Journal of Computer Engineering & Information Technology

Brief Report

A SCITECHNOL JOURNAL

Privacy and Security: Ethical Impact Assessment on Deploying Automated Facial Recognition Technology (AFRT) in Government Sectors

Vic Selvaraj*

Abstract

This research report details the findings from an analysis, evaluation, deployment of an Automated Facial Recognition Technology (AFRT) government utilize this system to magnify user authentication, authorization, and exclusive identification for access to various state-level services for instance to enhance an application for, and renewal of, state vehicle, boat, and firearms licences. The government put AFRA as a trial model to conduct an assessment to understand the preliminary's factors of project deployment, CAPEX/OPEX cost, performance, and benefits to the state departments. During the project trial, the State Police department have manifested their interest in AFRA and that they would like to see a roll-out of AFRA into the streets of all major cities in the state to enhance their monitoring, security capability, and quickly identify criminals and other "persons of interest". The role of AFRT will be part of the state police organizational routine operational activities. The national and economic day-to-day operations of countries across the globe now rely entirely on cyberspace as virtually all business processes, state government projects are vastly utilizing cloud resources for storage, access, and management operations. Because of any potential identity theft either any organization facing a major security breach of their data which emanate the disclosure of sensitive assets could have profound consequences which affect the organization's core values and causing financial impoverishment, disruption of services, legal and regulatory compliance issues, affects public reputation and workforce reduction. In this report, we consider the project potentials, all the possible risks, benefits, and ethical implications of the proposed deployment of the AFRA system in the state government services and vastly covered attack formulation phases, biometric use cases on the public and private sector, privacy policy, frameworks, data protection laws, and violations, and privacy impact assessment.

Keywords

Automated facial recognition technology (AFRT), Biometrics, Ethical, Government, Cloud computing, Privacy, Security, Law, Regulatory, Human rights

Introduction

Facial recognition technology recognizes and detects human face through a series of algorithmic concepts, tools, built-in hardware equipment, and with available contemporary technology. An automated facial recognition system uses biometrics indices on a human face to map facial patterns from a captured photograph, recorded videos, or through live video cameras. Once the input pattern is chosen, It juxtaposes the information with a structured database of previously known faces to find an exact match from the given input patterns, and result them in the output [1]. We associate the AFRT tool with the algorithmic approach process it comprises a series of templates of a face, then looks for exact match or similarities between the templates. In the statistical outcomes, AFRT shows the exact match, false positive, false negative, rate of error, and no match parameters [2].

The impetus of the AFRT varies from place to place, but in this report, we define it as to validate individual identity for the purpose of identification and authentication for the individuals who wish to apply for a relevant permit or renewal of a licence in the state service departments. An AFRT appraise the confidentiality, Integrity, Availability (CIA) triad principles and standards to ensure the trust, and security. The major role of AFRT would be used in the state police organizational routines operational activities. In the past 4 decades, facial recognition technology gone through different stages from the low-quality photography analysis to skin analysis, 3D capturing, sensors, thermal cameras, and high-definition photography. In the aftermath of the September 11, 2001 attack, countries around the world perturbed and fretful about their national security aptness. Since then, the use of facial recognition or automated facial recognition technology usage in service has grown rapidly, universities, commercial organizations, various research laboratories rolled out their advancement in AFRT deployment among numerous services. In this report, we will cast light on how the state government put AFRA in the trial to conduct an assessment on licence application, renewal, and handling stratagem in the state service, and how the state government and state police department have shown their interest to see a roll-out of AFRT into the streets of all major cities in the state to enhance their monitoring and security posture, and quickly identify criminals and other "persons of interest". Nevertheless, Non-profit organizations, fellow citizens expressed their concerns about the government's surveillance intentions, and deployment approaches. The perturbation about the context of discontentment, intentions, privacy infringement, utmost citizens were anticipated by the government to trade their individual privacy for higher security in the society [3].

Identity management and the role of biometrics

In the last decade, identity management played a remarkable role, and it is contemplated more important than ever before in information security, and biometrics. An identity management system comprised with a set of algorithms, frameworks, access policies, and discrete hardware for ensuring that the right people can have the appropriate access to the network resources. Because of the expeditious development of Internet, social media, web, online profile carry mammoth information than ever before and challenging the precision of the users. That being said, the role of biometrics, and data management capabilities have enhanced effectively as far as from partial to perfect touchstone. The characteristic of the

***Corresponding author:** Vic Selvaraj, Department of Computing & Mathematics, Charles Sturt University, NSW, Australia, E-mail: vigvic7@yandex.com

Received: July 31, 2021 **Accepted:** August 20, 2021 **Published:** August 27, 2021

biometric technology is defined by the substantial measurement of human beings. It includes the ability to conduct, measure several characteristics such as reading human fingerprints, recognizing the voice, iris scanning, thermal scanning, keystrokes, and facial recognition. The quintessential purpose is the identification, authentication, and management. In the contemporary Internet era, both private and public sector organizations utterly anticipated on information systems management. This reliance, which led to system vulnerability to information security threats that put data and people at risk [4].

According to the IBM Future of identity study report revealed, in the past six years, $112 billion dollars has been stolen through identity fraud, Figure 1 because of the public and private sector reliance on the internet for services, that's equating to $35,600 dollars lost every minute [5]. We defined a dissimilarity of biometric use cases between the terms I.e. "recognition", and "identification", "verification or authentication [6].

In Figure 2 The first row and second row indicated the open-set and close-set identification patterns, and the third row shows the successful verification results for the given input in the biometric system.

The identification trinity

The identification trinity is also known as three-factor authentication [7,8]. A list of approaches for the human-based authentication method is illustrated in Figures 3 and 4.

Purpose of the study

In recent publications, scholarly research were conducted on biometric, identity management, facial detection techniques, privacy concern, and facial detection techniques. Besides, many ontological models represented the traditional and modern vectors of facial recognition technology, biometrics type, and identity management. Albeit, it failed to depict attack formulation phases, biometric use cases on the public and private sector, privacy policy, frameworks, data protection laws, and violations, and privacy impact assessment. In this report, we formulated an endless set of scenarios, research analysis, ethical privacy evaluation, and privacy impact assessment of the state government's AFRT trial for various state services, and how state polices interest in rolling out AFRT on the streets, and how AFRT will play a prodigious role in these use cases.

- Section 1 Introduction about identification and biometrics management.
- Section 2 AFRT deployment, and use case evaluation.
- Section 3 Illustrate information about global authentication methods, biometric authentication, biometric adoption, technological threats, and security and privacy risk reports. Proposes the ethical and privacy impact assessment and framework model.
- Section 4 Illustrate information about global surveillance usage statistics.
- Section 5 Concludes the research report.

The distinction of the biometric system		
Identification	**Verification or Authentication**	**Recognition**
Identification is a process where the biometric system attempts to determine the identity of an Individual or the given input patterns.	Verification or authentication is a process where the biometric system attempts to verify an individual's asserted identity and provide access to the requested services where the individual should access.	Recognition is a generic term and does not necessarily imply either verification or identification in the process.

Figure 1: Distinction of biometric system.

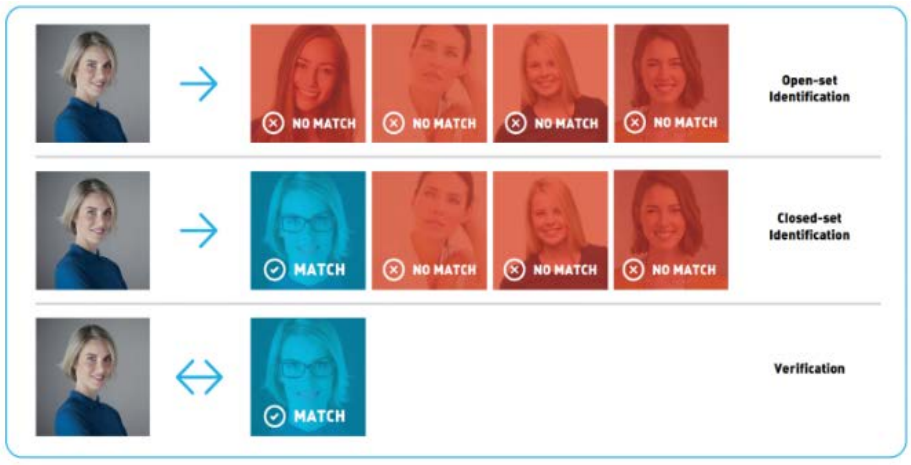

Figure 2: Identification Vs Verfication process in biometrics (Joe Gervais).

The Identification Trinity		
Something you are	**Something you know**	**Something you have**
Biometrics are part of the human body such as fingerprint or iris pattern, the biometric scanner can scan and recognize that. These parts are unique by birth, and harder to compromise. It helps you to distinguish from other patterns among the general population database.	This includes your personal passwords, various pass-phrases, personal identification number (PIN), and answers to security questions for authentication purpose only. These pieces of information are known only by you, and the computer system.	This includes your security tokens, keys, social security number (SSN) cards, driver license, travel passport, certificate, Work badges, etc.,

Figure 3: The identification trinity factors.

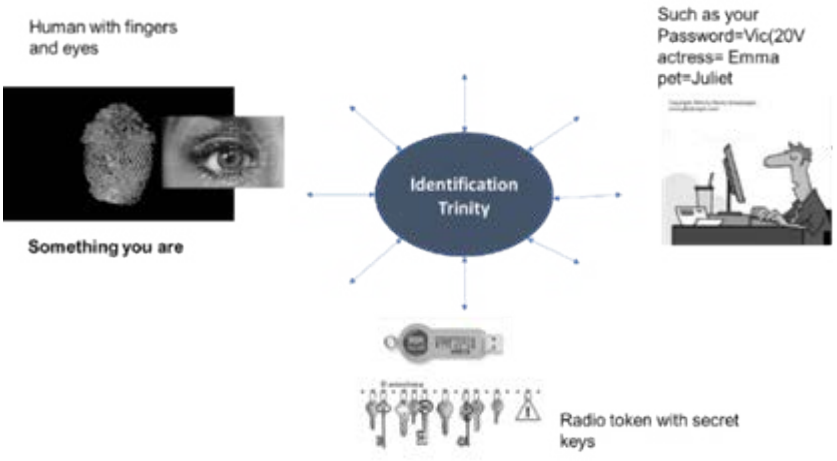

Figure 4: The Identification Trinity.

AFRT Use Case Evaluatıon and Deployment Phases

The impetus of the AFRT varies from place to place, but in this report, we define it as to validate individual identity for the purpose of identification and authentication for the individuals who wish to apply for a relevant permit or renewal of a licence in the state service departments. During the project trial, the state police department have manifested their interest in AFRA and that they would like to see a roll-out of AFRA into the streets of all major cities in the state to enhance their monitoring, security capability, and quickly identify criminals and other "persons of interest". The role of AFRT will be part of the state police organizational routine operational activities. In this report, we do not directly altercate the federal protection issues regarding the legality, or use, of AFRT technology by different law enforcement agencies. This report cornerstone the overall governance of the AFRT trial, practices, procedures, deployments of AFRT in state services, issues emerge out in relation to the state police AFRT considerations, ethical assessments, and human rights compliance. AFRT is gaining popularity among state police departments in various countries, could be used as a tool to identify persons of interest in criminal investigations. However, AFRT elevates a unique representation about biometric traits that are both demanding, and exposed to the public with privacy discontentment, which measures that unregulated use of AFRT in state police department against a vulnerable human beings [9].

Analytical approach

The goal of this case evaluation is to relinquish the pool for resource discourse, and policymaking around AFRT deployment in state government service sectors by providing a systematic approach, policy decision-making, analysis framework to assess to which proportion of regulatory policies safeguard the human rights, privacy, bias-discrimination, against in a democratic society or a particular region. In Section 4, we put forward the ethical and privacy impact assessment, framework model to assess, and understand how the AFRT trail consideration for state police department would affect, safeguard privacy, human rights, and benefit the society and the state government.

Research methods: In this research report, we follow a qualitative trinity approach to appraise the deployment trial, and deployment approach of the AFRT through the ethical analysis framework, data privacy, technical difficulties, cost, U.S. congress bill, E.U parliamentary protocols, Freedom of Information Act (FOIA)-U.S.C 552, S.3284, S.847, U.S-BIPA- 740 ILCS 14/1, London Metropolitan Police-LRT trial, south wales Police'-AFR trial, EU-GDPR, EU-FRA, and other substantial Internet archives clutched into the case studies.

Research case studies: We will make use of the list of case studies in our research, as shown in Figure 5. It weighs the qualitative trinity approach to case studies. As we stated before, the applied

Figure 5: AFRT deployment and usage statistics in the US (IBM Security).

research methods, and policy analysis are depicted in subsection. We contemplated a greater number of similarity factors among highly developed countries, structured democracies, and technologically advanced countries such as the U.S.A., the U.K. That being said, both countries comparatively impose different analytical, innovation, and market strategies. Correspondingly, we view the US as the technology leader, innovator, always pursue a fact-paced strategy. In contra, countries in European Union pursue a cautious, value-driven based strategy, rigid political systems, and lack of innovation hubs.

Although, the US is relatively five times more populous, and seven times economically stronger than the UK, and AFRT has been deployed extensively by various states in the US as shown in Figure 5. For this rationale, relatively extensive section of the policy reference, and analysis applies to map the AFRT use cases, regulatory policies, ethical and privacy impact assessment across the US [10].

AFRT system deployments and its benefits

In this section, we will discuss the facial recognition technology ethical usage, implications, working mechanisms, benefits and risk to the citizens and service employees.

AFRT System facilities to apply or renew a license in state service sectors: In recent decades, malicious attacks, online fraud, social engineering attacks, hacking activities are vastly spewed in cyberspace. If the traditional portal system approach gets compromised, state government service sectors could be at risk and pose an immense threat to the overall security system. To minimize the cyber threat, the state government rolled out and adopted the advanced authentication methods in state service sectors to improve the defense mechanisms and operational efficiency [11]. It can help to identify, evaluate, authenticate individual employees, and could enormously reduce malicious actions, and ease the overall online application experience, hurdles, cost, and manpower. The license applications are issued and managed by public key infrastructure (PKI). All digital identities are cryptographically encrypted and protected [12]. When state employees access the AFRT portal to apply or renew for the state vehicle licenses, boat, and firearms licenses. It will be identified and authenticated instantaneously by the system Figure 6.

We can break the principal functions of AFRT working mechanism and algorithms operations into a simplified workflow as shown in Figure 7.

State police proposed use of AFRT on streets: The chief of the police department believes AFRT will improve the monitoring functions, violence prevention, detection of crime, and public security.

In May 2017, south wales police (SWP) rolled out the new facial recognition technology (FRT), during the Champions League final week in two different cities. The SWP team proposed four colour-coded watchlist patterns for the event, as shown in Figure 8. The SWP did not share how the FRT would rationale the individuals. It contains images of the wanted person, possible suspects, person of interest, and missing persons [13]. Other usage of AFRT by the state police department for the purpose of law enforcement activities are not distinguished to the public.

The London metropolitan police service (MPS) used live facial recognition (LFR), conducted a total of 10 test deployments between the year of 2016 and 2019. South wales police used facial recognition technology (FRT) software, and the functionality is little different from London police event operations. However, both police forces follow a similar pattern in the deployment techniques [14]. Before it get weaving, London police created this template for the LFR deployment as shown in Figure 9.

Benefits and risks of using AFR/LFR technology: The AFR technology plays a major role in state service sectors, and the state police department in developed, developing and indistinctly together with communist countries [15]. The benefits and policing outcomes from the intended use and deployment of the AFRT in state service sectors for the licence application, and renewal operations as shown in Table 1.

AFR technology poses an ethical risk to service employees: The ethical risk and outcomes from the intended use and deployment of the AFRT in state service sectors for the licence application, and renewal operations as shown in Table 2.

Benefits and risks of using AFR/LFR technology in the streets: The benefits and policing outcomes from the intended use, and roll-

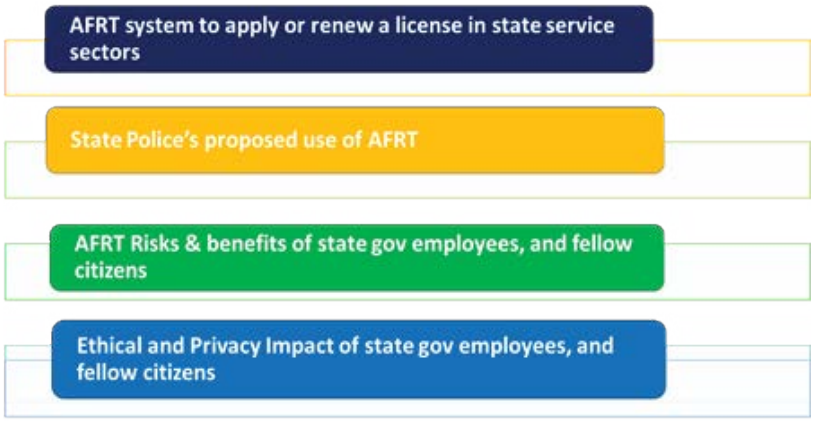

Figure 6: List of use cases and their scenarios.

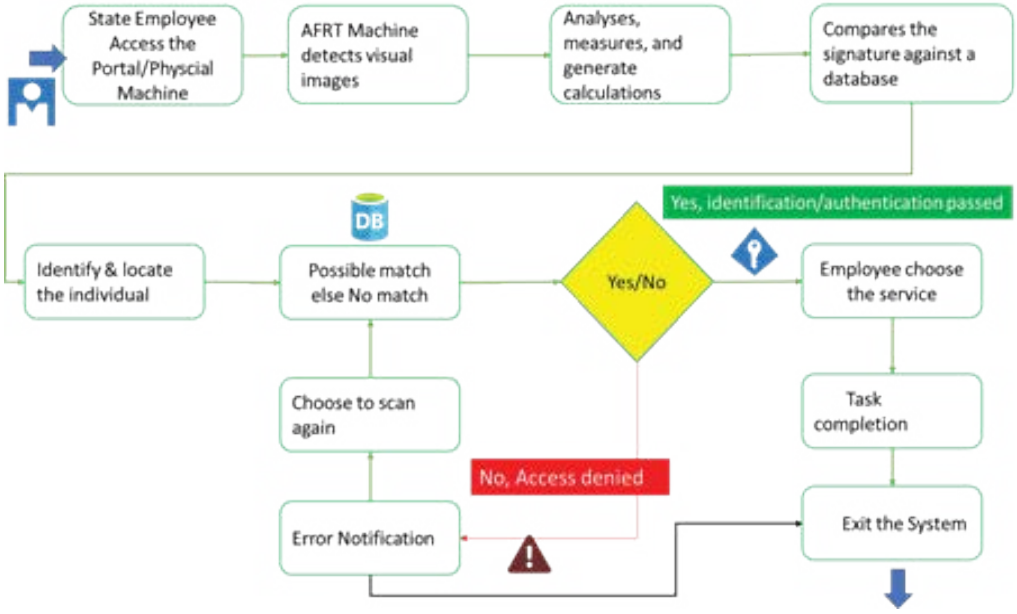

Figure 7: AFRT working mechanism and algorithmic operations.

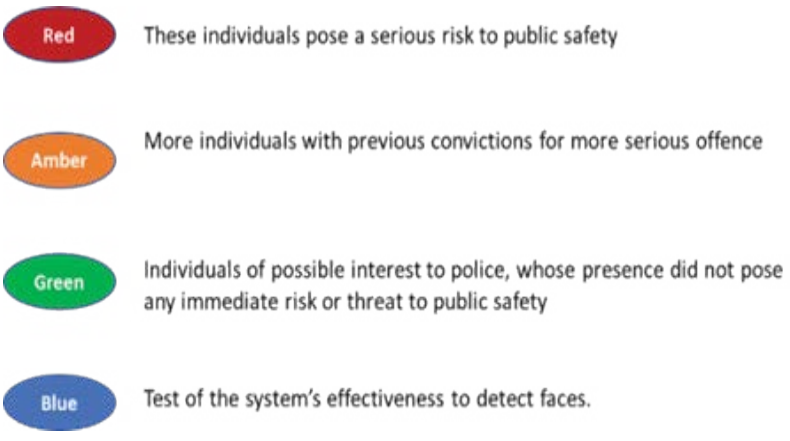

Figure 8: Color coded watchlist patterns used by SWP.

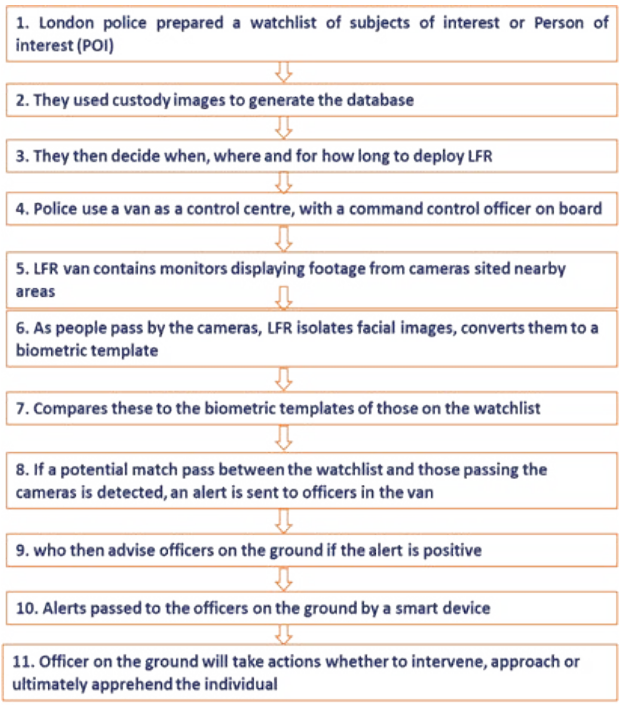

Figure 9: London Metropolitan police watchlist template.

Table 1: Benefits of using AFR technology in state service sectors.

Benefits of using AFR technology in state service sectors
Centralized access to the state services
Easy to navigate
Reduction in time on applications
Time management
Paper fewer actions
Automated verification and authentication
Speed in identify check
Reduction in approval time
Automated query response
Mitigate the risk for fraud, including identity theft
Improved in security
Cost-efficient
Administrative less operation
Reduction in Manpower and office space

Table 2: Risk of using AFR technology in state service sectors.

An Ethical risk to the state service employees
Risks to individual privacy
Auto rejection/deny upon errors
Inaccuracy in verification and authentication
Bias and discrimination
High false positives and false negative rate
Lack of Privacy impact assessment reports
Lack of more comprehensive regulation
Vulnerable to the threat
Digital identity stored in multiple locations
AFR technology primary control access granting varies by jurisdiction
Federal agencies gain access to the state service employee's data
Mandatory enrollment, there is no right to refuse enrollment
Lack of transparency
Risks to individual privacy

out the deployment of the AFRT on the streets in all states as shown in Table 3.

AFR technology poses an ethical risk to the citizens: The degree of risk that AFR technology poses to society will depend on the types of software systems, techniques, regions, operational control being used, and the manner of its deployment. Table 4 Ethical risk to the citizens.

Manpower and training requirements

The importunate for skilled workforce and training requirements are all clamouring for attention in the organization to improve an operational control of identity management systems, and biometric applications. It requires adequate training for the state police departments to address multiple things such as deployed applications, tools, privacy act, congress bills, human rights abuse, operational control, data handling, and maintenance. Above-mentioned causes form an insufficiency in the organization, even made starker in a state coalition-action environment.

Ethical and Privacy Impact Assessment (PIA)

In this section, we aim to abridge the governance issues in the ethical's practice impact assessment to contemplate decision-makers with some cogitation of the AFRT technology in usage or deployment

Role of ethics

The deployment of AFRT utterly creates a pivotal ethical, and privacy-related issue in many developed countries around the world. The emergence of new ubiquitous surveillance technology risk individuals to lose control of their personal data, lack of awareness in many circumstances.

Data protection principles

The GDPR's new principles are comparable to the principles defined in the Data Protection Act of1998. A magnificent data protection can be crafted by following these key principles as a compliance standard Table 5 [16-18].

Legitimacy of an interference with human rights

We can measure the legitimacy of an interference with these three terms. An encroaching of the right to privacy, the right to freedom of expression, or the right to freedom of association, and is obligatory in a democratic society in order to meet the core elements [19].

Data protection bill in the US

In the US, state jurisdictions vary greatly with the law enforcement, and their use of FRT. Some jurisdictions rolled out the FRT, set an example, such as Seattle city. Other jurisdictions raise concerns, oppose the use of FRT due to their inadequacy of privacy rights, and technology's risks, and required an effective communication with public before deployment. The list of recent US congress Bill on FRT as shown in Table 6 [20-25].

Metropolitan state service laws in the UK

The London police, the LFR trail report does not state distinctly about the legislation which allows police use of LFR technology, and MPS referred to several sources of law in relation to the authorization and use of the technology in the act as shown in Table 7 [26,27] .

The written report published by MPS furthermore refer to the section 33 (subsections 1-4) of protecting freedom act 2012. However, it only refers to the use of CCTV technology only. It does not provide authorization, MPS adjured the legislation to create the aforementioned legal action for the use of LFR in service There is no one specific law defining the conditions under which types of FRT can be used, and it is still governed by several UK laws and regulators across the country [28].

Why carry out a PIA

There are various reasons why organisations, both governmental and business, carry out a PIA. In some cases, as in Canada, the US and perhaps the UK, they are mandatory for government departments and agencies. In other cases, organisations carry out a PIA because they want to avoid or manage risks and gain certain benefits.

Privacy and data protection impact assessment

In 1953, European council passed a right to privacy law, and we identify the utilitarian elements in the right to privacy law as defined in Article.8 of the European Convention on Human Rights (ECHR) act [29]. It's a basic criterion to conduct a privacy impact assessment Table 8.

Data protection impact assessments: From 1995 to 2000, the European Parliament council created several regulations, frameworks based on data protection rights in the European Union. The content of the data regulations are very detailed in nature, and in this report, we are focused on the key assessment items in the checklist from a technical point of view as shown in Tables 9 and 10 [30-35].

Table 3: Benefits of using AFR technology in the streets.

Benefits of using AFR technology in the streets	
Reduction in investigation and prosecution times	Mobile phone app- Alert & controls
Increase in community cohesion	Body-worn video;
Location tracking and identification	Automated Number Plate Recognition
Identification of vulnerable or at-risk individuals	Improved in security
Effective monitoring in Private and public events	Cost-efficient
Reduction in patrols	Automated verification and authentication
Easy to blacklist the suspect	Time management
Counter-terrorism	Centralized data management and control
Reduction in repeated offenses	Improvement in potential detections
Biometric trait & templates	Automated identify checkup
Automated pattern recognition and sorting data subjects	Portability

Table 4: Ethical risk to the citizens.

Ethical risk to the citizenS		
Breach of privacy	System Inaccuracy	Bias & discrimination
Massive data storage	Data handling & Management	Power abuse
Vulnerability in recognition	Criminal abuse	Lack of transparency
Law enforcement & safety	Hacking	Lack of Privacy act
Lack of privacy act	Human rights abuse	Decision making process
Private companies missuse customer data	Anonymity is vanishing	False positives trigger, puts individuals to the watchlist

Table 5: GDPR-7 Data protection principles.

S.NO	GDPR- 7 Data protection Principles
1	Lawfulness, fairness, and transparency
2	Purpose limitation
3	Data minimization
4	Accuracy
5	Storage limitation
6	Integrity and confidentiality (security)
7	Accountability

Table 6: Data Protection Bill in the US.

116th CONGRESS IN THE SENATE OF THE UNITED STATES	
A BILL	
S.847-Commercial Facial Recognition Privacy Act of 2019	To create, control, and prohibit any entities applying or using any facial recognition technology to identify or track any end-user without taking end-user permission.
S.3284 - Ethical Use of Facial Recognition Act, February 12, 2020	We pause the ethical use of facial recognition technology on the government for a certain period until standard guidelines and limitations issued by the commission on ethical use.
S.2878-Facial Recognition Technology Warrant Act of 2019	To create and curb the use of facial recognition technology warrants issued and used by the Federal agencies.
S.4084 - Facial Recognition and Biometric Technology Moratorium Act	To prohibit and curb biometric surveillance used, obtained, engaged by the Federal agencies or any Government without clear law authorization to withhold any safety grants from the local and state governments.
S.3456 - Consumer Data Privacy and Security Act of 2020	To protect the privacy of consumers.
S. Rept. 107-240 - ONLINE PERSONAL PRIVACY ACT	To protect the online privacy of individuals who use the Internet.
ACT	

Table 7: UK Metropolitan state service Laws in practice as of -5-Apr-2019.

UK Metropolitan state service Laws in practice as of (5-Apr-2019)	
List of Laws	Authorization role
Common law	Article 8(2) Provides implicit authorization, but requires to be examined
Human Rights Act of 1998	Does not specify the controls
Freedom of Information Act 2000	Regulate the use of LFR without explicit legal authorization, but requires to be examined
Protection of Freedom Act 2012	Provides implicit authorization
Data Protection Act of 2018	Refer, Article 9(2) GDPR, For detailed consent at Article 4(11), also refer s35(8)(b) DPA 2018
Regulations of Investigatory powers act	To intercept communications, and acquisition of communications data
Criminal Justice and Public Order Act 1994	Police has the power to require removal of facial coverings in England and Wales

Table 8: European Convention on Human Rights (ECHR)- right to the privacy.

European Convention on Human Rights (ECHR)- right to the privacy.	
Table 8. European Convention on Human Rights (ECHR)- right to the privacy.	Everyone has the right to respect for his or her home, private, family life, and personal communications.
Table 8. European Convention on Human Rights (ECHR)- right to the privacy.	Everyone has the right to protect and access their personal data with compliance, if it is concerning him or her.

Table 9: European Parliament and Council – Data Protection directive.

European Parliament & Council- Data Protection Directive		
NAME	CODE	Year
Data Protection Directive	95/46/EC	24-Oct-95
e-Privacy Directive	2002/58/EC	12-Jul-02
Data Retention Directive	2006/24/EC	15-Mar-06
Council Framework Decision	2008/977/JHA	27-Nov-08
Regulation	45/2001	18 De 2000

Table 10: European Parliament and Council – Data Protection Directive-Article extensions.

European Parliament and Council Data Protection Directive			
SNO	**NAME**	**DESCRIPTION**	**ARTICLE.NO**
1	**Personal data must be fairly and lawfully processed**	The term Fairness defines one should only handle data in a way it's reasonable, and accepted, and cannot adversely effects on them.	Art. 6(1)(a)
2	**Data Minimisation**	It's collected based on explicitly defined purposes on specific and legitimate terms and should not further be processed in a way incompatible with those purposes. Data kept only for as long as is necessary to fulfill that purpose and the term (implicitly).	Art. 6(1)(b) Art. 6(1)(c)
3	**Data Quality**	The collected data is adequate, relevant, and not excessive in relation to the purposes for which they collected, obtained, and/or further processed where necessary, kept up to date.	Art. 6(1)(c) Art. 6(1)(d)
4	**Legitimate basis**	The unambiguous consent of the data subject contract to which they base the data subject on the party compliance with a legal obligation of the data protection and vital interest of the data subject task carried out in the public interest or exercise of official authority approval or handled by the legitimate interest pursued by the controller.	Art. 7
5	**Data Anonymisation**	Data kept in a form which permits identification of data subjects for no longer than is necessary.	Art. 6(1)(e)
6	**Data Security**	Confidentiality of processing	Art. 16
		Security of processing	Art. 17
		Notification of processing data	Art. 18(1)
		Data breach notification	Art. 4(3)
7	**Data Subject rights**	The right to be informed about processing his/her personal data in a clear and understandable language of the intended user.	Art. 12(a),
		The right to access his/her own personal data.	Art. 12(a)
		The right to rectify any wrong or incomplete information.	Art. 12(b),
		The right, in some cases, to object to the processing on legitimate grounds.	Art. 14
		An automated decision intended to evaluate certain personal aspects relating to the data subject such as his performance at work, creditworthiness, reliability, conduct.	Art. 15
		The right to demand and to receive monetary compensation from the data controller for any damage caused to the person.	Art. 22, Art. 23
8	**Data controller's obligations**	The data subject's rights are observed.	Art. 8(1)
		Data observance performed based on the data minimization principle.	
		It uses the Data observance criteria for making the data-processing.	
		To safeguard the confidentiality and security of data processing.	
		To notify the processing of personal data to the national data protection authority (DPA).	
		When the data is transferred to the third countries in different jurisdictions, ensure that these countries provide an adequate level of protection to the data.	Arts. 25-26

Global AI Authentication and Facial Recognıtıon Technology Usage Statistics

The Carnegie Endowment for International Peace is the world's most comprehensive running think tank archive on AI and Facial recognition technology. Globally, this think tank study, analyze, measure, evaluate and report about the country's current usage, deployment, and future considerations of FRT/AFR. The key trends of the 2019 AI Global Surveillance (AIGS) index show that a growing number of countries, states, and authoritarian regimes are deploying millions of advanced AI-based FRT/AFRT surveillance technology tools to analyze, monitor, track, perform automated and manual surveillance on its own citizens. In AIGS index report covers 176 countries around the world various aspects and usage of the technology, government's ability, control, and monitor individuals [36].

- Smart-City–56 countries
- Facial recognition/Automated facial recognition technology (FRT/AFRT)-64 countries
- Smart Policing- 52 countries
- The category of democracies, and government, as shown in Table 11.

In fully democratic countries, the government using a range of technology such as AI, FRT, AFRT for their smart city project as well surveillance system.

LD-In liberal democratic countries, around 51 percent of government from these countries are an active user of AI.

CA-In closed autocratic states, around 37 percent of more active users of AI.

EA-In electoral autocratic/competitive autocratic states, around 41 percent of more active users of AI.

ED-In electoral democracies/liberal democracies, around 41 percent of more active users of AI.

In autocratic and semi-autocratic countries like China, Russia, Saudi Arabia, government blatantly abuse the use of AI-based surveillance technology for mass surveillance, human rights violations, political suppression compared to other categories of government [37-38]. The perspective of governance may help to understand whether their objective is genuine for future development or in how much percentage it affects, abuse, and violate human rights violations. The key trends of the 2019 AI Global Surveillance (AIGS) index are shown in this section [39].

Table 11: Types of ruling around the world.

Ruling Types	Definition
EA	Electoral Autocracy
ED	Electoral Democracies
LD	Liberal Democracies
CA	Closed Autocratic
SA	Autocratic & Semi-Autocratic
EA	Electoral Autocratic & Competitive Autocratic
D	Dictatorship

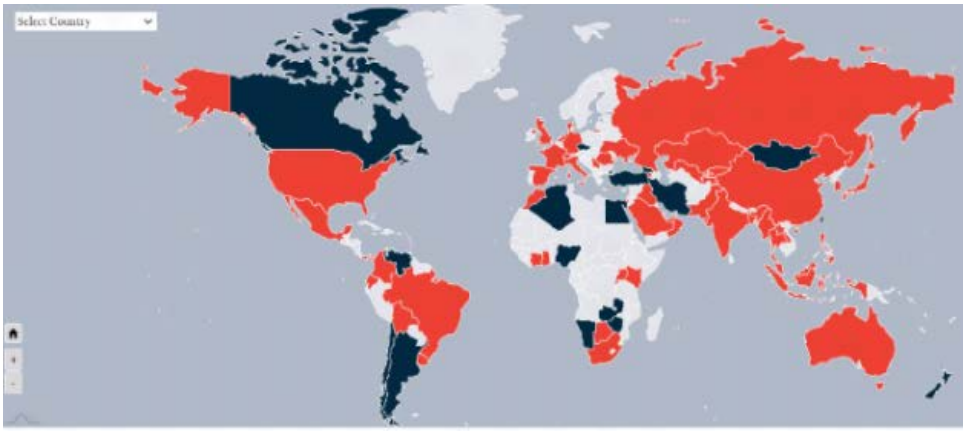

Figure 10: Smart city project statistics (carnegieendowment).

Smart city

Smart-city projects are implemented with real-time data transmission with the help of the sensors, command control centres (CCC) to facilitate service delivery, prevent crimes and improve public safety Figure 10.

Facial recognition systems

In recent years, technology improvement on biometric is rapidly speeding up. Using, biometric system, an individual or group of individuals can be matched with the existing database or aggregated with the demographic trends via FRT crowd scanning features Figure 11.

Smart policing

In smart policing, it develops an application with the help of the AI, FRT, and predictive algorithms to shape up the smart policing concepts on crime control Figure 12.

AI surveillance technology origin

China bases the production and supply chain of global, and it inhabited huge market share on FRT and AFRT technology. The given below map illustrated the global players on facial recognition, and surveillance technology Figure 13.

AI-FRT manufacturer

Globally, besides Chinese manufacturers, there are several other significant players supplying advanced facial recognition and surveillance technology to the private and public sectors around the world. Some noteworthy players such as the United States, Japan, Germany, and France etc., The given below figure break down the leading companies from different countries and the number of market share they propogate Figure 14.

Top 25 most surveilled cities in the world

We inherited and analyzed the Comparitech and the IHS Markit report on global surveillance program. The Comparitech researchers published a report on the most sursurveilled cities around the world, and primary attributes define camera per 1000 people in usage. According to the IHS Markit the latest report on global surveillance, china host 22 out of the top 25 most surveilled cities in the world. Globally, 770 million cameras were in use, china accounting 54% of the total proportion, and the mass surveillance program is estimated to hit higher than the rest of the world by 2025 Figure 15 [40,41].

Conclusion

In this report, as we delineated in the previous sections, the trial, deployment of AFR technology raises a number of complex issues in terms of individual privacy, legitimacy, and security ethics. A key finding of this evaluation from different case studies indicated that how AFR technology is assessed by the state police to identify individuals, group of individuals, or a possible suspects in crime, and the AFRT competence is totally depended upon the functional performance of AFRT technology, interpretations and decisions of command control operators. We identified it's tremendously possible that the AFRT trial process adopted by the state police would be held unlawful if challenged before the courts by the human rights groups.

In this research report we concluded that the implicit legal authorization claimed, used by the police for the purpose of AFRT on the streets, an effective incorporation of human rights elements into all stages of the police AFRT decision-making process should be stated

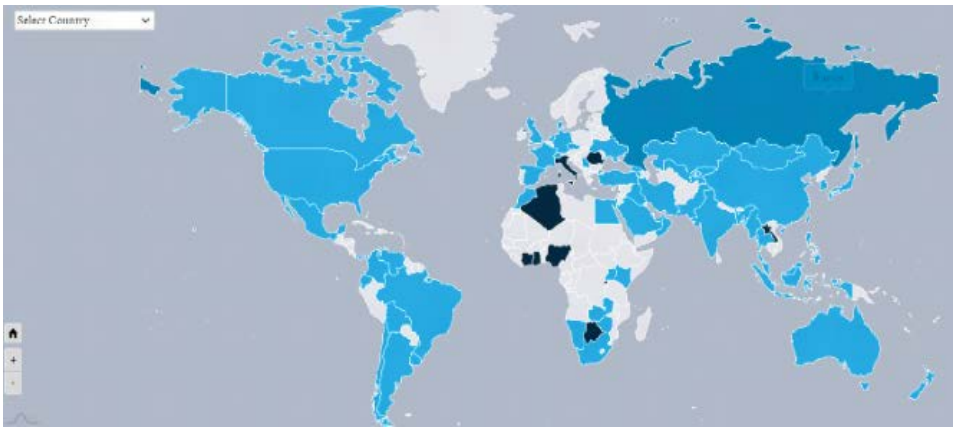

Figure 11: Facial Recognition Systems (Source: carnegieendowment).

Figure 12: Smart policing (Source: carnegieendowment).

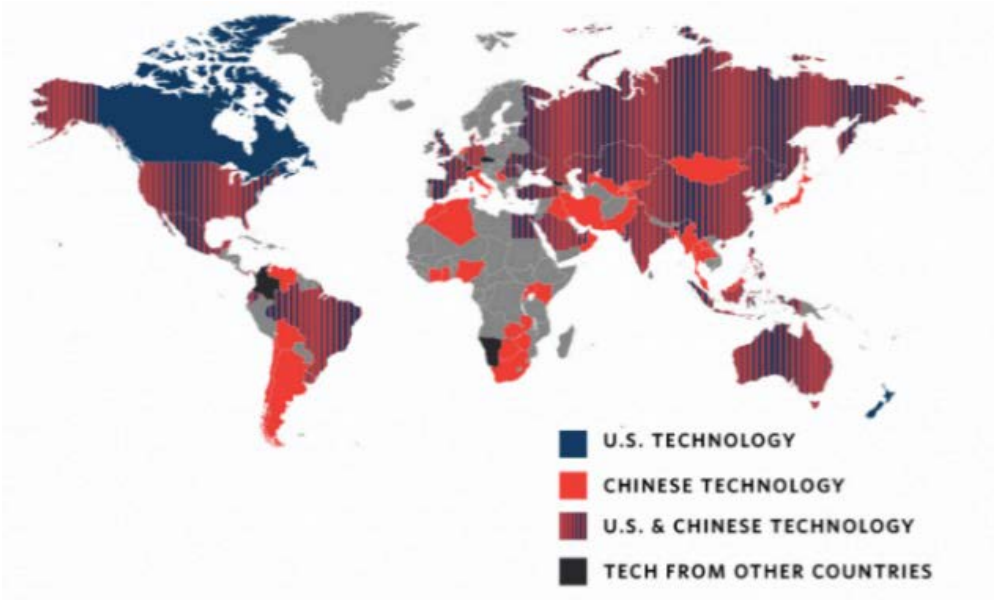

Figure 13: Global supply chain of surveilance technology (Source: carnegieendowment).

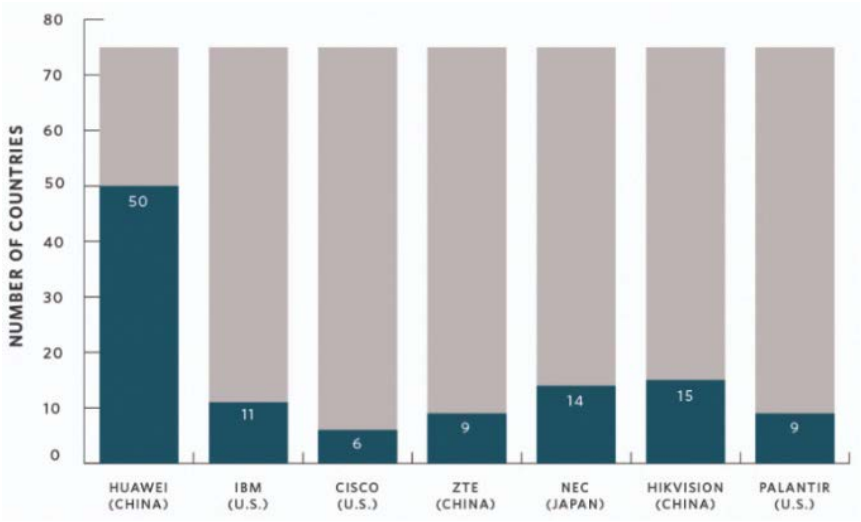

Figure 14: Top 6 global players in manufacturing (Source: carnegieendowment).

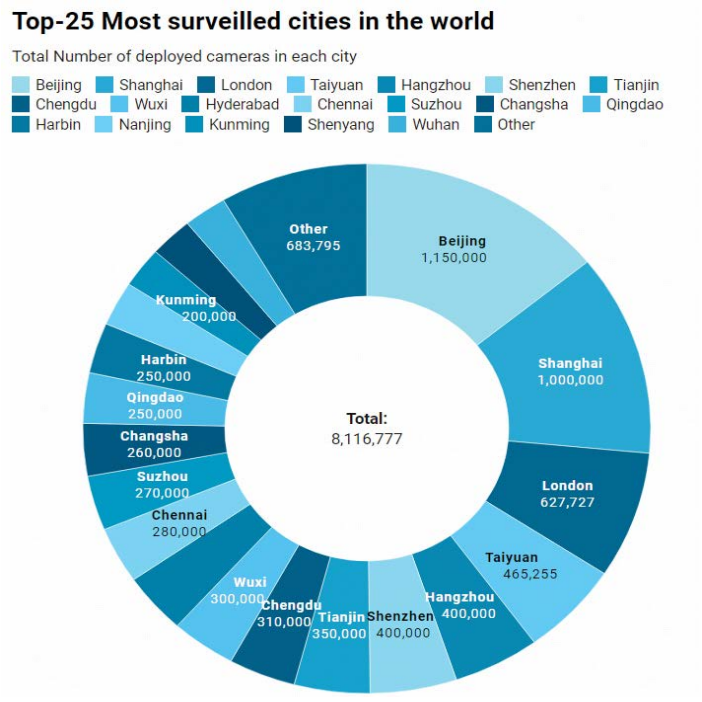

Figure 15: Top 25 Most surveilled cities in the world.

in function need to be reformed with the legislations and lawmakers. The lack of privacy act, data protection standards, AFRT practising, public consultancy, police decision-making process, including with respect to if, and how, trials should be undertaken are inadequate to the public for review, and understanding about the technology in usage. However, this report highlights the moral, ethical implications of the human rights law, and obligate a privacy impact assessment to be conducted to the prior requirement, design, installation, operational policies, and deployment considerations in the cities. The state Police department is longing in using innovative technology like AFRT to keep safe the public order, and new regulatory frameworks will probably be necessary as this technology becomes more widely adopted in all parts of the world.

This work helps the security researcher to gain insights into AFRT/LFR from a different perspective, and precisely it enhances the current and future research on AFRT/LFR, privacy, security, and ethical implications mechanisms prior to the deployment. It highlights the privacy and ethical impacts requirements for private, public sectors, business partners, and customers to analyse and identify gaps in their organization's AFRT implementation practices. In future work, the AFRT/LFR, privacy and security, offensive and defensive implications can serve as the foundation model for a new

policy adoption or a mechanism to improve an existing program in the country.

References

1. Snapshot Series Facial Recognition Technology (2020) POLITICO – European Politics, Policy, Government News.
2. Gervais J (2020) How does facial recognition work. Norton Life Lock Inc.
3. Pavone V, Esposti S D (2020) Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. Public Understanding of Science 21(5): 556-572.
4. Orgill GL, Romney GW, Bailey MG, Orgill PM (2004) The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. Proceedings of the 5th conference on Information technology education - CITC5 '04.
5. Limor Kessem (2018) IBM Security: Future of Identity Study. CISSP Eighth Edition 579-621.
6. Report of the Défense Science Board Task Force On Défense Biometrics (2007) Department of Défense (DOD). 52 (2020) Federation Of American Scientists – Science for a safer, more informed world.
7. Report of the Défense Science Board Task Force On Défense Biometrics (2007) Department of Défense (DOD). 26 (2020) Federation of American Scientists – Science for a safer, more informed world.
8. Goodrich M, Tamassia R (2014) Introduction to computer security Pearson Higher Ed.
9. Ruhrmann H (2019) Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement. Technology policy research & Engagement in the Interest of Society - Citris Policy Lab 9.
10. Ruhrmann H (2019) FACING THE FUTURE: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement. Technology policy research & engagement in the interest of society - CITRIS Policy Lab p.9.
11. Advanced authentication market in defense industry - Growth, trends, and forecast (2020 - 2025). Mordor Intelligence.
12. Brunelli R, Poggio T (1993) Face recognition Features versus templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 15(10): 1042-1052.
13. Davies B, Innes M, Dawso A (2018) South wales police.
14. Fussey P, Murray D (2019) HRBDT Independent Report on the London Metropolitan Police Service's Trial of live Facial Recognition technology HRBDT.
15. Masupha L, Zuva T, Ngwira S, Esan O (2015) Face recognition techniques their advantages disadvantages and performance evaluation. International Conference on Computing, Communication and Security (ICCCS).
16. The principles (2021) Guide to the General Data Protection Regulation GDPR ICO.
17. Office of the Austrailian Information Commissioner Australian Privacy Principles (2020) OAIC.
18. Privacy Principle . (2020) City of Seattle.
19. UK surveillance regime: some aspects contrary to the Convention (2020). European Convention on Human Rights ("ECHR").
20. S.847 - 116th Congress (2019-2020) Commercial facial recognition Privacy Act of 2019. Congress.gov -Library of Congress.
21. S.3284 - 116th Congress (2019-2020) Ethical use of facial recognition act. Congress.gov - Library of Congress.
22. S.2878 - 116th Congress (2019-2020) Facial recognition technology warrant Act of 2019. Congress.gov- Library of Congress.
23. S.4084 - 116th Congress (2019-2020) Facial recognition and biometric technology moratorium Act of 2020. Congress.gov - Library of Congress.
24. S.3456 - 116th Congress (2019-2020) Consumer data privacy and security Act of 2020. Congress.gov - Library of Congress.
25. S. Rept. 107-240 - Online personal Privacy Act. Congress.gov - Library of Congress.
26. Surveillance camera code of practice (2014) GOV.UK.
27. Live Facial recognistion-MPS-legal manadate (2019) Metro police-UK.
28. Understanding the law on facial recognition software (2019) Personal & Business Legal Services Solicitors - DAS Law.
29. European Convention on Human Rights (ECHR) (1953).
30. EUR-Lex - 31995L0046 - EN - EUR-Lex. EUR-Lex (2020) Access to European Union law.
31. EUR-Lex - 32002L0058 - EN - EUR-Lex. EUR-Lex — Access to European Union law — e-Privacy Directive 2002/58/EC. (2020).
32. EUR-Lex (2020) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC . EUR-Lex - 32006L0024 - EN - Access to European Union law -Data Retention Directive 2006/24/EC.
33. EUR-Lex - 32008F0977 - EN - EUR-Lex. (n.d.). EUR-Lex - Access to European Union law-Council Framework Decision 2008/977/JHA. (2020).
34. EUR-Lex - 32001R0045 - EN - EUR-Lex. (n.d.). EUR-Lex -Access to European Union law- Regulation No 45/2001. (2020).
35. Wright D, Hert P D (2012) Privacy Impact Assessment. Springer Science & Business Media.ISBN 978-94-007-2542-3. e-ISBN 978-94-007-2543-0: 33-37.
36. Feldstein S (2019) The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace Pp: 6-7.
37. Feldstein S (2019) The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace p: 7.
38. Feldstein S (2019) The Global Expansion of AI Surveillance. Carnegie Endowment for International Peace Pp: 1-4.
39. AI global surveillance. (n.d.). Carnegie Endowment for International Peace. (2019).
40. Video surveillance & analytics market share database - 2020 - Omdia. (n.d.). Omdia – Connecting the dots - Omdia.Year: 2020-2021 Informatac (2019).
41. Surveillance camera statistics: Which city has the most CCTV cameras? (2019, August 15). Comparitech (2019).

Author Affiliation

Top

Department of Computing & Mathematics, Charles Sturt University, NSW, Australia