Executive Summary

There has been an increase in the development of digital identity worldwide with both public and private sectors utilising big data analysis and facial recognition to improve the efficiency and convenience of services. Through the support of artificial intelligence and deep learning, the accuracy of facial recognition by robots has surpassed that of humans, as shown in the GaussianFace algorithm developed by the Chinese University of Hong Kong in 2014.

According to a tech economy report, the global market of facial recognition will increase by US$3.3billion in 2024, with a compound annual growth rate of 12% from 2020 to 2024. This shows that facial recognition has great potential to develop in the age of big data.

In recent years, the HKSAR Government has been attempting to catch up with the rest of the world in terms of digital governance, including the introduction of the "LeaveHomeSafe" app and the "Multi-functional Smart Lampposts" Pilot Scheme. Yet, the recently proposed Real-name Registration Programme for SIM Cards and criminalisation of doxxing legislation has raised the public's concerns regarding the legal protection of their personal privacy.

Currently, the protection of local-citizen personal data privacy comes under the Personal Data (Privacy) Ordinance (the "PDPO") (Cap. 486), that is enforced by the Privacy Commissioner for Personal Data (PCPD). Since the PDPO came into force in 1996, it has been criticised for being outdated (e.g. regarding the definition of personal data and duration of retention i.e. there is no "right to be forgotten"). In addition, the PCPD has been criticised for lacking deterrence when it comes to monitoring data processors, especially in the execution of personal data breach notifications. Without criminal investigation and prosecution powers, the public has become concerned about the effectiveness of the PCPD to secure the public's personal privacy.

There has been rapid development of privacy protection worldwide (e.g. the EU's General Data Protection Regulation "GDPR"), with citizens and relevant industry stakeholders placing increasing importance and paying

more attention to the issue. It would therefore be worthwhile for the Hong Kong Government to consider updating the PDPO, especially in legal terms as it relates to such areas as sensitive personal data, data retention, and the accountability system of the data user. The Government could also review how the PCPD can better balance: crime prevention, securing the public's right to know, technological advancement and citizens' personal data privacy.

This research aims to understand the public's concerns between their own privacy protection and using innovative technology for public health, public security, and news reporting purposes. It also aims to review and improve the system that monitors the use of personal data by private and public organisations, so that the interests of the various stakeholders involved can be better balanced in the age of Big Data.

Main Discussions

1. The laws that protect citizens' privacy in Hong Kong are relatively outdated given the rapid development of big data analysis and artificial intelligence.

Artificial Intelligence (AI) has been developing rapidly in recent years, out of which big data analysis and facial recognition are the most prevalent technologies. However, these technologies have had an increasingly significant impact on the privacy of individuals, that have caught the attention of international governments and Human Rights concern groups.

This research collected data through an on-site survey interview of 808 residents (aged 15-65) between 5th and 17th March 2021. Most respondents placed a high value on privacy, rating it at an average of 6.66 (on a scale of 0-10). It indicates, in general, that Hong Kong citizens value their own privacy.

Our on-site survey result showed that the work of the PCPD scored 5.97 (on a scale of 0-10), indicating that Hong Kong citizens are generally satisfied with the work of the PCPD. The main reason for dissatisfaction with the PCPD (42% of respondents) was due to the lack of compliance monitoring and supervision.

As the survey results demonstrate, Hong Kong citizens do value their own privacy, but consider that the PCPD's work needs to improve, especially in monitoring the data users. An interviewed scholar also pointed out that the PDPO is relatively outdated in securing citizens' rights to privacy, which is significant when reviewing both the bureau and the Ordinance.

2. **Citizens are concerned with the safety of their privacy rights due to the outdated PDPO.**

Given the impact technological advancement has on privacy and morals, the EU implemented the GDPR in 2018, with the aim of letting data subjects retake control by increasing the accountability and transparency of data users. The progress made by GDPR shows that the PDPO of Hong Kong is outdated, causing local citizens to become more concerned with their privacy rights.

Following the implementation of GDPR, the PCPD did realise the insufficiency of the PDPO, and proposed the following amendments in January 2020: "a) Establish a mandatory data breach notification mechanism; (b) Strengthen the data retention period regulation; (c) Review penalties for the non-compliance with the PDPO by increasing relevant criminal fines and exploring the feasibility of introducing direct administrative fines; (d) Regulate data processors directly to strengthen the protection of the personal data being processed; (e) Amend the definition of "personal data" to cover information relating to an "identifiable" natural person; and (f) Curb doxxing behaviour through criminalising doxxing, conferring on PCPD statutory powers to request the removal of doxxing contents from social media platforms or websites, as well as the powers to carry out criminal investigations and prosecutions, etc."

3. **The proposed amendments of the PDPO are controversial, and highlights why the interests of all stakeholders should be balanced between the privacy of individuals and public interest.**

Although the PCPD's proposals to amend the PDPO can strengthen the protection of citizens' privacy, stakeholders from all sectors have varying opinions on the importance of the right to privacy. When interviewed, the former Privacy Commissioner for Personal Data reminded the public that the reform of the PDPO should be guided by factors that include: the legitimate purpose of the reform, the pressing need for the reform, the proportionality between the proposed change and the pursuance of the legitimate purpose, and whether there are any other practical and effective means to address the problem.

As the public become more concerned with their privacy, subsequent policies, and the proposed amendment of PDPO, are raising some controversies in Hong Kong:

3a. The definition of personal data in the PDPO is outdated, and there is a lack of regulation on data retention. Despite such, citizens' concerns about the privacy issues of the LeaveHomeSafe app have not been addressed.

The Office of the Government Chief Information Officer (OGCIO) implemented the LeaveHomeSafe app on 16th November 2020 to allow citizens to keep track of entering and leaving different venues electronically. However, the data security and privacy protection implications of the app has been controversial among the public.

The on-site survey result of a research study, conducted by Youth I.D.E.A.S. in November 2020, showed that almost three quarters of respondents (73.8%), will not use the LeaveHomeSafe app. The survey result of this research showed that over half of the respondents had not yet installed the LeaveHomeSafe app and were either still considering (25.5%) or did not intend to use it (26.2%). Of these 80.9% said they did not use the app because of concerns about privacy.

Even though Mr. Alfred Sit (Secretary for Innovation and Technology Bureau) has assured the public that the app passed the security risk assessment and personal-privacy impact assessment by an independent third-party, an interviewed expert pointed out that the PDPO's definition of personal data is narrower than that of the GDPR - i.e. it does

not cover data that can be used to identify a person. Another interviewed expert added that while the location data can be used to identify an individual, there is no law to regulate the Government's data retention. This explains the hope that the PCPD can amend the definition of personal data in PDPO and regulate data retention.

3b. The PDPO has not yet adjusted the current data breach notification mechanism, undermining the accountability of data users; the Real-name Registration Programme for SIM Cards should not be implemented in a rush.

To combat crime, the HKSAR government launched a public consultation on 30th January 2021 regarding the Real-name Registration Programme for SIM Cards. The Government proposes to implement the Programme through a regulation made pursuant to the Telecommunications Ordinance, providing the necessary legal basis for telecommunications operators to register, collate and keep the registration information of users as required under the regulation. The survey result of this research showed that close to half of the respondents (41.8%) were against legislation to introduce Real-name Registration Programme for SIM Cards. Major concerns included damage to privacy (65.5%) and freedom of speech (42.3%).

Indeed, some key requirements in the Real-name Registration Programme for SIM Cards have raised concerns among members of the public and relevant stakeholders. The survey result of this research shows that over half of the respondents (52.7%) were not in favour of the requirement that "in certain urgent or emergency situations, LEAs could request telecommunications operators to provide registration information of a SIM card without a warrant." Also, over half of the respondents (53.5%) were not in favour of the requirement that "the records of the registered SIM card users should be kept by the respective telecommunications operators for at least 12 months after the SIM cards have been deregistered."

An interviewed expert pointed out that not all telecommunications operators can maintain the cybersecurity of their database. Given that the PDPO is relatively outdated in terms of preventing data-breaches, he

added, the only way to protect users' privacy is to minimise the personal data collected by telecommunications operators and shorten the duration of data retention. An interviewed telecommunication operator also pointed out that there is not sufficient time for them to prepare for complying with the registration requirements. She suggested the government extend the preparation phase to at least 2 years and provide a grace period.

As the research results demonstrate, the legislation of the Real-name Registration Programme for SIM Cards is still controversial, especially the key requirements that raise privacy concerns of the public, and preparation challenges to relevant stakeholders. Therefore the Programme should not be implemented in a rush before the PDPO has been reformed to provide better protection against data-breach accidents and more accountability for data users.

3c. The PDPO has not yet improved the protection of sensitive personal data despite the infringement to privacy by facial recognition, highlighting privacy concerns about Smart Lampposts and security cameras.

Since the end of June 2019, the HKSAR government has launched the "Multi-functional Smart Lampposts" Pilot Scheme to collect various types of real-time city data such as meteorological data, air-quality data and traffic flow.

In general, DPP6 and section 18 of the PDPO provides data subjects with the right to request access to, and correction of their own personal data. However, section 58 of the PDPO provides exemptions from the compliance requirement under circumstances related to crime prevention or prosecution. The on-site survey result of this research showed that two-thirds of the respondents (66.1%) are in favour of this exemption, whereas the youth have reservations about such terms.

In addition, the PCPD once stated that if a CCTV system is installed for real-time surveillance purpose without the intention or attempt to identify individuals, its use will normally not involve collection of personal data as defined under the Ordinance and is therefore not

regulated under the Ordinance. An interviewed expert thought that such regulations are outdated as facial recognition technology these days can be used to analyse the recordings of security cameras at a later date to track a person's whereabouts thereby identifying him/her.

The survey result of this research showed that 92.5% of respondents agreed that biometric data such as fingerprints and facial images were sensitive. Moreover, over half of the respondents (56.6%) agreed that CCTV footage for real-time monitoring should be regulated under the PDPO. The survey result also shows that members of the public are concerned if biometric data (facial images) is protected by the PDPO given the rapid development of facial recognition.

3d. The respondents agree that doxxing should be dealt with by granting more power to the PDPC. However, some interviewed experts worried that such a move would harm freedom of speech and the freedom of the press in Hong Kong.

Given the emergence of online content hosts and popularisation of outsourcing the processing of personal data, the storage, collection (other than from the data subject directly) and dissemination of personal data has become much easier. Yet, this also makes it easier for data subjects to suffer from doxxing (personal data being disclosed without consent).

There are voices in the public that the PDPO is insufficient to address doxxing in Hong Kong. To deal with the problem, the Chief Executive proposed in February 2021 that the PDPO will be amended as follows: "(a) Doxxing acts will be criminalised as an offence; (b) The PCPD will be empowered to carry out criminal investigation/s and institute prosecution/s; (c) The Commissioner will be conferred statutory powers to serve notices to demand actions to cease or restrict disclosure of doxxing content and apply for injunctions. It is aimed that the drafting of amendments will be finished for scrutiny within this Legislative Council term."

The survey result of this research showed that nearly two-thirds of respondents (65.5%) were in favour of criminalising the act of doxxing.

However, more than half of the respondents (59.9%) agreed that the PCPD should have statutory powers to request the removal of doxxing content from social media platforms or websites. Moreover, 70.8% agreed that the PCPD should be empowered to carry out criminal investigations and prosecution. However, the survey results also showed that youth have reservations regarding the three proposed amendments.

An interviewed scholar worried that such amendments will hinder the press from conducting journalistic investigations through searching online public records of various government departments, thus infringing the freedom of the press and the right-to-know of the public. Without doubt, it is a difficult challenge for the Government to balance the privacy-protection interests of the public and relevant stakeholders.

Recommendations

Based on the research results and discussion points, we have made the following suggestions to update the PDPO and improve the PCPD's effectiveness to better balance privacy and public interest where public health, public security, technological development and the right to information are affected.

1. **Expand the definition of Personal Data and introduce the category of "sensitive personal data" in the PDPO.**

   Although the PCPD had already proposed in January 2020 to expand the definition of "personal data" under the PDPO to cover information relating to an "identifiable" natural person, such a proposal has yet to effectively address privacy concerns in view of today's wide use of tracking, data analytics and facial recognition technology.

   With reference to Article 4(1) and Article 9 of the EU's GDPR, this research recommends the Government to expand the definition of Personal Data to cover information that can be used to track and identify a person, such as location data and real-time monitoring of CCTV footage.

The Government should also introduce a new category of 'sensitive personal data', the processing of which should be subject to specific conditions. It is the Government's obligation to renew the definition of personal data in the 1996 PDPO to better protect citizen's privacy in the age of Big Data.

2. **Introduce the "Accountability Principle" and a '"certification scheme".**

This research found out that the government did not carry out third-party Privacy Impact Assessments (PIA) for neither the LeaveHomeSafe app nor Smart Lampposts before these two technologies were introduced and led to the public's privacy concerns.

With reference to Article 35 and Article 42 of the EU's GDPR, this research recommends the Government to introduce an "Accountability Principle" for assessment and a certification scheme for high-risk projects. High-risk projects include: "(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of sensitive personal data, or of personal data relating to criminal convictions and offences; and (c) a systematic monitoring of a publicly accessible area on a large scale."

3. **Introduce a "tech supervisory sandbox" for start-ups.**

As interviewed experts said in this research, some relevant stakeholders, especially startups, worried that the amendment of the PDPO may hinder technological development.

Referring to the Fintech Supervisory Sandbox (FSS) launched by the HKMA in September 2016, this research recommends the Government introduces a mechanism that allows some exemptions for start-ups so that they can make gradual refinements to their data privacy strategy before complying in full with PCPD supervisory requirements.

The management of a tech start-up that is allowed to use the Sandbox should ensure that the following safeguards are in place: "(a) boundary – clear definitions about the scope and phases (if any) of the pilot trial, the timing, and termination arrangements; (b) customer protection measures – measures for protecting the interests of customers during the trial, which generally cover the selection of customers who understand the associated risks and voluntarily join the trial, complaint handling, compensation of any financial losses suffered by customers, and arrangements for customers to withdraw from the trial; (c) risk management controls – compensating controls for mitigating the risks arising from less than full compliance with supervisory requirements and the risks posed to the bank's production systems and other customers; and (d) readiness and monitoring – readiness of the systems and processes involved in the trial and close monitoring of the trial."

Such a mechanism allows start-ups to collect data and users' feedback so that they can make refinements to their initiatives, thereby expediting the launch of new technology products and reducing development costs. In this way, the amendment of the PDPO would not hinder the technological development of Hong Kong.

4. **Provide access to a complaints agency and court-ordered remedies for victims of doxxing.**

Since the social movement in 2019, the issue of doxxing has been of great concern to Hong Kong society. There is no doubt that cyberbullying has to be curbed. Yet the proportionality between tackling cyberbullying and the proposed penalties should be taken into consideration during the PDPO's review to maintain the balance between citizens' freedom of expression and privacy rights.

With reference to New Zealand's Harmful Digital Communications Act (HDCA), this research suggests that the offence of doxxing should have a relatively high criminal threshold; the Government introducing a two-tier complaint handling process as an informal resolution mechanism, comprising content moderation by online content hosts and complaint handling by the PCDC.

There should also be a "safe harbour" provision in the PDPO for online content hosts to protect themselves against legal liability through a "notice and takedown" system for allegedly harmful content. It is suggested that upon receiving a complaint, the online host is required to notify the author of the content and request the author's agreement to take down the content. If the author refuses to take down the content after notification, the online content host is required to leave the content in place and inform the complainant within the next 48 hours. The victims of cyberbullying can then seek remedies from the court. The above procedure incentivises online content hosts to moderate cyberbullying without infringing citizens' freedom of expression.

As for the role of the PCDC, it should seek to settle complaints through negotiation, mediation and persuasion. Failing that, court proceedings may be initiated. The court is required to consider whether the disclosure of personal data is in the public interest before granting protection orders, and its civil and criminal decisions can be appealed.

5. **Amend the PDPO first before enacting the Real-name Registration Programme for SIM Cards legislation.**

The Government should amend the PDPO before introducing legislation for the Real-name Registration Programme for SIM Cards.

Some relevant stakeholders interviewed in this research worried that there were still a lot of unaddressed concerns about the Real-name Registration Programme for SIM Cards given such a short consultation period. These concerns vary from data retention, the number of SIM Cards allowed for registration, the legal liability of the telecommunication operators to the duration of preparation time. An interviewed expert also added that the current PDPO is relatively outdated in terms of data-breach prevention. He suggested that the Real-name Registration Programme for SIM Cards should not be implemented in a rush before the loopholes of the PDPO have been filled to avoid an increase in cybersecurity risk.

This research suggested the bureaus responsible for the Real-name Registration Programme for SIM Cards and the PDPO amendments should negotiate to first let the PDPO be amended before the telecommunications operators collect data from the more-than-half of mobile subscribers (56%) in Hong Kong. It is believed citizens would have greater confidence in the Real-name Registration Programme for SIM Cards with sound protection of their personal data.