpose only in section 4. This would put other data used beyond commercial transactions purposes, particularly in FRT to be under PDPA's jurisdiction. This is because most data used under FRT are not for commercial transactions but for security and surveillance purposes where the limited definition of 'personal data' significantly reduces the applicability of PDPA in protecting personal data when used by this technology. The meaning of 'personal data' must be improved by clarifying that it includes any data that can be identified or identifiable to a natural person directly or indirectly using any references. This would ensure facial image data used in FRT are included in PDPA and be subjected to personal data rights.

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 480 - 487), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1086

The next recommendation is to clarify the meaning of 'consent' in PDPA which is currently silent upon its meaning. This allowed organisations utilising FRT to manipulate the process of getting consent from data subjects illegally by confusing or tricking them. Having a clear meaning would provide a proper guideline for them upon how they should get the consent of their data subject when using FRT. The meaning of consent should be something that is frankly given, specific, informed and precise indication of the data subject's wishes by a statement or clear affirmative action that shows their agreement to the processing of personal data related to them. This gives clear guidelines as to how data subjects consent must be collected before using FRT on them. These additions and improvements of meanings are among the things that are listed in the proposed amendment of PDPA.

Improving the Current Safety Procedures and Methods

Moreover, PDPA must improve its safety procedures enumerated inside the act. Among things that must be changed is the word 'practical' in section 9 when requiring data users upon their protection of personal data. Greenleaf (2010) suggested that this word should be replaced with 'reasonable'. This will put a higher standard of safety that needs to be fulfilled by data users when handling personal data. Moreover, there is a need to re-examine the exemption clause in section 45 where complete exemption is given when the data are used for prevention or detection of crime, for investigation purposes and apprehension or prosecution of offenders. This provision needs to be included with some reasonable requirements and standards to ensure the safety of personal data even if it is done for the interest of the public like security reasons. Serious consideration on basic human rights as enumerated in Malaysia's Federal Constitution must be required to be fulfilled by PDPA before allowing a complete exemption in the section without possible liabilities by only exempting data processing under PDPA when it is done for a legitimate purpose, following any law and it is necessary for the society.

Additionally, it is suggested that PDPA implements data protection by design as used by the GDPR. This will provide an extra layer of security even before the data is processed by ensuring the methods, technology and system intended for that purpose can ensure enough protection to personal data. This requirement must make it compulsory for the data users to put appropriate technical and organisational measures effectively and combine any necessary safeguard into the processing of the data especially the pseudonymisation technique used in GDPR. Adopting pseudonymisation methods with encryption of data when processing personal data in PDPA would create a strong safety design for data processing under FRT. This will make the data to be unlikable and harder to use which allows data users and any affected parties to take necessary measures should a data breach happen. This concept of privacy by design are among the things that the government intended to add in their proposed amendment of PDPA.

Expanding the Liability and Jurisdiction

The PDPA also needs to widen the scope of liability and jurisdiction of this act that seems weak and too narrow. Amendment may be made to section 3 of this act by including the state and federal government under its jurisdiction while also extending its applicability outside Malaysia. To establish a stronger and effective law, the PDPA may consider increasing the punishment available. This is due to concerns of possible violation by big organisations that are willing to face the risk of a fine for greater profit. Although the maximum fine of RM500,000 or 3 years maximum imprisonment seems to be a huge punishment available in PDPA, some bigger organizations may afford the fine. The PDPA should increase the amount of fines and imprisonment period available under PDPA so that it can be more effective as deterrence tools for data privacy violations especially against bigger organisations using FRT that operate outside Malaysia. The fine may be based on a certain percentage of their annual global income, for example, 2%, or any greater amount of fine that can be imposed under this act. Although this recommendation may cause objection from some industries, increasing the fine would motivate more organisations utilising FRT to obey this act. In addition, PDPA must also provide a proper medium for a civil remedy to be claimed by private individuals in this act. A specific requirement upon parties that may initiate a private suit for their data privacy must be established to avoid opening the floodgate of civil suits in court. This would ensure more power upon the public over their data privacy rights.

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 480 - 487), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1086

Enforcing Personal Data Impact Assessment

Malaysia also needs to provide a compulsory data protection impact assessment as done by the GDPR. This assessment is also planned to be added into the PDPA in future amendments where it allows a more thorough inspection of FRT's capabilities in protecting personal data in its system by systematically and comprehensively analysing its data processing system to identify and minimise any data protection risk that may occur in future. This assessment must be made compulsory when any processing of personal data involves high risk, especially for FRT. It must be required when the processing involves personal aspects relating to natural persons or when it is related to any automated processing machines that are capable of producing a legal effect or when involving large-scale processing of the special type of data like personal data, biometric data, criminal or security record to decide the data provided.

Creating Comprehensive Data Breach Procedures

The PDPA needs to have comprehensive procedures in the event of a data breach. It needs to provide a clear and thorough guideline when a data breach happens toward any entities handling the data. PDPA must make it compulsory for data users or controllers to notify the data subjects or any affected parties regarding the breach at least within 72 hours when it poses a high risk toward an individual's rights and freedom. The breach notification must also be sent to the Data Protection Department so that further action can be taken by them. This method would give time to data subjects to further solidify their data safety and make any necessary action to mitigate the breach on their own. Although this may alert the perpetrator to the breach, a serious consideration still needs to be made in adding this method as it would greatly raise the standard of security and enhance personal data protection rights. Proper guidelines to manage data breaches like shutting down the compromised system causing the breach or shutting it down must be provided by PDPA in a separate order. A comprehensive data breach procedure will ensure minimization of damage can be done by the FRT system in the event of a data breach.

Specific Regulation on FRT

Aside from strengthening the PDPA, the government may also consider enacting a specific regulation on FRT as done by the US. This regulation is necessary given the complex nature of FRT which is capable of collecting massive amounts of personal data which as facial images and comparing them with another data set. These features must be closely and properly regulated by the government by controlling how this technology is used in public and private sectors. The regulation preferably includes clear guidelines on its allowed purpose of usage, method of usage, security measures and other necessary rules to ensure ethical usage of FRT in Malaysia. The absence of such regulation would invite violation of data privacy by organisations seeking to take advantage.

Conclusion

It can be concluded that data privacy under FRT in Malaysia is yet to be fully acknowledged by the judiciary. This can be seen from lack of suitable and comprehensive provisions inside the PDPA to ensure personal data safety. Special attention must be observed on the PDPA, the sole statute on personal data privacy in Malaysia which is lacking in many areas compared to the more universal and comprehensive GDPR by the EU. Comparison between these two laws on data privacy and protection had revealed many shortcomings of PDPA when ensuring data privacy rights in FRT. Any organisation utilising FRT must be made to adopt stronger safety procedures to avoid being attacked by hackers. Strengthening these areas would ensure FRT can be properly used in Malaysia without risking the public's data privacy. The government may also choose a direct approach by enacting a specific law on FRT given its increasing usage in Malaysia and also due to its dangerous capability of collecting data. Further improvement must be made toward this issue upon both the policy and the law on data privacy to enable FRT to be safely used in Malaysia.

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 480 - 487), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1086

References

Andrejevic, M. & Selwyn, N. (2020). Facial Recognition Technology in Schools: Critical Questions and Concerns. *Learning, Media & Technology*, *2*, 115-128.

Balasingam, U., & Qamar Siddique Bhatti, S.Q, (2017). Between Lex Lata and Lex Ferenda: An Evaluation of the Extent of the Right to Privacy in Malaysia. *Malayan Law Journal*.

Boehm, P. D. (2015). *A Comparison Between US and EU Data Protection Legislation for Law Enforcement Purposes*. Brussels: Policy Department C - Citizens' Rights and Constitutional Affairs European Parliament

Brey, P. (2004). *Ethical Aspects of Facial Recognition Systems in Public Places*. Troubador Publishing Ltd.

Buang, S. (2019). *Urgent need for a Privacy Act*. New Straits Times (1 March 2019)

Greenleaf, G. (2020). *Limitations of Malaysia's Data Protection Bill*. Privacy Laws & Business International Newsletter, at pg 5-7.

Morris, S. (2019). The Guardian (22 May 2019).

Munir, A. B., & Mohd Yasin, S.H. (2012). Personal Data Protection Act: Doing well by Doing Good. *Malaysian Law Journal*.

Nissenbaum, H. (1998). Protecting Privacy in An Information Age: The Problem of Privacy in public. *Law and Philosophy*, 559–596.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press.

Nurul Azma Abdullaha, Md. Jamri Saidi, Nurul Hidayah Ab Rahmanb, Chuah, C. W., & Isredza Rahmi A. Hamidd (2017). Face Recognition for Criminal Identification: An Implementation of Principal Component Analysis for Face Recognition. *AIP Conference Proceedings, 1891*, 020002. https://doi.org/10.1063/1.5005335

Pascu, L. (2020). *Malaysia Commissioner Wants Facial Biometrics Security in Personal Data Protection Act*. Biometric Update (16 March 2020) <https://www.biometricupdate.com/202003/malaysia-commissioner-wants-facial-biometrics-security-in-personal-data-protection-act> accessed 5 May 2020.

Setterfield, B. & Warren. (2018). *Online Data Privacy from Attitudes to Action: An Evidence Review*, Carnegie United Kingdom Trust.

Sivarasa Rasiah v Badan Peguam Malaysia & Anor (2010) 2 MLJ 333

Zeng, Y., Sun, Y., Lu, E., & Tian, R. (2019). Responsible Facial Recognition and Beyond. https://arxiv.org/ftp/arxiv/papers/1909/1909.12935.pd

Zorkadis, V & Donos, P. (2004). On Biometrics-Based Authentication and Identification from A Privacy-Protection Perspective: Deriving Privacy-Enhancing Requirements. *Information Management & Computer Security*, *12*(1).