A response to:

PUBLIC CONSULTATION FOR APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

Issued 27 July 2017

By the Noggin Asia and HAT Community Foundation Asia

Noggin Asia

Chua Lai Chwang
laichwang@nogginasia.com

71 Ayer Rajah Crescent #3–11
Singapore 139951

nogginasia.com

Tel: +65 6836 4655

HAT Community Foundation Asia
(HCF Asia)

Jonathan Holtby
contact@hatcommunity.org

hatcommunity.org

HAT Community Foundation Asia is a sub group of the HAT Community Foundation Ltd (1st Floor, 160-164, Gray's Inn Road, WC1X 8ED), UK

Introduction

This document is a response to the Personal Data Protection Commission Singapore (PDPC)'s Public Consultation for Approaches to Managing Personal Data in the Digital Economy (PDPC, 2017).

This document provides collective views from the leading respondents (Noggin Asia and HCF Asia), on PDPC's proposal on Notification of Purpose and Legal or Business Purpose approaches as parallel bases for collecting, using and disclosing personal data, and the proposed mandatory data breach notification regime under The Personal Data Protection Act 2012 (PDPA) (PDPC, 2017).

A total of 19 individuals are part of this response. See the name list at the end of this document.

Q1: Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?

Much of the future of the regulatory framework for the protection of individuals' data in our society will be hinged upon granting that individual rights to information, rather than requiring action from the individual to assert and acquire such rights. While we acknowledge the costs and friction in the market caused by granting such rights, we consider such rights to be fundamental and important.

It is desirable that in a regulatory framework, the citizen is given the right to be informed about the use of their data, the right to be given access to it where it rests, the right to rectify its inaccuracy or incompletion, the right to erase it should they so desire, the right to restrict its processing, the right to its portability in their service, the right to object to its misuse, and the right to protect themselves against automated decision-making and profiling. As a point of reference, such rights are granted in Europe under the General Data Protection Regulation (GDPR) (EC, 2017) (ICO, 2017). As a developed nation that have made great strides in governance and citizenry, should we not expect no less in terms of our fundamental data rights. We believe that such rights of individual are also critical in steering and shaping the new data economy, and in keeping an organization's data ethics as part of her corporate social responsibilities. Why should not Singapore uphold individual rights to data with moral authority and trust? Doing so will put us in good stead as a digital leader in the advancement of a Smart Nation/City in Asia.

With such considerations in mind, we propose that any provision of Notification of Purpose as a basis for the collection, use, and disclosure of personal data without consent would require that the rights of the individual are protected. It should not be possible for the organisation to withdraw behind Notification of Purpose to obviate their need to obtain consent. It is also important that both legislation and compliance should always consider the rights of individuals as a fundamental axiom, before considering the costs and efficiencies of organisations.

The current proposal suggests mandating NoP, but opens to manipulation to waive the need for consent in practice. We believe this is a slippery slope, both in terms of legislation, as well as compliance. As such, while we agree with the NoP intention, we suggest a further mandatory

consent for any collection, use and disclosure of personal data unless under very strict circumstances (e.g. in case of medical emergencies). For normal cases, we believe there are innovative and available technological and design solutions for organisations to employ to achieve compliance, and to ensure such rights are upheld.

We suggest that PDPC should encourage the use of innovative solutions to mandate getting user consent prior to any change of existing data collection, processing, and use. We suggest providing notification for users' new consent on such matters, and enabling access and updates to personal information. While we acknowledge that consent fatigue may occur, we fundamentally believe this can be solved by the market; services that are more innovative in ensuring consent is given will prevail.

Q2: Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)?

While we recognise the challenges indicated by the PDPA in obtaining individuals' consent, we wish to stress two important arguments. Firstly, it is the duty of the state (with PDPC as proxy for personal data) to uphold the rights of individuals and to ensure such rights are upheld without exemptions, otherwise there is a wider ramification that could lead to an erosion of trust. Secondly, should there be any exemption given, PDPC, together with other legislation and legal organisations, should explicitly defined such exemptions. Any ambiguity of interpretation and market gamification of the rules could lead to consequences that would result in an erosion of trust in the PDPC. Hence, we propose that:

1. It ought to be a legal requirement for every organisation to seek consent for the collection and use of personal data in every instance, and for PDPC to be the compliance body to enforce this. There should be no ambiguity on conditions for exemption.
2. Technological advances have shown that responsible data management is possible and there are innovative solutions to obtain consent, if the organisation bothers with the giving of consent as part of its user experience design. It is of course expected of organisations to lobby and present the challenges in achieving this, as they would prefer the legislation to not exist, since it is costly. PDPC has the duty to decide, on the balance of issues, if individual rights are important enough to ensure compliance. We believe it is.
3. Finally, the economic argument at a macro level does not justify relaxation of consent-giving. Given there are solutions for consent fatigue, organisations that are more innovative and better at obtaining consent would prevail. This would make Singapore organisations better in first world services that uphold individual rights.

Based on our arguments, we therefore consider clause 3.9 too forgiving in allowing organisations to use the NoP mechanism without prescriptions or consent. We only see rarely existed extreme exemption cases where NoP could be used without consent. However, we see exceptions as a big risk for PDPC itself, as the body with the trust of citizens.

In the extreme cases where consent absolutely cannot be obtained, we suggest that the organisation follows statutes protecting the rights of individuals to be informed, to access, to

rectify, to erase, to restrict, to transport, and to object to their data's misuse. In such cases, the market would also prevail. Organisations can be self regulated to ensure they comply with consent and use of personal data if there is a fear of reprisal by individuals (e.g. Through a class action suit).

Question 3: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?

It is possible that admissible Legal or Business Purpose might be used as a basis to collect, use, and disclose personal information without consent and notification. Where such action is legally approved, however, it should still be considered vital that the organisation record:

- The parties involved in any and all exchange of relevant personal data
- The data involved in any exchange
- The term of length under which any data will be kept by the receiving party
- The exact legal criteria according to which such exchange is granted, and its limitations
- The explicit purpose (usage) of the processing or holding of such data that is undergone
- Any and all further disclosure of data to third party individuals or organisations

It is important that regulation recognise the growing technological distinction that is raised by the advent of Personal Information Management Systems (PIMS) (Project-VRM, 2017) (EDPS, 2017) and Private Data Accounts (PDAs). The latter technologies empower the individual to become their own data controller, and would therefore impact any regulation governing data management.

In this scenario, it is more accurate to consider the Legal or Business Purposes for obtaining a person's private information without their consent to be akin to invading (in order to search) a person's house. This activity is allowed for under the law, but the invading authority is required to produce court warrant. Data protection should require similar documentation before any such actions were taken, and notification of the individual should a pre-requisite to its being allowed.

An explicit collection, usage disclosure, and documentation process for obtaining personal data can be used to improve and inform upon future audits in this way.

We appreciate that some data may have been collected without consent (e.g. CCTV footage of a person), particularly from a legal perspective. And such data have been been researched, reviewed, categorised and approved by the authorities. However, we see no justification for collecting data without consent for business purposes, unless proper procedures are put in place to apply for and receive approval from the authorities. Again, exemptions for business purposes puts PDPC as a trust broker at risk.

Question 4: Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?

We recommends the conditions for the Legal or Business Purpose obtainment of personal data be subject to three conditions:

1. That the obtaining organisation identify clearly who has control over the personal data in question, so as to enable the suitable DPIA.
2. That, in the case of it being an individual who holds the data and controls the data, a new proposal and alignment with other legal bodies is considered and pursued, with full disclosure.
3. That fully explicit terms of data collection, data use, and data disclosure are issued, accompanied by an auditable archive of past subjected transactions.

Question 5: What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?

We advocate the mandatory inclusion of fully auditable records governing the data control and processing by any data-controlling organisation. Having these records will ensure that organisations are capable of tracking and assessing the full impact of any data breach, serving the organisation, the regulator, and the affected individuals. (EC, 2017)

Furthermore, we suggest that the PDPA consider data breach in a tiered, scored mechanism that alerts breached individuals of their exposure according to any means that is practical for the organisation. It proposes that a three-tier notification framework, in which: any scale of breach, of any organisation of any kind, be reported to the figure of authority. We propose that the rationale for notification is based on impact, rather than the number of individuals affected. For example, we suggest any breach where it is likely to result in a high risk to the rights and freedoms of individuals, regardless affected numbers, should be reported to both authority and affected individuals. “High risk” refers to “result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. (EC, 2017) (EC, 2017)

In the case of revealing the tiered structure, we use 50,000 as an example. Breaches of a limited scale – less than, say, 50,000 personal data records – are disclosed to those affected; and breaches of a greater scale are disclosed to all of the users contained within that database. See below:

1. Tier 0 – any and all breaches must be reported to the authority (e.g. highly sensitive data or categories e.g. children, PII data, health data, etc.

2. Tier 1 – breaches of less than 50,000 personal data records with low impact, require that the breached organisation notify those affected
3. Tier 2 – breaches of more than 50,000 personal data records, or breaches of less than 50,000 records with high impact, require that the breached organisation notify all users in the affected database

We advise that the PDPA consider the impact of a significant data breach from the perspective of the affected individual, for whom the sensitivity of certain data is of the utmost importance. We suggest that special consideration be given to the danger presented by breached data potentially acting as a signature by which third party linking organisations can identify otherwise anonymised data sources (Berinato, 2015), and that such potential links be highlighted as a part of the risk of impact. We suggest that special consideration be given to the impact and effect of a breach of data on the information of a child or dependent. We also suggest that the regulating authority consider how breach ought to be treated if and when the data controller of the affected individual is the individual themselves, as it may be in the case of those using PDAs and PIMS.

We advocate a definition of a tiered structure that can be used to assess the risk of impact, with scoring, that incorporates the above concerns, and its deployment under "Aggregated Assessment," i.e. the use of both a risk of impact score and a scale indicator together. This process may provide a clearer result on the actual impact to affected individuals.

Question 6: What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?

We supports the proposed concurrent application of PDPA's data breach notification requirements and further suggests that a fully auditable record of any breach be submitted to the PDPC in order to enable improvements on the future of breach prevention.

We suggest for efficiency and consistency reasons, PDPC should set up a single point of contact to facilitate concurrent reporting rather than requiring organisations to track and report to each individual authority concurrently. Organisations faced with dealing with incidents need to focus and minimise distractions resulting from multiple reporting requirements.

Question 7: What are your views on the proposed exceptions and exemptions from the data breach notification requirements?

We recommend the following meaningful special consideration to the proposed exceptions and exemptions.

We suggest that while "encryption to a certain level" may end up being effective in stopping encrypted data from being decrypted today, it may lose its effectiveness in the future. We suggest to consider further protecting mechanisms against advances in decryption. Essentially, it is dangerous to use this as a reasonable measurement to grant exemption, given the potential

for future advances in technology to yield privacy violations from this sort of exposed information. We recommend considering the exponential and non-linear nature of advance in assessment of this criterion.

On questions relating to conditions for not providing NoP or getting consent, and conditions for exception, there must be provision for PDPC to audit the use of the explicitly defined conditions or exception to detect and penalise misuse. We do not think providing exemptions should be costless. We propose PDPC should provide economic incentives to behave well and make it costly to gain any form of exemptions. For example, rather than getting an exemption of consent, organisation will have to obtain a consent for exemption instead. In this case, the organisation in concern will have to firstly, document potential exemption scenarios; secondly, report to PDPC and ensure compliance with "exemption" rules set by PDPC (assuming PDPC sets the rules); thirdly, communicate explicit exemption conditions with the individuals for their consent prior to any of such scenarios may happen; finally, exercise the exemption only when such consent is already in place. We also believe that exemptions, as stated previously, is a slippery slope and its ambiguity would be risky to PDPC.

Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?

We support a maximum responding time (we propose a limit of 72 hours) for breached organisations, and suggest that notification to individuals should include explicit terms involving the data in concern. The following should be disclosed within this time period:

- The data points that have been leaked
- The stage of data transfer at which the leak occurred
- The original use or purpose of the affected data
- The parties of the original data exchange that experienced the breach
- The time of the breach
- How many were affected
- What impact the breach has already been known to have had

Conclusion:

Protecting individuals' data in regulation hinges upon granting that individual rights to information more than requiring complicated new actions from gathering institutions. We believe PDPC should empower the individual as our first priority.

Encouraging the leverage and use of technology to get user consent for any data collection, data processing, and data use is the responsibility of the PDPC. We believe it is no longer acceptable to say that consent is impractical to obtain. Organisations should be incentivised to gather it, and individuals ought to be empowered by regulation to stand up for themselves with richly apportioned rights.

Where, in the rare instance, consent absolutely cannot be obtained the organisation ought to follow statutes that protecting the rights of individuals to be informed, to access, to rectify, to erase, to restrict, to transport, and to object to their data's misuse, doubly insisting their

considered treatment against fear of reprisal by the empowered individual. If they should fail to do so, the law should allow them to advocate for themselves by the terms of regulation.

A growing technological distinction is being raised by the advent of Personal Information Management Systems (PIMS) and Private Data Accounts (PDAs). These technologies empower the individual to become their own data controller, and resultantly impact any regulation governing data management.

The data protection rights of the individual will in the future be a fundamental human one. Forward-looking societies will champion these rights for their citizens, empowering them to stand up for themselves against any seeking to gain insight. (Agrawal, 2017)

ANNEX

About us:

Noggin Private Limited

In the digital economy, NOGGIN (aka Noggin Asia) is solving the problem of organizations wanting the 'private & personal' insights they don't have for customer intimacy. NOGGIN is offering the digital alternative where people can safely share truths and intents willingly with worthwhile organizations seeking customer intimacy, and yet they get to monetize directly from their data unlike today. We call this the NOGGIN.ai platform that allows for developers to make apps, things and content for the 'market of one'. This is powered by the platform's privacy-preserving, private data profiling and collective intelligence technology, and driven by a data monetization business model.

For more details about NOGGIN, please visit nogginasia.com.

HAT Community Foundation Asia

HAT Community Foundation Asia represents individuals and organisations in Asia empowered by the HAT Private "Microserver" Data Account, supported by the HAT Community Foundation.

The HAT Community Foundation (HCF) is a non-profit social enterprise established to grow and regulate personal data exchange on the Hub of All Things technology. Our vision is that everyone, everywhere is empowered to get the full value of their personal data as they trade it across the Internet. Our mission is to continually improve the HAT data exchange for the benefit of HAT Owners worldwide.

For more details about HCF, please visit hatcommunity.org.

CONTRIBUTORS NAME LIST
Chua Lai Chwang
Alyce Chow
Voon Ngee Yiew
Terry Lee
Jeremy Chen
Chak Kong Soon
Kang Meng Chow
Punit Nathani
Jasdeep Singh
Kane Ong
Quoc Nghi
Tay Jun Ming
Nurhazman bin Abdul Aziz
Dennis Lee
Paul Tasker
Irene Ng
Anna Dewolf
Jonathan Holtby
Xiao Ma

Bibliography

WMG Service Systems Research Group, 2016. *HAT Briefing Paper 6 : Personal data exchange ecosystem : code of practice release 1.* [Online]
Available at: http://wrap.warwick.ac.uk/77858/
[Accessed 11 9 2017].

Agrawal, R., 2017. *India Supreme Court rules privacy a 'fundamental right' in landmark case.* [Online]
Available at: http://edition.cnn.com/2017/08/24/asia/indian-court-right-to-privacy/index.html
[Accessed 11 09 2017].

Berinato, S., 2015. *There's No Such Thing as Anonymous Data.* [Online]
Available at: https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data
[Accessed 11 9 2017].

Chesterman, S., 2017. *Privacy and our digital selves.* [Online]
Available at: http://www.straitstimes.com/opinion/privacy-and-our-digital-selves
[Accessed 11 9 2017].

EC, E. C., 2017. *Communication of a personal data breach to the data subject.* [Online]
Available at: https://gdpr-info.eu/art-34-gdpr/
[Accessed 11 9 2017].

EC, E. C., 2017. *Notification of a personal data breach to the supervisory authority.* [Online]
Available at: https://gdpr-info.eu/art-33-gdpr/
[Accessed 11 9 2017].

EC, E. C., 2017. *Records of processing activities.* [Online]
Available at: https://gdpr-info.eu/art-30-gdpr/
[Accessed 11 9 2017].

EC, E. C., 2017. *Reform of EU data protection rules.* [Online]
Available at: http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[Accessed 11 09 2017].

EDPS, E. D. P. S., 2017. *Personal Information Management System.* [Online]
Available at: https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en
[Accessed 11 09 2017].

Gordon, S., 2017. *Our personal data are precious — we must take back control.* [Online]
Available at: https://amp.ft.com/content/3278e6dc-67af-11e7-9a66-93fb352ba1fe
[Accessed 11 9 2017].

ICO, I. C. O., 2017. *Overview of the General Data Protection Regulation (GDPR).* [Online]
Available at: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
[Accessed 11 09 2017].

PDPC, T. P. D. P. C., 2017. *Personal Data Protection Act Overview.* [Online]
Available at: https://www.pdpc.gov.sg/legislation-and-guidelines
[Accessed 11 09 2017].

PDPC, T. P. D. P. C., 2017. *Public Consultations.* [Online]
Available at: https://www.pdpc.gov.sg/legislation-and-guidelines/public-consultations#ACTR1
[Accessed 11 09 2017].

Project-VRM, 2017. *VRM Development Work.* [Online]
Available at: https://cyber.harvard.edu/projectvrm/VRM_Development_Work
[Accessed 11 09 2017].
The Economist, 2017. *Data is giving rise to a new economy.* [Online]
Available at: https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy
[Accessed 11 9 2017].
The Economist, 2017. *The world's most valuable resource is no longer oil, but data.* [Online]
Available at: https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource
[Accessed 11 9 2017].
WMG Service Systems Research Group, 2015. *HAT briefing paper 1 : Engineering a market for personal data : the Hub-of-all-Things (HAT).* [Online]
Available at: http://wrap.warwick.ac.uk/65605/
[Accessed 11 9 2017].
WMG Service Systems Research Group, 2015. *HAT Briefing Paper 2 : The Hub-of-all-Things (HAT) economic model of the multi-sided market platform and ecosystem.* [Online]
Available at: http://wrap.warwick.ac.uk/65607/
[Accessed 11 9 2017].
WMG Service Systems Research Group, 2015. *HAT Briefing Paper 3 : The Hub-of-all-Things (HAT) code of practice on personal data.* [Online]
Available at: http://wrap.warwick.ac.uk/65608/
[Accessed 11 9 2017].
WMG Service Systems Research Group, 2016. *HAT Briefing Paper 4 : HAT personal data exchange ecosystem - technology architecture briefing.* [Online]
Available at: http://wrap.warwick.ac.uk/77855/
[Accessed 11 9 2017].
WMG Service Systems Research Group, 2016. *HAT Briefing Paper 5 : Rolling out HATs and creating the market for personal data - the HAT foundation.* [Online]
Available at: http://wrap.warwick.ac.uk/77857/
[Accessed 11 9 2017].
WMG Service Systems Research Group, 2016. *HAT Briefing Paper 6 : Personal data exchange ecosystem : code of practice release 1.* [Online]
Available at: http://wrap.warwick.ac.uk/77858/
[Accessed 11 9 2017].