66th ABA Section of Antitrust Law Spring Meeting
Wednesday, April 11, 2018

Protecting Consumers and Competition – International Emerging Technologies

Session Chair: **Robert Mahini, Senior Counsel, Google Incorporated, Washington, DC**

Moderator: **Deon Woods Bell, Senior International Attorney, Federal Trade Commission, Washington, DC**

Speakers: **Falk Schöning, Hogan Lovells LLP, Brussels**
Shaundra Watson, Director, Policy, Business Software Alliance, Washington, DC
Stephen Kai-yi Wong, Barrister, Privacy Commissioner for Personal Data, Hong Kong, China

Engineering Privacy through Accountability

by Stephen Kai-yi Wong, Barrister
Privacy Commissioner for Personal Data, Hong Kong, China

Table of Contents

Executive Summary

Prevalent use and diverse applications of big data analytics, AI, FinTech and other digital platforms and tools in the modern ICT age have transformed our daily lives and business developments. Yet, lurking privacy risks and ramifications challenge the regulatory strengths of our existing data protection laws. Ubiquitous and covert data collection undermines privacy principle of data minimisation, attenuating individuals' control over data. Unpredictable analytics contest the principles of notice and consent, and purpose and use limitations. As profiling amplifies risks of re-identification, the traditional dichotomy between "personal data" and "non-personal data" defining the ambits of data protection laws is slowly eroded. Applications of predictive or derived outcomes in automated decision making in vital areas such as credit rating, employment and law enforcement may lead to discrimination or negative societal effects besetting individuals' dignity and fundamental human rights.

Data protection regulators around the world are racing to devise effective regulatory solutions to keep pace with revolutionary developments in the ICT age. Law amendment by, for example, expanding the definition of "personal data" and extending the regulation to new data processing methods like profiling is one of the feasible solutions where there are community consensus, as well as governments' and lawmakers' support. Nonetheless, fast-paced technological developments threaten to unsettle regulators' legal efforts.

To embrace new technologies as they emerge and build a strong bulwark of privacy protection, regulators must make a regulatory shift from instructional rules to long-standing directional principles. Accountability, a comprehensive, flexible and responsibility-based framework encapsulating these directional principles, rises as one of the solutions. Recognised in data protection instruments and by data protection regulators, it can strike a balance between seemingly irreconcilable interests of personal data protection and innovative use of data in data-driven economies. Moreover, accountability helps data protection regulators achieve more with less, strengthening regulatory effectiveness by transforming abstract privacy principles to concrete protection mechanisms. It also allows businesses to make innovative use of data responsibly and trustfully. Education efforts in cultivating privacy awareness, if not a culture, amongst businesses and consumers are crucial in generating momentum for businesses to embrace accountability.

Part I – Privacy Risks and Ramifications in the ICT Age

Revolutionary technologies such as big data analytics, AI and the rise of digital platforms and tools such as FinTech in the modern ICT age have proved to be transforming not only the business world but also the personal data privacy protection landscape.

Big data analytics, in simple terms, is "*the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decisions*[1]". Data sources employed in big data analytics are often described as "high-volume", "high-velocity" and "high-variety"[2] and are gathered ubiquitously from individuals' offline and online footprints. AI algorithms propel big data analytics to produce intelligent inferences and anticipate future events. Today, data-driven businesses draw insights from big data analytics and AI to inform their decisions in areas from marketing, health services, manufacturing, education, transportation to law enforcement.

Widely popular social media and e-commerce platforms tap into big data and AI analytics to provide personalised user experiences and streamlined advertising to aggrandise user databases and revenues. Rise of FinTech such as crowdfunding, mobile payment and money transfer services help financial institutions revolutionise user experiences[3]; similar to digital platforms, they utilise big data analytics to inform their decisions.

Significant business progress and commercial benefits brought by new technologies and platforms in the ICT age have created equally palpable privacy risks and implications that challenge the regulatory strengths of existing data protection laws.

(1) Ubiquitous and Covert Data Collection Challenges Data Minimisation and Individuals' Control over Data

Powerful computing and low-cost storage enable organisations to collect data ubiquitously, covertly and automatically on a large-scale to feed into the pool of

[1] European Data Protection Supervisor. (Nov 2015). *Opinion 7/2015 - Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability*. Retrieved from https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[2] Gartner. *IT Glossary: Big Data*. Retrieved from https://www.gartner.com/it-glossary/big-data

[3] Marr, Bernard. (2017, Feb 10). The Complete Beginner's Guide To FinTech In 2017. *Forbes*. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/02/10/a-complete-beginners-guide-to-fintech-in-2017/#6a3cd5233340

intelligence data. Individuals' use of smart devices and systems like smartphones, wearable devices and social media networks may lead to release of their information in public domains, and tracking of their online and offline behaviour, sometimes without their knowledge. The rise of data brokers facilitates covert circulation of data and undermines individuals' ability to control how their data is collected, used and transferred.

Big data analytics and AI thrive on enormous amount of data being collected to produce profound insights, running counter to the principle of data minimisation. Ubiquitous and covert data collection blurs the demarcation between private and public spaces and challenges the principles of adequate notification and data transparency, thus eroding individuals' control over their data.

(2) Unpredictable Analytics, Principles of Notice and Consent, Purpose and Use Limitations

As big data and AI analytics "rely not on causation but on correlations[4]", they may generate surprising revelations. All too accurate predictions may reveal sensitive and "core private information[5]", causing embarrassment, psychological and reputational harms to individuals. For instance, Target, a U.S. retailer, analysed consumption patterns to predict a teenager's pregnancy status well before her father knew, revealing her pregnancy status to her family members[6]. Powerful algorithms now boast the ability to infer, by analysing Facebook "likes", detailed sensitive information like sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, addictive substances use, parental separation, age and gender with high accuracy[7].

Powerful analytics render even organisations themselves at a loss as to what data may potentially reveal, attenuating their ability to inform individuals of attendant risks during data collection. Individuals are unable to understand, or be informed

[4] Rubinstein, I. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law, 3 (2)*, 74-87.

[5] Millar, Jason. (2009). Core privacy A Problem for Predictive Data Mining. In I. Kerr, V. Steeves & C. Lucocket (Eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (pp. 103-119). New York, N.Y.: Oxford University Press.

[6] Duhigg, Charles. (2012, Feb 16). How Companies Learn Your Secrets. *The New York Times Magazine.* Retrieved from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

[7] Kosinski, M., Stillwell, D. & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the USA, 110(15)*, 5802-5805. https://doi.org/10.1073/pnas.1218772110

of the full extent of privacy consequences and give informed consent [8]. Unpredictable analytics challenge the principle of purpose limitation [9] as organisations are unable to specify how they will use the data. Individuals are stripped of the ability to control "when, how and to what extent information about them is communicated[10]" and adopt privacy protection accordingly. Uncertainty looms as to whether predicted/derived data are protected under existing data protection laws, which mostly regulate standing facts/descriptions.

(3) Profiling[11], Risks of Re-identification and Distinction between "Personal Data" and "Non-Personal Data"

Profiling, big data and AI analytics uncover new correlations to produce insights for decision making (often automated) in businesses. Profiling often involves aggregating and combining datasets, at the expense of destroying individuals' anonymity or revealing their sensitive information. For instance, in 2008, Netflix released anonymised Netflix movie ratings dataset to contenders in a competition to help improve their service; little did they know that the contenders were able to combine the anonymised ratings with publicised Internet Movie Database ratings dataset to re-identify subscribers and indirectly reveal their political views and religious beliefs through their list of movies viewed[12].

Risk of re-identification undermines the effectiveness of anonymisation and the fundamental distinction between "personal data" and "non-personal data" [13], casting doubts on when data protection comes in for businesses to take up obligations and reciprocally, for data subjects to be entitled to their rights.

---

[8] Tufekci, Zeynep. (2018, Jan 30). The Latest Data Privacy Debacle. *The New York Times*. Retrieved from https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html

[9] European Data Protection Supervisor. (Nov 2015). *Opinion 7/2015 - Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability*. Retrieved from https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

[10] Westin, A. (1968). *Privacy and Freedom.* New York, NY: Atheneum.

[11] There is no universal definition for "profiling". Under Article 4(4) of the General Data Protection Regulation , "profiling" is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[12] Narayanan, A. & Shmatikov, V. (2008). *Robust De-anonymization of Large Sparse Datasets*. In *Proceedings of the 2008 IEEE Symposium on Security and Privacy*. Paper presented at 2008 IEEE Symposium on Security and Privacy, Oakland, California, USA (pp.111-125). Los Alamitos, California: IEEE Computer Society.

[13] Rubinstein, I. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law, 3 (2)*, 74-87.

Revelation of sensitive information through re-identification may cause emotional and psychological harms to individuals. It undermines individuals' control over data as they do not know what inferences may be drawn or what their other data would be revealed when they hand over their data.

(4) Inaccuracy of Inferences, Discrimination and Other Negative Societal Effects

Inaccurate inferences drawn and predictions made by big data and AI analytics may conflict with the principle of data accuracy under data protection laws[14]. When these outcomes are used for automated decision making in vital areas such as credit ratings, job prospects, eligibility for insurance coverage and welfare benefits[15], the individuals' socio-economic status may be adversely affected, causing them irreparable harms and impacting their fundamental rights beyond privacy intrusions. An extreme reality is that people will be judged not on the basis of their actions, but on the basis of what all the data about them indicate their probable actions may be[16].

Inputs of inaccurate or prejudicial data into algorithms may reinforce social prejudices and lead to discriminatory decisions. For instance, algorithms heavily relying on factors like commuting distance with unproven correlation to employees' duration of staying with jobs unfairly exclude those living in remote areas despite their qualifications[17]. Creditors using algorithms to assign credit risks to individuals who shop at certain stores, based on the default histories of other shoppers frequenting the same stores, may well unfairly discriminate against the individuals[18]. Improper use of algorithms to predict crime hotspots and allocate

[14] Rubinstein, I. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law, 3 (2)*, 74-87.
[15] Rubinstein, I. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law, 3 (2)*, 74-87.
[16] Datatilsynet. (2013). *Big Data – Privacy Principles Under Pressure*. Retrieved from https://www.datatilsynet.no/en/about-privacy/reports-on-specific-subjects/big-data--privacy-principles-under-pressure/
[17] Executive Office of the President. (May 2016). *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf
[18] Staab, S., Stalla-Bourdillon, S., & Carmichael, L. (2016). *Observing and Recommending from a Social Web with Biases (Part I Web Science Institute (WSI) PUMP-PRIMING PROJECT).* Retrieved from *https://arxiv.org/pdf/1604.07180*

police manpower[19] may lead to "race-based policing" discrimination[20]. Sole reliance on algorithms by U.S. courts for sentencing to reduce recidivism[21] may also end up with unfair discrimination because of the lack of value judgement and context consideration. When algorithms and decision-making processes are automatic, opaque and lack transparency, individuals cannot exercise effective control over their own data, not to mention defence of their own interests and rights.

Digital platforms' efforts in providing their users with personalised contents and news feeds have sparked concerns of "filter bubble" effect – the notion that users would become separated from information that disagrees with their viewpoints (for the algorithms only present them with information that they would like to see). The practice is also alleged of interference in users' thoughts, as well as elections as alleged in the recent Facebook/Cambridge Analytica incident. Further, when governments team up with digital platforms to provide data-driven public services, detailed mapping of individuals' lives threaten to entangle individuals in "datasurveillance[22]" system and create "panoptic" effects[23] causing "self-censorship[24]".

[19] Staab, S., Stalla-Bourdillon, S., & Carmichael, L. (2016). *Observing and Recommending from a Social Web with Biases (Part I Web Science Institute (WSI) PUMP-PRIMING PROJECT).* Retrieved from *https://arxiv.org/pdf/1604.07180*

[20] Withrow, B. (2004). Race-Based Policing: A Descriptive Analysis of the Wichita Stop Study. *Policy Practice and Research, 5(3),* 223-240.

[21] *State of Wisconsin v. Eric L. Loomis* (2016) Case no: 2015AP157-CR. Available from http://caselaw.findlaw.com/wi-supreme-court/1742124.html

[22] Bennett, C.J. (1996). The Public Surveillance of Personal Data: A Cross-National Analysis. In D. Lyon & E. Zeureik (Eds.), *Computers, Surveillance and Privacy* (pp. 237-259). Minneapolis: The University of Minnesota Press.

[23] Ibid.

[24] Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review, 50(4),* 1193-1294.

Part II – Hong Kong Personal Data (Privacy) Ordinance (Cap 486, Laws of Hong Kong)

How should we as data protection regulators respond in the wake of these new challenges in the privacy landscape? To make amendments to our existing data protection laws may be a straightforward solution, if data protection authorities can reach consensus in communities and garner governments' and lawmakers' support. Legislative instruments providing consequences for non-compliance will inject concrete support into our data protection laws.

Surveying Hong Kong's data protection law, the Personal Data (Privacy) Ordinance (**PDPO**), the following observations are worth noting:

(1) Definition of "Personal Data", ICT Realities of Re-identification, Profiling and Analytics

This proposition builds on the lapsing demarcation between "personal data" and "non-personal data" in the ICT age, exacerbated by amplified risks of re-identification and strengthened profiling and analytics. Powerful analytics enable the revelation of intimate details of individuals' lives from innocuous data (e.g. location data, online identifiers like IP address and posts on social media platforms). Availability of powerful search engines, people search services and data brokers create a treasure trove of data for data users (i.e. data controllers) to weave together disparate bits of data to reveal individuals' identities, their movement patterns, occupations, preferences, friends, etc. New technological developments have created new regulatory challenges, making it necessary for us to revisit the definition of "personal data" under the PDPO to broaden its scope of protection.

Hong Kong's PDPO comes into play when data qualifies as "personal data" by fulfilling three limbs: (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable. [Section 2(1)] Non-fulfillment of any of the three limbs disqualifies the data as "personal data". Under limb (b), we take a "totality approach" to consider all relevant data controlled by the data user to decide if the threshold is satisfied[25].

[25] Wong, Stephen Kai-yi & Zhu, Guobin. (Eds.). (2016). *Personal Data (Privacy) Law in Hong Kong – A Practical Guide on Compliance*. Hong Kong: The Office of the Privacy Commissioner for Personal Data, Hong Kong and The City University of Hong Kong Press.

While the definition of "personal data" under the PDPO is widely crafted, it may nonetheless fall short in effectively regulating emerging privacy harms in the ICT age – running counter to people's widely held expectations or even worse, leading to absurdities. These can be illustrated by three examples:

(i) Under the PDPO, a telephone number *per se* does not qualify as "personal data" as it does not enable the identity of individual to be ascertained. This runs contrary to widely held expectations that a telephone number, in particular a mobile telephone number, is "personal data". Moreover, given powerful search engines and the prevalence of telephone number look-up services, it is possible to track down an individual by using his telephone number alone. Reportedly hackers are also able to track an individual's geolocations and record his telephone calls without his knowledge by using his mobile telephone number[26] [27].

(ii) Email addresses with brief identifying information as usernames such as <skywong@gmail.com> may not qualify as "personal data" under the PDPO, because the username *skywong* alone may not enable the identity of an individual to be ascertained, and the domain name *gmail.com* does not reveal any affiliations. Nonetheless, with powerful search engines and/or sophisticated profiling techniques, it is likely that the identities of the owners of such email addresses can be uncovered by combining fragmented information in the public domains.

(iii) An IP address is used to identify a computer, not an individual. Therefore it has long been considered that IP address alone is not personal data under the PDPO[28]. However, profiling may enable the identity of an individual to be pinned down via an IP address. The EU's position in this regard is noteworthy, under which IP address has received recognition as "personal data". The CJEU earlier ruled on the

[26] Bureau, Brigitte, Cullen, Catherine, & Everson, Kristen. (2017, Nov 22). Hackers only needed a phone number to track this MP's cellphone. *CBC News*. Retrieved from http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338

[27] Recently, the Hong Kong Government has proposed to set up a statutory do-not-call register to ban telemarketers from making person-to-person calls to individuals who register their telephone numbers on the register. The proposal follows public opinion over telemarketers having been trying to get around the PDPO regulation by using individuals' telephone numbers only (without identifying the individuals concerned by name, etc.) to make person-to-person marketing calls. It is proposed that the Privacy Commissioner for Personal Data, Hong Kong, China would administer the register and enforce the new rules. Law amendment is required for putting in place the new rules.

[28] *Shi Tao v The Privacy Commissioner for Personal Data* (2007), Case No. 16/2007 of the Administrative Appeals Board. Available from https://www.pcpd.org.hk/english/enforcement/decisions/files/AAB_16_2007.pdf

application of Data Protection Directive 95/46/EC to IP address in two cases, namely *Scarlet Extended*[29] and *Breyer*[30]. In *Scarlet Extended*, the CJEU held that the IP addresses in the possession of Internet service providers were protected personal data because the IP addresses allowed the Internet users to be precisely identified. In the more recent *Breyer*'s case, the CJEU held that a dynamic IP address recorded by a website operator (in this case a German government body) when an individual visited the website constituted personal data of that individual, provided that the website operator had the legal means enabling it to identify the individual with the additional information in the possession of the Internet service provider. The EU General Data Protection Regulation (**GDPR**), effective in May 2018, consolidates this position by explicitly recognising "online identifiers" as "personal data"[31].

Risks of re-identification powered by profiling and analytics in the ICT age trigger the fast collapse of the traditional demarcation between "personal data" and "non-personal data". Given the strong data processing powers of neural networks, machine learning and AI, it is perhaps no exaggeration to suggest that re-identification will soon be a given. In the circumstances, so long as a piece of data relates to a living individual, it qualifies as "personal data", without the need to consider whether the individual concerned is identified or identifiable. These developments urge us to revisit our definition of "personal data" under the PDPO, in particular the meaning and applicability of limb (b): "*from which it is practicable for the identity of the individual to be directly or indirectly ascertained*". In assessing the practicability of identification, it may be necessary to take into account all means reasonably likely to be used by a data user or any other person to identify an individual. For clarity purposes, the feasibility of a prescriptive approach specifying recognised data items in the definition (as in the EU GDPR) should be explored.

---

[29] *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (2011), Case C-70/10. Available from http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=306533

[30] *Patrick Breyer v Bundesrepublik Deutschland* (2016), Case C-582/14. Available from http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945

[31] Under EU GDPR Article 4(1), 'personal data' is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, **an online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

On the other hand, a definition that is too wide and aims to preempt every challenge foreseeable may unduly restrict organisations' innovative use of data. It is hence pertinent to balance various interests in crafting a definition in line with the ICT realities, to cope with regulatory challenges and to bring the PDPO in line with widely held expectations as well as overseas data protection legal standards.

(2) "Collection of data" in *Eastweek Publisher Limited & Another v Privacy Commissioner for Personal Data* (CACV 331/1999); [2000]2 HKLRD 83

Background of the *Eastweek* Case

The *Eastweek* case is a landmark case on the PDPO. The case is of cardinal importance as it defines the meaning of "*collect*" with respect to personal data and clarifies under what circumstances the PDPO comes into play.

The *Eastweek* case arose from a complaint lodged with the Privacy Commissioner for Personal Data, Hong Kong, China (**PCPD**) back in September 1997. The complainant, while walking on the street one day, was photographed by a magazine photographer without her knowledge or consent. The photograph was subsequently published in the magazine accompanied by unflattering and critical comments on her dressing style. The matter caused embarrassment and inconvenience to the complainant amongst her clients and colleagues.

The PCPD decided that the publisher of the magazine contravened Data Protection Principle (**DPP**) 1(2)(b) in Schedule 1 to the PDPO, i.e. fair collection of personal data. The publisher took the PCPD's decision to the Court of First Instance for judicial review, but the application was dismissed. The publisher then appealed to the Court of Appeal. In March 2000, by 2-1 majority, the Court of Appeal reversed the decision of the Court of First Instance, and quashed the PCPD's findings.

Implications of *Eastweek* case

The Court of Appeal laid down two necessary conditions for the collection of personal data:

(i) the collecting party must be thereby compiling information about an individual; and
(ii) the individual must be one whom the collector of information has identified or intends or seeks to identify.

The Court of Appeal held that there was no collection of personal data by the publisher because of "*the complainant's anonymity and the irrelevance of her identity so far as the photographer, the reporter and Eastweek were concerned*", and that the publisher "*remained completely indifferent to and ignorant of her identity right up to and after publication of the offending issue of the magazine.*"

In the *obiter dicta*, the Court of Appeal discussed a few provisions of the PDPO that could "*only operate sensibly on the premise that the data collected relates to a subject whose identity is known or sought to be known by the data user as an important item of information*", such as an individual's right to request for access to his own personal data [section 18] and the use limitation of personal data [DPP 3].

By interpreting the above judgement and *obiter dicta*, it appears that there is a third condition for "collection" of personal data which is closely related to the second condition, i.e.

(iii) the identity of the individual must be an important item of information to the collecting party.

The *obiter dicta* also imply that the PDPO would not come into play if there is no collection of personal data in the first place.

<u>"Collection of data" in the *Eastweek* case in the ICT Age</u>

The incident of the *Eastweek* case occurred more than 20 years ago. It is indisputable that ICT developments and our ways of processing data (including personal data) have undergone revolutionary changes. ICT developments invite us to revisit the meaning of "collect" as defined in *Eastweek* case, which, as illustrated in the following examples, may deprive individuals of PDPO protection in face of emerging privacy harms.

(i) Businesses may track individuals' online activities with cookies and slowly build up profiles to send targeted marketing messages to them. The businesses may not have identified or intend to identify the individuals in the first place, hence according to the dicta in the *Eastweek* case, there is no "collection" of data and as such, the PDPO would not apply, leaving the data about the individuals' online activities unprotected. The application of the *Eastweek* case also places extra burden on the individuals and regulators to prove the intent of the

businesses before the individuals can exercise their privacy rights in respect of the data.

(ii) While data users getting hold of data may be completely indifferent to and ignorant of the identities of the individuals being tracked initially, it is nonetheless possible for them, or other parties, to subsequently identify individuals directly or indirectly and reveal details of their intimate lives by applying techniques of big data analytics and profiling. It is therefore desirable for the PDPO to come into play in the first place to ensure that the data users have afforded adequate protection to the data.

(iii) As in other world cities, CCTVs are widely used in Hong Kong and many other parts of the world for security purposes. Under the PDPO, if a person installs CCTVs merely for monitoring the surroundings, as opposed to identifying individuals, in the absence of "collection", the PDPO will not come into play. Yet, it is undeniable that amassing databases of CCTVs' images increases risks of privacy harms from data mishandling or breaches.

(iv) Big data analytics and AI algorithms mostly function to predict trends to inform business decisions, as opposed to identifying individuals, though the operations necessarily involve use of personal data. If general privacy principles (e.g. transparency, data minimisation, use limitation, data security) do not apply as a result of not meeting the conditions of "collect", this may undermine protection of the mass of data.

Surveying the position in overseas jurisdictions such as the European Union[32], Singapore[33], Canada[34], Australia[35] and New Zealand[36], it appears that their laws do

[32] Under EU GDPR Article 4(2), 'processing' is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". There is no "identification" threshold before a processing activity qualifies. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[33] Singapore's Personal Data Protection Act does not define the term "collection" and the term would apply as it is commonly understood. "Collection" refers to any act or sets of acts through which an organisation obtains control over or possession of personal data. Please refer to:
Personal Data Protection Commission. (2013, rev. 2017). *Advisory Guidelines On Key Concepts In The Personal Data Protection Act.* *https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-(270717).pdf?la=en*

not impose any condition on "collect", and the data protection laws come into play whenever personal data is involved, which denotes a broader scope of data protection.

Given the foregoing, revisiting the definition or the necessary conditions of "collect" as defined in the *Eastweek* case may be necessary to align the PDPO with the realities of modern ICT development, commonly held expectations and keep it on a par with overseas data protection laws.

(3) Privacy Protection for Profiling

Profiling and automated decision making lead to privacy risks which cannot be left unattended.

DPP 1 and DPP 3 of the PDPO regulate the collection and use (including disclosure) of personal data respectively. While the six DPPs[37] of the PDPO intend to regulate the whole lifecycle of data processing, there is no explicit reference to "processing" or "profiling" in the DPPs. This calls into question whether profiling alone (i.e. a stage in the lifecycle of data processing after collection and before use or disclosure) is regulated by the PDPO.

Moreover, while the use of derived/predicted data generated by analytics and profiling may have an impact on the interests, rights and freedom of individuals, it is unclear whether such data falls within the ambit of the PDPO and so it remains uncertain whether such activities are regulated as a practical matter.

We observe that overseas jurisdictions have extended their reach to regulating privacy harms from profiling and automated decision making. For instance, the EU GDPR, effective in May 2018, regulates "profiling"[38] and protects individuals from impactful automated decisions.

---

[34] Canada's federal privacy law for private-sector organisations - The Personal Information Protection and Electronic Documents Act (PIPEDA) does not impose "identification" threshold for data collection. http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[35] Australia Privacy Act 1998 does not impose "identification" threshold for data collection. https://www.legislation.gov.au/Details/C2017C00283

[36] The New Zealand Privacy Act 1993 does not impose "identification" threshold for data collection. http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

[37] DPP 1 – collection of data; DPP 2 – retention and accuracy of data; DPP 3 – use of data; DPP 4 – security of data; DPP 5 – transparency of privacy policy and practice; DPP 6 – access to and correction of data.

[38] The EU GDPR defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health,

Given profiling and the use of profiling for automated decision making may cause privacy harms to individuals if unregulated, it is pertinent to make clear in the PDPO that it regulates such activities.

---

personal preferences, interests, reliability, behaviour, location or movements" [Article 4(4)]. Article 22(1) allows data subjects to have the right not to be subject to a decision *based solely* on automated processing, including profiling, which produces *legal effects* concerning him or her or *similarly significantly affects him or her*. General data protection principles apply to profiling activities, such as requirement for processing to be lawful, fair and transparent, as well as data minimisation, purpose limitation, data accuracy and storage limitation. Data subjects are also entitled to rights such as the right to be informed, the right of access, the right to object and the right to rectification.
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Part III – From Compliance to Accountability

Efforts to amend data protection laws to expand the scope of privacy protection are laudable. When more data and data processing activities are rightly brought under the shield of data protection laws, the next step is to consider how to provide effective protection to the data. In the ICT age where technologies are rapidly evolving, attempts to set out precise rules and procedures for data users to follow may be futile[39]. An approach that is static and reactive will not help us meet the goal of achieving regulatory effectiveness. Instead, we must take on an approach that embraces "contingency, flexibility and openness to the new[40]" to effectively tackle new regulatory challenges as they emerge. Facing waves of ever-evolving technologies, a shift from rules to long-standing principles[41] will create a strong bulwark of privacy protection.

Accountability is a comprehensive, flexible and responsibility-based framework that encapsulates these long-standing principles. It is the solution that guards against new privacy challenges in today's data-driven economy.

Accountability is a comprehensive paradigm requiring data users or processors to put in place *appropriate steps* to safeguard personal data, and prevent harms to data subjects. It embodies a variety of built-in policies, procedures, controls, oversights and review mechanisms to lock in privacy protection across the whole lifecycle of data processing. Practicable steps to give effect to accountability include appointment of data protection officers, conducting privacy impact assessments and implementing privacy by design. Data users can flexibly take a risk-based approach and adopt measures proportionate to the possibility and severity of privacy harms. Under the accountability principle, data users take on responsibility for data protection, and will be held liable if insufficient safeguards are put in place to prevent privacy harms.

(1) Accountability

Accountability is not novel to our data protection community. It has been recognised in various data protection guidelines and legislation and advocated by data protection authorities. Accountability found its way into some of the earliest

[39] Fenwick, M., Kaal, W.A., & Vermeulen, E.P.M. (2016). Regulation Tomorrow: What Happens When Technology is Faster than the Law? *American University Business Law Review, 6(3),* 561-594.
[40] Fenwick, M., Kaal, W.A., & Vermeulen, E.P.M. (2016). Regulation Tomorrow: What Happens When Technology is Faster than the Law? *American University Business Law Review, 6(3),* 561-594.
[41] Fenwick, M., Kaal, W.A., & Vermeulen, E.P.M. (2016). Regulation Tomorrow: What Happens When Technology is Faster than the Law? *American University Business Law Review, 6(3),* 561-594.

data protection instruments, including the 1980 OECD Privacy Framework[42](revised in 2013) and the EU Data Protection Directive 95/46/EC[43], which require data users to adopt measures to ensure privacy principles are complied with. The APEC Privacy Framework 2005[44] enriches accountability with "Preventing Harm" principle[45], which requires data users to engineer personal data protection in such a way as to prevent data misuse, and follow a risk-based approach to adopt preventive and remedial measures proportionate to the possibility and severity of privacy harms.

Accountability is also depicted in detail in the EU GDPR through various requirements. For example, data controllers are required to implement technical and organisational measures to ensure compliance [Article 24], adopt data protection by design and by default [Article 25], conduct data protection impact assessment for high-risk processing [Article 35] and (for certain types of organisations) designate Data Protection Officers [Article 37]. In Hong Kong, although accountability is not explicitly mentioned in the PDPO, the PCPD encourages organisations to implement Privacy Management Programme to make a shift from compliance to accountability and adopt privacy by design. In 2014, the PCPD issued "Privacy Management Programme: A Best Practice Guide[46]" to assist data users to design and implement Privacy Management Programmes within organisations.

From data protection authorities' viewpoint, accountability translates high-level legal principles into concrete mechanisms for implementation to ensure privacy protection[47]. By requiring data users to take appropriate steps to safeguarding

[42] The 1980 OECD Guidelines brings in the Accountability Principle, which states that a data user should be accountable for complying with measures which give effect to the various privacy principles. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[43] Under Article 6(2) of the *1995 Data Protection Directive*, it shall be for the data user to ensure that various privacy principles is complied with. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[44] Centre for Information Policy Leadership. (Oct 2009). *Data Protection Accountability: The Essential Elements – A Document for Discussion*. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_protection_accountability-the_essential_elements__discussion_document_october_2009_.pdf

[45] Principle I of APEC Information Privacy Principles in APEC Privacy Framework. Please refer to: APEC. (2005). *APEC Privacy Framework*. https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

[46] The PCPD. (Feb 2014). *Privacy Management Programme: A Best Practice Guide*. Retrieved from https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf

[47] Article 29 Data Protection Working Party. (2010, July 13). *Opinion 3/2010 on the principle of accountability*. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

privacy, accountability bridges the gap between high-level principles and the modus operandi. Only data users themselves would know how they are going to process personal data, and, after conducting proper privacy impact assessment, determine the risks to individuals' rights and interests as a result of the processing. This puts the data users in the best position to determine the *appropriate steps* to mitigate the risks. It may well be counterproductive for regulators to set out the precise rules and procedures for the data users to follow.

Accountability offers effective protection as it views privacy protection not as an afterthought but a preventive measure, so that privacy harms can be nipped in the bud. As more data users shoulder their responsibilities and conduct reviews of their privacy practices, they will become, in the long run, more privacy aware and privacy friendly, in addition to compliant with legal requirements. Data protection authorities can then divert their limited resources to areas which require their attention.

While accountability takes on the fundamental ideal that data users should shoulder the bulk of responsibilities, it does not solely work to the advantage of data protection authorities. From organisations' viewpoint, accountability assists them to be compliant with privacy laws, and saves them expenses from remedying the aftermaths of privacy excursions at a later stage[48]. Accountability also helps businesses earn trust of customers and build up their reputation in the long run. As organisations garner more trust, they can drum up businesses from customers[49]. Organisations' investment in privacy is an investment in brands, because it shows clients that they are concerned with things that concern the customers, and in turn helps them generate businesses[50]. As UK's Information Commissioner Ms Elizabeth Denham rightly puts it, accountability helps organisations garner people's trust and "having customers' trust [is] a cornerstone to good business[51]". Notably, earning trust from customers will ultimately help organisations win the "holy grail", their data. As organisations become more privacy-focused and invest in enhancing transparency, user control and accessibility over their data, users will

[48] Office of the Privacy Commissioner of Canada. (2012, Apr 17). *Getting Accountability Right with a Privacy Management Program*. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/

[49] Gensler, Arthur. (2015, Jul 28). Trust is the most powerful currency in business. *Fortune*. Retrieved from http://fortune.com/2015/07/28/trust-business-leadership/

[50] Goldberg, I. (2001). Trust, Ethics and Privacy. *Boston University Law Review, 81(2)*, 407-422.

[51] UK ICO. (2017, Jan 17). GDPR and Accountability – Speech delivered by Ms Elizabeth Denham at a lecture for the Institute of Chartered Accountants in England and Wales in London [News and blogs]. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/

be more willing to share their data with organisations. Organisations can then tap into the vast ocean of data for innovative use and developments.

From the foregoing, accountability represents a perfect balance between seemingly irreconcilable interests of personal data protection and innovative use of data in data-driven economies. It helps data protection regulators realise abstract privacy principles, and allows businesses to make innovative uses of data so long as they use data responsibly, minimise risks and prevent harms to data subjects.

(2) Mechanics of Accountability

The core ideal of accountability is that data users should shoulder a larger share of responsibilities. However, why should data users (as opposed to data subjects) shoulder this responsibility? A justification is fairness - it is only fair that organisations are prepared to share the wealth created by the processing of personal data with individuals whose data they process by giving them greater control over their own data[52]. Data users wishing to tap into the enormous value of data should be prepared to take care of the negative consequences and externalities. At this juncture, it should be noted that accountability allows organisations to garner the greatest benefit (earn customers' trust) at a minimum cost.

Regulation always starts with enforcement. What is the appropriate enforcement model for accountability? We observe that mandatory accountability in privacy laws backed by punitive consequences best commands compliance and strengthens protection. Compared to voluntary and self-regulatory models, a mandatory model is more feasible and effective.

In pushing accountability forward, data protection regulators may need to place increased efforts in educating citizens to help them realise their privacy rights and train them to be privacy aware in selecting goods and services. This in turn helps to create a momentum and incentive for businesses to engineer privacy through accountability and provide more accountability-based goods and services.

The EU GDPR expressly incorporates the accountability principle as a major part of the revised European regulatory framework. Organisations/businesses are required to demonstrate their compliance with the principles of processing of

[52] European Data Protection Supervisor. (Nov 2015). *Opinion 7/2015 - Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability*. Retrieved from https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

personal data; implement appropriate technical and organisational measures to ensure compliance and integrate data protection into their processing activities[53].

(3) Data Ethics and Trust

It is no exaggeration to say that nowadays "smart" technologies such as the Internet of Things, big data analytics, AI and machine learning fuel the engine of the digital economy. While they make consumers' lives easier, consumers provide their data to make them work better. As consumers disclose to data users or controllers all their sensitive data, data users or controllers are expected not to betray consumers' trust. Herein, accountability involves taking proactive and preventive measures to ensure privacy protection and legal compliance.

Data security is the first and foremost concern when it comes to data protection and accountability. It is a necessary condition in protecting personal data privacy. There is no privacy without data security. Nonetheless, privacy protection is more than data security alone, and data users or controllers owe an ethical obligation to protect individuals' personal data. Data users or controllers need to pay attention to the reasonable expectations, rights, interests and freedoms of the individuals concerned when processing personal data. They are urged to embrace two principles, namely (i) no surprise to consumers and (ii) no harm to consumers.

Consumers who have trust and confidence in a company are more ready and willing to share their data with the company, generating positive feedback to the digital ecosystem and reinforcing the symbiotic relationship between individual consumers and the "smart" technologies.

As consumers' privacy awareness and expectation increases, and ICT development expedites, the attitude of data users and processors should correspondingly be changed. On top of fair enforcement and regulating, regulators should work together with organisations, public and private data users or controllers and processors included, for a better and safer digital ecosystem in this age of data.

[53] Articles 5, 24 and 25 of the GDPR

Concluding Remarks

Revolutionary and innovative developments in ICT like big data analytics, AI and Fintech present challenges to the regulatory strengths and effectiveness of existing data protection laws. These developments set forth races by data protection regulators to come up with novel regulatory solutions, including expansion of the scope of data protection laws.

In face of rapid technological developments threatening to annihilate robust law amendments efforts, it is suggested that regulators explore the possibility of accountability as the solution. Comprehensive, flexible and responsibility-based, accountability is the crucial framework to strike a balance between data protection and facilitation of businesses and innovation.

Regulatory framework aside, regulators should consider engaging and incentivising organisations/businesses in cultivating/strengthening the privacy culture, particularly in Asia, by facilitating them in building trust and reputation, observing ethical standards and respecting data of their customers and consumers.