12-2018

Protecting consumers' personal data in the digital world: Challenges and changes

Man YIP
Singapore Management University, School of Law, manyip@smu.edu.sg

PROTECTING CONSUMERS' PERSONAL DATA IN THE DIGITAL WORLD – CHALLENGES AND CHANGES*

YIP Man†
LLB (Hons) (National University of Singapore), BCL (Oxford); Advocate and Solicitor (Singapore)

I. Introduction

1 At the Personal Data Protection Seminar 2017, Dr Yaacob Ibrahim, Minister for Communications and Information, said that Singapore must "aspire towards a high standard of data protection that strengthens trust with the public, gives confidence to customers whose data is collected and used, while providing an environment for companies to thrive in the digital economy".[1] In his speech, he acknowledged that the Personal Data Protection Act 2012[2] ("PDPA") was crafted in an era where the majority of the data were derived from physical or online form filling exercises. The age we are in, however, is where data are being constantly generated and mined through transactions and activities on the Internet and other forms of technology.[3] The digital economy is built on the model of *efficient data sharing*. Dr Yaacob Ibrahim thus calls for a change in data protection mindset and culture: to move from compliance to accountability.

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of her employer. All errors remain the author's own.

† Associate Professor of Law, School of Law, Singapore Management University. Yip Man is the Deputy Director of the Centre for Cross-Border Commercial Law in Asia, the Asia Pacific Digest Editor for the *Restitution Law Review* and a co-Administrator of the Singapore Law Blog. She previously served as a member of the Singapore Academy of Law Law Reform Committee.

1 Dr Yaacob Ibrahim, Minister for Communications and Information, "From Compliance to Accountability: A Robust and Progressive Data Protection Framework" Personal Data Protection Seminar 2017 (27 July 2017) <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2017/7/personal-data-protection-seminar-2017> (accessed on 11 January 2018).

2 Act 26 of 2012.

3 For example, the facial recognition technology.

Businesses are to play an active role, in partnership with the Personal Data Protection Commission ("PDPC"), in protecting their customers' data. The focus shifts from regulator to data controller.

2 Thus far, the PDPC is taking swift action to help build and strengthen industry accountability in respect of the harvest, use and transfer of consumer data.[4] The emphasis of the proposed approach[5] is in part targeted at businesses' obligations (data breach mandatory notification) and business accountability under an enhanced framework for the collection, use and disclosure of personal data[6] (for example, conducting a risk and impact assessment). Indeed, the mandatory obligation to notify of data breach is part of enforcing greater business accountability. Elsewhere, in Europe and the US, legislative proposals have adopted a different strategy by placing control in data subjects (*ie*, consumers). These are crucial, though initial, steps to kickstarting the change in the mindset and culture of data protection.

4 "Data Privacy Laws Changing in Tune with Digital Economy" *The Straits Times* (28 July 2017).

5 See Personal Data Protection Commission, "Public Consultation for Approaches to Managing Personal Data in the Digital Economy" (27 July 2017) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/publicconsultationapproachestomanagingpersonaldatainthedigitaleconomy270717f95e65c8844062038829ff000.pdf> (accessed 17 March 2018); Personal Data Protection Commission, "Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in Digital Economy" (1 February 2018) <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-Managing-Personal-Data-in-the-Dig.pdf> (accessed 17 March 2018).

6 The enhanced framework allows for the collection, use and disclosure of personal data (a) through deemed consent by notification of purpose or (b) without consent on the basis of "legitimate interests".

3 This article discusses challenges that require us to rethink the present regulatory approach and explores what more can be done in the future. The starting point is a clear acknowledgment of two facts:[7] data are the bloodline of the digital economy; and data processing by businesses or data sharing between businesses may be beneficial to consumers. An unduly restrictive approach would stifle innovation and undermine the value which the appropriate and legitimate use of data could bring to society. This article argues that we should adopt a multi-pronged, balanced approach of placing responsibility on the regulator, businesses as well as the consumers themselves for consumer data protection.

II. Challenges

4 To skillfully navigate the challenges posed by the digital world, we must first understand what these challenges are.[8] As a starting point, there are four obvious challenges in respect of regulating the protection of consumers' data in the digital marketplace. The first challenge is the difficulty of using consent as an effective means of authorising the collection and use of data in the digital world. One constraint is the inefficiency from having to obtain consent constantly. It has been pointed out that "an overemphasis of autonomous authorisation" will lead to an overload of consent transactions[9] with the consequence that consumers suffer from "consent fatigue" and "consent desensitisation", rendering consent an ineffective authorisation mechanism.[10] Indeed, the PDPA does not overemphasise the role of consent in data protection.[11] The PDPC's proposed reform of introducing "Notification of Purpose", in the absence

7 The UK government has acknowledged these two facts in mapping out its strategy for "unlocking the power of data in the UK economy and improving public confidence in its use". See *UK Digital Strategy 2017* (1 March 2017) section 7 <https://www.gov.uk/government/publications/uk-digital-strategy> (accessed 17 March 2018).

8 Undoubtedly, new challenges will continue to arise.

9 This problem is particularly acute in the context of Internet activities.

10 B W Shermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171 at 176–179.

11 See Yip Man, "Personal Data Protection Act 2012: Understanding the Consent Obligation" [2017] PDP Digest 266.

of obtaining consent, as an appropriate basis for data collection, use or disclosure acknowledges that in some circumstances it may be impractical to obtain consent.[12] The other problem with over-reliance on consent is related to technological advancement. As Hermstrüwer explains, the individualistic conception of privacy "misses a crucial feature of modern data analytics (Big Data) and the behavioral forces underlying the diffusion of personal information in networked environments". That is, in a networked environment, it is possible to predict, on the basis of probabilities, the traits of users, who did not disclose their personal information, based on the personal information disclosed by these individuals' friends in the same environment by running a simple logistic regression based on certain parameters.[13] A further technological challenge to obtaining consent is the design of the technological device itself: people frequently conduct transactions over their mobile phones and the size of the screen poses a significant challenge for obtaining meaningful consent. Moreover, it is well established that the readership of terms and conditions for online consumer contracting is very low.[14] The consumer may thus

12 See Personal Data Protection Commission, "Public Consultation for Approaches to Managing Personal Data in the Digital Economy" (27 July 2017) at para 3.8.

13 Yoan Hermstrüwer, "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data" (2017) 8 *Journal of Intellectual Property, Information Technology and Electric Commerce Law* 9 at 12–13. The more information disclosed by the friends, the higher the probability of determining the personal information relating to the users who did not consent to the disclosure. See also, UK Government Office for Science, "Artificial Intelligence: Opportunities and Implications for the Future of Decision Making" (9 November 2016) at p 14 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/566075/gs-16-19-artificial-intelligence-ai-report.pdf> (accessed 17 March 2018).

14 European Commission, "Study on Consumers' Attitude Towards Terms and Conditions (T&Cs): Final Report" (Brussels 2016) at p 9 <http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/terms_and_conditions_final_report_en.pdf> (accessed 17 March 2018); Yannis Bakos, Florencia Marotta-Wurgler & David R Trossen, "Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts" (2014) 43 *Journal of Legal Studies* 1.

blindly or without consideration accept unfair or onerous terms on the processing and use of their data.[15]

5 Second, online business strategies, prompted by technological developments, may make it harder for consumers to realise that their personal data are being harvested, stored and/or used. In particular, many online "free" services are not provided by businesses free of charge but are in exchange for the consumer's disclosure of personal data. These businesses' main source of revenue is advertising; and consumers' data could help them improve and enhance their advertising strategies (for example, customer churn prediction, targeted advertising or interest-based advertising) for companies who sought the advertising service. Facebook, Google and Instagram are notable examples of businesses that operate on such a model. Yet, there is real concern that consumers are unaware of how their data will be used by the businesses.

6 Thirdly, business models are also evolving rapidly. Buzz terms like "sharing" economy,[16] collaborative economy, collaborative consumption and on-demand services[17] are emblematic of the change that is swiftly taking place. Singapore's attitude is to embrace such innovations and the associated technologies. Liu Feng-Yuan, Director of the Government Technology Agency of Singapore's Data Science Division, said: "From a public good point of view, we're really keen on encouraging these technologies. The sharing economy is about better utilisation, better sharing

15 Stephanie Law, "At the Cross-roads of Consumer Protection, Data Protection and Private International Law: Some Remarks on *Verein fur Konsumenteninformation v Amazon EU*" (2017) 45 *European Law Review* 751 at 765.

16 See generally Lisa Gansky, "How the Sharing Economy Can Create Value from Waste" *Huffington Post* (11 October 2015) <https://www.huffingtonpost.com/lisa-gansky/sharing-economy-value-waste_b_8522490.html> (accessed 17 March 2018).

17 For definitions, see Rachel Botsman, "Defining the Sharing Economy: What is Collaborative Consumpion – And What Isn't?" (27 May 2015) <https://www.fastcompany.com/3046119/defining-the-sharing-economy-what-is-collaborative-consumption-and-what-isnt> (accessed 17 March 2018).

and better services for the people."[18] However, such business models raise data protection concerns as the companies which own these platforms are in possession of large volumes of personal data of the users.

7 Finally, there is an acceleration of concentration of power over data in the hands of corporate giants,[19] such as Amazon, Apple, Facebook and Google. Facebook has been embroiled in online privacy controversies since its takeover of WhatsApp in 2014. It has been fined €110m by the European Commission for providing incorrect or misleading information[20] on the possibility of data sharing between Facebook and WhatsApp.[21] It has also come under investigations and scrutiny by several national data protection and/or competition authorities in the European Union ("EU").[22] Further, it has been observed that five companies – Alphabet, Amazon, Apple, Facebook and Microsoft – have dominant control, through acquisitions of startups, over the talent and intellectual property behind the emerging field of artificial intelligence ("AI") and machine learning.[23] One concern is that these companies "sit on vast stores of user data that are

18 "The Sharing Economy of Data" (30 June 2017) <https://www.tech.gov.sg/TechNews/Innovation/2017/06/The-sharing-economy-of-Data> (accessed 17 March 2018).

19 See generally Giovanni Buttarelli, "Strange Bedfellows: Data Protection, Privacy and Competition" (2017) 13 *Competition Law International* 21 at 22–23.

20 See European Commission Press Release, "Mergers: Commission Alleges Facebook Provided Misleading Information about WhatsApp Takeover" (Brussels, 20 December 2016) <http://europa.eu/rapid/press-release_IP-16-4473_en.htm> (accessed 17 March 2018).

21 See news report by CNBC: <https://www.cnbc.com/2017/05/18/facebook-fine-eu-whatsapp-takeover.html> (accessed 17 March 2018).

22 See, for example: <https://www.theguardian.com/technology/2017/dec/19/facebook-use-of-third-party-apps-violates-data-protection-principles> (Germany); <https://www.theguardian.com/technology/2017/dec/19/france-orders-whatsapp-stop-sharing-user-data-facebook-without-consent> (France); and <https://www.bloomberg.com/news/articles/2017-10-12/facebook-is-watching-you-belgian-privacy-agency-warns-in-court> (Belgium) (accessed 17 March 2018).

23 Vinod Iyengar, "Why AI Consolidation Will Create the Worst Monopoly in US History" (24 August 2016) <https://techcrunch.com/2016/08/24/why-ai-consolidation-will-create-the-worst-monopoly-in-us-history/> (accessed 17 March 2018).

rivaled only by governments".[24] The trend of such power concentration in large private companies sets off alarm bells on the transparency of these companies' activities, in particular, how regulators could effectively monitor their collection, use and transfer of personal data. Transformative technological advancements such as AI and machine learning – which enable automated decision-making – could easily outstrip the pace of regulatory reform, thereby exacerbating the problem. Regulatory response is reactionary. As Commissioner Pamela Jones Harbour put it in her dissenting statement in respect of Google's acquisition of DoubleClick:[25]

> The truth is, we really do not know what Google/DoubleClick can or will do with its trove of information about consumers' Internet habits. The merger creates a firm with vast knowledge of consumer preferences, subject to very little accountability. [reference omitted]

8 The market monopoly trend also signals the need for competition regulators to assess economic activities with consumer protection and data protection angles in mind. As such, collaboration amongst these three authorities would be sensible.

III. New regulatory philosophy: Enabling individual control, shared responsibility and enhancing trust

A. EU General Data Protection Regulation

9 Against these challenges highlighted above and other challenges that are associated with the digital environment, a new regulatory philosophy begins to emerge. This is evident in the new regime set out in the EU's General Data Protection Regulation ("GDPR"). The GDPR, which will replace 28 local laws in the EU Member States, will take effect in May

---

24 Vinod Iyengar, "Why AI Consolidation Will Create the Worst Monopoly in US History" (24 August 2016) <https://techcrunch.com/2016/08/24/why-ai-consolidation-will-create-the-worst-monopoly-in-us-history/> (accessed 17 March 2018).

25 Dissenting judgment of Commissioner Pamela Jones Harbour in *In the matter of Google/DoubleClick* (FTC File No 071-0170) at p 10 <https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf> (accessed 17 March 2018).

2018. The GDPR is marked by a number of key changes.[26] Five changes – relevant to the present discussion – will be highlighted. First, it increases the territorial scope of application, covering all businesses (whether situated within or outside of the EU)[27] which process the personal data of data subjects residing in the EU. Second, higher penalties are imposed on breaches of the rules, with the maximum fine being 4% of a company's total global turnover. Third, the new regime enhances the role of consent by strengthening the conditions for obtaining consent from data subjects.[28] Article 12 of the GDPR obliges the companies to provide information to users "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". Fourth, the GDPR prescribes a broad range of rights for data subjects,[29] including the right to rectification and erasure, right to restrict processing, right to data access and right to data portability. Fifth, the GDPR shifts the responsibility of personal data protection on data controllers and processors[30] by prescribing a number of obligations, including mandatory data breach notification, the requirement to design systems with data protection from the outset and the obligation to put in place data protection officers.

10 The GDPR has received mixed reviews, with some considering it to be overly heavy-handed, thereby increasing the costs of compliance for businesses[31] – a consequence that would be most severely felt by smaller

26 For a summary, see <https://www.eugdpr.org/key-changes.html> (accessed 17 March 2018).

27 For a summary of key aspects of the legislation, see <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/eu-gdpr-factsheet--041017.pdf> (accessed 17 March 2018).

28 *Cf* Yoan Hermstrüwer, "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data" (2017) 8 *Journal of Intellectual Property, Information Technology and Electric Commerce Law* 9 at 17. Hermstrüwer argues that the transparency obligation does not sufficiently address the information asymmetries between companies and customers and it is inconsistent with the requirement regarding the kind and quantity of information that must be made available to customers under Art 14 of the European Union General Data Protection Regulation.

29 European Union General Data Protection Regulation Ch 3.

30 European Union General Data Protection Regulation Ch 4.

31 "Data Protection: Brussels' Heavy Hand on Europe's Digital Economy" *Financial Times* (22 November 2017).

businesses. The discussion here is not focused on the shortcomings of the new regime. Rather, what is not to be missed is the regulatory shift towards enabling the data subjects to control the use of their data through the provision of a range of rights and putting heavier responsibility on data controllers/processors through the provision of a range of obligations. Importantly, these obligations on controllers/processors systematically require these actors to integrate data protection into their business models. As such, the emerging regulatory picture is one of shared responsibility between the regulator, the controller/processor and the data subject (*ie*, the consumers).

B. US Consumer Privacy Bill of Rights

11 The Obama administration put forward the Consumer Privacy Bill of Rights in 2012 to improve privacy protection for consumers; the same was reintroduced again in 2015.[32] The Consumer Privacy Bill of Rights 2012 provides blueprint guidance on enhancing online privacy protection, setting out seven basic "rights": "(1) individual control; (2) transparency; (3) respect for context; (4) security; (5) access and accuracy; (6) focused collection; and (7) accountability".[33]

12 The intentional paradigm shift that was made in the Consumer Privacy Bill of Rights was the emphasis on the consumers' rights.[34] In particular, the right to individual control has two core aspects: "'providing customers with easily used and accessible mechanisms' with which to exercise control and two, 'consumer responsibility', which recognises that the use of personal data turn upon the individual's decision to share data with others".[35] Commentators have thus said that this amounts to enabling

32 See <https://www.whitecase.com/publications/article/white-house-re-introduces-consumer-privacy-bill-rights-act> (accessed 17 March 2018).

33 Hakeem Rizk, "Fundamental Right or Liberty: Online Privacy's Theory for Co-Existence with Social Media" (2013) 56 *Howard Law Journal* 951.

34 "Why a Push for Online Privacy is Bogged Down in Washington" *New York Times* (28 February 2016). See also George Jepsen, "Big Data and Insurance Symposium" (2014) 21 *Connecticut Insurance Law Journal* 255 at 258–259.

35 Andy Crabtree *et al*, "Enabling the New Economic Actor: Data Protection, the Digital Economy and the Databox" (2016) 20 *Pers Ubiquit Comput* 947 at 950.

a new economic actor, the data subject, in the data protection process, an aspect that is also evident in the EU approach discussed above.[36]

13 The Consumer Privacy Bill of Rights further proposed a more vigorous participation scheme in the form of a "parallel self-regulatory process".[37] This self-regulatory process, operating under the Commerce Department, was to involve both businesses and consumer groups working together to "devise voluntary privacy practices for mobile apps, drones and other technologies".[38] This proposal clearly recognised the need for shared responsibility in data protection and to better facilitate the consumers' voice to be heard in the process.

C. *Building trust*

14 Societal attitudes towards data sharing are also changing. People are becoming more accepting towards the practice of disclosing personal information in exchange for services or before making purchases online.[39] The most important factor for consumers' willingness to share personal data is their trust in the business. As such, a regulatory approach that focuses on business accountability and requiring businesses to build data protection into their business design is a step in the right direction. Beyond legal requirements, in the light of survey findings, businesses should be incentivised to take further action to build the customers' trust in their data protection practices. As such, self-regulation by businesses may be the most timeous and effective solution to some of the challenges arising in the age of big data and the digital economy.

---

36 Andy Crabtree *et al*, "Enabling the New Economic Actor: Data Protection, the Digital Economy and the Databox" (2016) 20 *Pers Ubiquit Comput* 947 at 950.

37 "Why a Push for Online Privacy is Bogged Down in Washington" *New York Times* (28 February 2016).

38 "Why a Push for Online Privacy is Bogged Down in Washington" *New York Times* (28 February 2016).

39 "What Marketers Need to Know About Consumers' Attitudes to Sharing Data" *The Guardian* (9 July 2015). See also <https://www8.gsb.columbia.edu/newsroom/newsn/3850/study-shows-that-consumers-are-willing-to-share-personal-data-if-the-benefits-and-brand-are-right> (accessed 17 March 2018).

VI. Going forward: Other concerns

15 The discussion above has highlighted the main challenges to data protection brought about by the digital world and technological advancements. It has also analysed the rise of a new regulatory philosophy that is built upon the core concepts of consumer control, shared responsibility and trust. Of course, these core concepts could be implemented in practice in various ways, and not necessarily all efforts are to be undertaken by the PDPC alone. For example, industry can play a more active role in the development of sector-specific data protection requirements or coming together to formulate core responsible corporate practices. Indeed, many businesses have overseas operations and are thus confronted with the issue of having to meet the privacy regulatory requirements of different jurisdictions. Whether companies should adopt a fragmented corporate response for each jurisdiction or a uniform, multi-jurisdictional corporate response is a matter that is best left to businesses to decide. In this regard, major industry players can take on a thought leadership role.[40] It may also be that parallel/facilitative processes could be set up by related agencies, for example, establishing an awards scheme to recognise businesses that innovate data protection practices.[41] This scheme would not only reward businesses and help them in building greater public confidence, it would also foster a local culture of self-regulation and industry-driven code of good practices.

16 Further, going forward, there are other concerns to address. First, attention must be paid to the international dimension of data protection. The Internet and other technologies have made it easy to carry out cross-border transfers or processing of personal data. National legislation alone would not be sufficient to combat abusive use or processing of data. Regional co-operation and consensus would be necessary.[42] In this regard,

40 See Advertorial: "Personal Data Protection: An Intrinsic Priority of Singapore's Largest Bank" *Business Tmes* (9 January 2017).

41 The Personal Data Protection Commission has announced plans to introduce the Data Protection Trustmark Certification Scheme by end 2018. See <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Press-Room/2017/pdps2017-media-release---(260717).pdf> (accessed 17 March 2018).

42 See "Consumer Protection in E-commerce: OECD Recommendation" (2016) at para 54 <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf> (accessed 17 March 2018).

Singapore has recently become[43] a member of both the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules System[44] and the APEC Privacy Recognition for Processors System.[45] Other steps could include building a collaboration network amongst the national data protection agencies in the region to share, within legal limits, information and experiences.

17 Second, greater co-operation and communication between competition, data protection and consumer protection agencies can be fostered. This ensures that policies would be devised with a more holistic perspective on the impact and implication of certain economic activities.

18 Third, there is a need to focus on developing effective dispute resolution rules and mechanisms for e-commerce consumers in domestic and international disputes. Special attention should be paid to rules on jurisdiction, choice of law and rules to determine if jurisdiction clauses and choice of law clauses are unfair to the consumer who has no opportunity or ability to negotiate these terms. These rules have an impact on the level of data protection for the consumers. Further, dispute resolution mechanisms for e-commerce consumers should be effective, efficient, user-friendly, transparent and cost-friendly.[46] Singapore, as the incumbent Chair of the Association of Southeast Asian Nations ("ASEAN") for 2018, could leverage on the ASEAN infrastructure to push forward the agenda as well as enhance regional co-operation. In this connection, it is noteworthy that the ASEAN Economic Community Blueprint 2025 considers the need to devise correlated strategic measures relating to the rise of e-commerce, in particular, measures targeted at consumer protection, online dispute

43 See the Personal Data Protection Commission's announcement on 6 March 2018 <https://www.pdpc.gov.sg/pdpc/news/press-room/2018/03/singapore-joins-apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems> (accessed 17 March 2018).

44 Singapore is the sixth member. Other members are Canada, Japan, Korea, Mexico and the US.

45 Singapore is the second member, after the US.

46 See "Consumer Protection in E-commerce: OECD Recommendation" (2016) at paras 43–45 <https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf> (accessed 17 March 2018).

resolution for e-commerce and personal data protection.[47] Moreover, Singapore's priority focus for 2018 as ASEAN chair is improving ASEAN economic connectivity through the digital economy.[48]

19 Finally, Singapore should promote more focused research on data science, behavioural science on decision-making of consumers as well as sociological empirical research on consumer attitudes. These research studies would greatly aid regulators in deciding the best regulatory and non-regulatory responses to new challenges in the digital world.

VII. Conclusion

20 The rapid rise of digital economy has brought both benefits and challenges. It is important to recognise what these challenges are. It is equally important to embrace necessary changes to respond to the challenges. Whilst the PDPA has laid down the baseline framework for personal data protection, we are clearly in the next phase of regulatory challenge and innovation.

21 In *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight*, the authors said:[49]

> Data was no longer regarded as static or stale, whose usefulness was finished once the purpose for which it was collected was achieved … Rather, data became a raw material of business, a vital economic input, used to create a new form of economic value. In fact, with the right mindset, data can be cleverly reused to become a fountain of innovation and new services. The data can reveal secrets to those with the humility, the willingness, and the tools to listen.

22 This article points out that we need to embrace a new mindset in effectively handling the challenges generated by the age of big data and the digital economy. The responsibility of enabling data to become "a fountain

---

47 ASEAN Economic Community Blueprint 2025 at para 53 <http://www.asean.org/storage/images/2015/November/aec-page/AEC-Blueprint-2025-FINAL.pdf> (accessed 17 March 2018).

48 "Singapore to Focus on Digital Economy, Trade Facilitation as ASEAN Chair in 2018" *Business Times* (12 September 2017).

49 Victor Mayer-Schonberger & Kenneth Cukier, *Big Data: The Essential Guide to Work, Life and Learning in the Age of Insight* (John Murray, 2017) at p 5.

of innovation and new services" is to be shared between the regulator, the businesses and the consumers. Everyone must participate to derive the maximum benefits promised by the new economy.