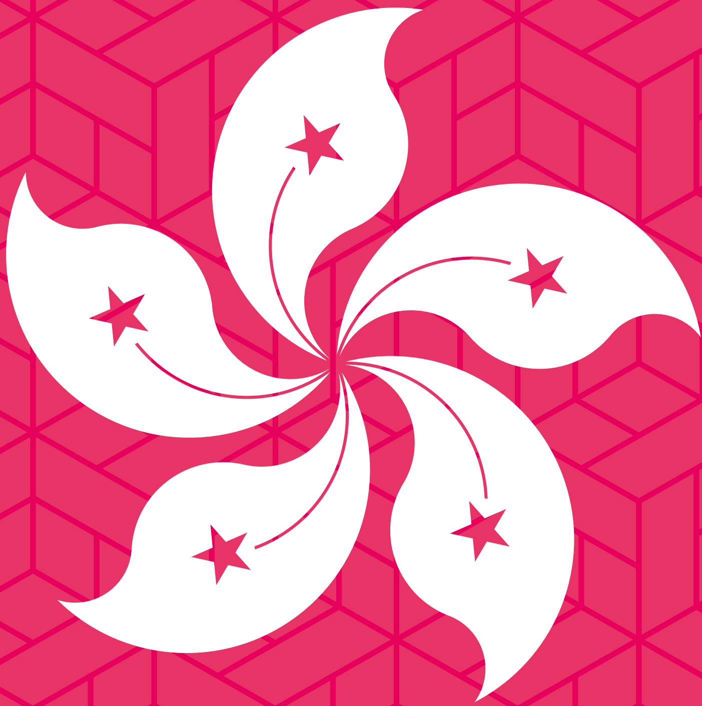
KONRAD
ADENAUER
STIFTUNG



Fintech, Data, Innovation and Privacy in Hong Kong

Marko M. Skoric, Chun Hong Tse and Juma Kasadha
City University of Hong Kong
Jeremy Pui, King's College

DATA AND INNOVATION
IN ASIA-PACIFIC

www.kas.de

CONTENT

PREFACE

Data fuels digital change. It forms the basis for numerous new products and services and can bring about specific advantages such as personalised medicine, autonomous driving, or more efficient administration. While data may be indispensable for the generation of new knowledge and may aid rational decision-making in the spheres of politics, society, and the economy, it brings with it an element of fear stemming from issues such as vulnerable consumers, privacy concerns, and the possibility of algorithm-based decisions being executed independent of human control.

The ability to collect and process ever-increasing amounts of data is a **key to innovation and growth**. For states such as Germany with a globally networked and high-tech economy, this presents enormous opportunities – especially due to the increasing amount of non-personal data made available through industrial processes as well as public sources. However, neither Germany nor Europe is fully exploiting the innovative potential of data for the benefit of society, the economy, science, and the state. The collection and analysis of data does not have to be in conflict with the **European approach to data protection, which marks an important standard for the responsible handling of data** in the global context.

Numerous US and Chinese companies have occupied central strategic positions in the digital economy in recent years. These include cloud systems, digital payment systems, online trading, and Artificial Intelligence (AI). **Despite some notable successes, Europe and Germany still lack a comprehensive vision for the "age of data".** Nevertheless, in the spring of 2020, the European Commission launched its roadmap for digital policy – a "Data Act" to create a single European data market is planned for 2021.

Against this background, it is worth taking a **comparative look at the Asia-Pacific region** as it is generally considered the region that currently leads in both global innovation and economic growth.

Hence the Konrad Adenauer Foundation's regional programme "Political Dialogue" based in Singapore started a large-scale study in September 2019 on *Data and Innovation in Asia-Pacific*. We want to turn our gaze away from Silicon Valley to other important "data nations" in order to investigate the ambiguous and not-at-all-clear **connection between the use of digital data and the innovative capacity of economic and social systems**. However, we will not limit our analysis to technical and economic issues as the exploration of this ambiguous connection inevitably involves the fundamental political question concerning the *systemic competition* between liberal-democratic societies and authoritarian development models – in particular, that of the People's Republic of China – with regard to the manner in which data is attained and used. To put it more pointedly, the question is: in times of omnipresent data generation and its use by increasingly AI-based systems, is the ability to innovate only to be had at the price of the complete disclosure of private data to governments and corporate actors? Or can an alternative approach, one balancing both the protection of basic rights and promotion of innovation, be found?

The study was carried out in collaboration with the National University of Singapore (NUS) and was supported by the country offices of the Konrad-Adenauer-Stiftung in Asia-Pacific. We selected **Hong Kong SAR, India, Japan, the People's Republic of China, Singapore, South Korea, and Taiwan** as the contexts to be examined. We looked at the areas **of transport, finance, administration, health, and Industry 4.0** to understand how added value for society and the economy can be created through modern data use.

We aim to contribute to the discussion on how to balance data usage and data protection in order to promote innovation in this digital age.

The following questions guided us in this study:

Narratives
How do companies, state actors, and civil society understand the handling of data – especially personal data – and the ethical assessment of such use? What are the prevailing narratives in each country?

Legal Bases
What are the laws and regulations that apply to the collection, use, storage, provision, disclosure, retention, and disposal of personal and non-personal data? What is the status of the development of legislation for these matters and how do different stakeholders deal with the issues of data protection and data portability between different (private and public) systems?

Ecosystem
Data is part of a larger "innovation ecosystem". Its potential can only be realised through interaction with other innovation-promoting elements. What specific legal, technological, infrastructural, cultural, and economic aspects of a country shape the respective ecosystems and determine performance?

In Singapore, Japan, and Taiwan, the study is also supplemented by a representative population survey on data culture.

We hope that the diverse pictures presented on the subject of data and innovation in Asia will provide food for thought in Germany, Europe, and Asia itself.

Dr. Peter Hefele
Director Asia and the Pacific

SUMMARY

Through a combination of semi-structured expert interviews, desk research, attendance and records of fintech talks and seminars, and a survey of 1170 Hong Kong residents, this reports provides key insights on data protections, innovations and perceptions particularly in the domain of fintech in Hong Kong. Here are some key findings:

1. Hong Kong, as one of the Special Administrative Regions of the People's Republic of China, provides an attractive environment for the development of the fintech industry, through its pro-business environment, supported by simple and low taxation, common law protections, well-developed financial sector, easy access to Mainland China, and world-class digital infrastructure.

2. The Government of Hong Kong actively supports the development of fintech industry by providing incentives for fintech companies to operate in Hong Kong and by setting up frameworks for implementation and testing of fintech solutions such as the Fintech Supervisory Sandbox.

3. Regtech, Blockchain, and Insurtech are among the top three fastest growing fintech industries.

4. The legal and regulatory framework, the Personal Data (Privacy) Ordinance (PDPO), provides a solid protection for personal data in general, balancing business interests with individual privacy protection, but greater definitional clarity may be needed when it comes to different types of digital data.

5. Although operating under separate legal and regulatory frameworks from Mainland China, Hong Kong-based fintech companies are likely to come under increasing pressure from more stringent regulation of fintech services in Mainland China, as shown by the Ant Group's cancelled IPO.

6. Regarding the public perception towards data privacy and protection, Hong Kong residents are generally cautious about sharing their personal data and are active in performing data protection practices. On the other hand, they have relatively low trust towards government and private companies for appropriate data use.

7. Regarding the data protection responsibility, Hongkongers tend to emphasize that it is government's main duty to uphold data protection followed by their own responsibility. Companies are the least responsible in this matter.

8. Most Hongkongers also feel that the current data and privacy protection laws and policies are inadequate, as reflected by the survey.

9. Hongkongers also emphasize individual responsibility for personal data protection, beyond those of the government and the private sector, despite majority entrusting the government more when compared to the private sector.

The goal of this project is to describe and analyse one of the key fields of the data innovation landscape in Hong Kong – the emerging financial technology (fintech) industry. Our aim is to deepen our understanding of innovation and data policies, as well as citizens attitudes towards data sharing, and contribute to debates that often focus on European models of data protection such as the General Data Protection Regulation (GDPR) framework. The report is centred on data privacy practices in Hong Kong and The Personal Data (Privacy) Ordinance (2012).

> Our aim is to deepen our understanding of innovation and data policies, as well as citizens attitudes towards data sharing, and contribute to debates that often focus on European models of data protection such as the General Data Protection Regulation (GDPR) framework.

Through a combination of semi-structured expert interviews, desk research, attendance of fintech talks and seminars, and a survey of 1,170 Hong Kong residents, we seek to understand the emerging innovative data practices in the context of relationships among key stakeholders such as citizens, government agencies, corporations, and research institutions. We find that in general, Hong Kong Government has a strong commitment to protecting personal data and privacy of its residents, while at the same time maintaining a pro-business mindset and encouraging the development of fintech services that leverage on the large-scale access and analysis of consumer data. Moreover, the Government takes a proactive stance in encouraging data-driven innovation; for instance, the Fintech Supervisory Sandbox allows fintech companies to conduct trials to receive data and feedback from a limited number of participants, under the supervision of the Hong Kong Monetary Authority. In terms of public perceptions and attitudes regarding personal privacy, we find an interesting pattern. Although Hongkongers are quite sensitive about personal privacy in general, they are also pragmatic in terms of being prepared to share some basic personal information with companies in exchange for greater convenience and improved shopping experience. Furthermore, Hong Kong residents tend to trust the Government most when it comes to protecting their personal data, while at the same time emphasizing individual responsibility for data protection.

This report begins with an introduction to the Hong Kong context and the key trends and organisations in data regulation. Next, it discusses (1) collection and the use of data and the impact on innovation capacity (Part A), (2) people's perceptions around data and innovation (Part B), and (3) data and value creation (Part C). Finally, it concludes with a recap of the factors and players which drive innovation in Hong Kong, and looks ahead at how the discourses around data may evolve in the future.

THE CONTEXT OF HONG KONG

Formerly a British colony from 1842 to 1997, the sovereignty of Hong Kong was transferred back to the People's Republic of China in 1997. Being the Special Administrative Region of China, the "one country, two systems" principle maintains the governmental, legal, economic, and financial systems to be independent of Mainland China.

According to the statistics from the Census and Statistics Department (2020), Hong Kong has 7.47 million people. While the Chinese form the majority of the population, Hong Kong is a place with a significant foreign population. More than 500,000 non-Chinese, including Indonesians, Filipinos, Britons, Americans, Indians, Japanese, Australians, Pakistanis, and Nepalese currently reside in Hong Kong.

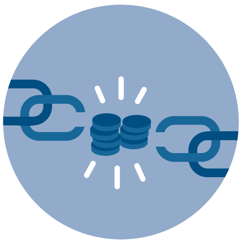
The constitutional framework is provided by the Basic Law enacted by the National People's Congress of the People's Republic of China (PRC). Different from Mainland China, the Basic Law is based on a common law system. Freedoms of speech, assembly, and religion are protected, and torture and unwarranted searches, seizures, and arrests are prohibited under the Basic Law. A point that is worth noting is a recent introduction of the National Security Law in Hong Kong by the National People's Congress of the People's Republic of China. At the time of writing, the national security law has been implemented for less than a year (the law was passed on 1 July 2020), and its effects on the fintech industry and Hong Kong's image as the international financial center are still rather unclear.

Hong Kong has been widely recognized as Asia's premier financial center. The "one country, two systems" principle allows Hong Kong to leverage on both China's economic dynamism as well as its pro-business, common law-based regulatory and legal environment. In Hong Kong, there are more than 1.3 million local companies and over 13,000 non-local registered businesses, fully utilizing the city's strategic advantages, including finance, sales, operations, research and development (R&D), distribution, and regional headquarters. Hong Kong is well-known for several advantages:

1. **Simple and competitive tax system:** Hong Kong is one of the most tax-friendly places globally, with only three kinds of taxes imposed, including profits tax, salaries tax, and property tax. Salaries tax and property tax are both 15%. Hong Kong does not impose taxes, such as sales tax, estate tax, withholding tax, capital gains tax, etc. Furthermore, the free trade port status provides a conducive environment for businesses to operate in, particularly if they operate internationally.

2. **Legal system:** After the handover in 1997, Hong Kong maintained its own currency, political and common law legal systems under the "one country, two systems" principle. This includes the following advantages: free movement of capital, talent, goods, and information, English as one of the official languages, and no foreign ownership restrictions.

3. **Economic freedom:** According to the 2020 Index of Economic Freedom by the Heritage Foundation, Hong Kong was ranked as the second freest economy out of 186 economies. The index assesses from various perspectives, namely size of government, legal system and property rights, sound money, freedom to trade internationally, regulation.



4. **Location:** Hong Kong connects not only Mainland China but also places along with Asia, Europe, and the Middle East. The new Guangdong-Hong Kong-Macao Greater Bay Area plan allows Hong Kong to reap the cluster's benefits, leveraging on several strengths (finance, technology, trade, and manufacturing) from across the cluster.

5. **Trade and economic ties:** Fully utilising the advantage of the Belt and Road Initiative, Economic and Trade Offices (ETOs) promote the trade and economic ties along with the belt and road places. Thus, goods and services can be better exported from Hong Kong to Greater China and across the globe.

6. **Good digital infrastructure:** Being one of the most connected places globally, Hong Kong has 5.5 million Internet users (out of 7.47 million residents) with a 92.8% household broadband penetration rate in 2018. A 79% smartphone penetration rate indicates most Hong Kong residents have access to advanced digital services and applications.

Fintech Industry in Hong Kong: An Overview

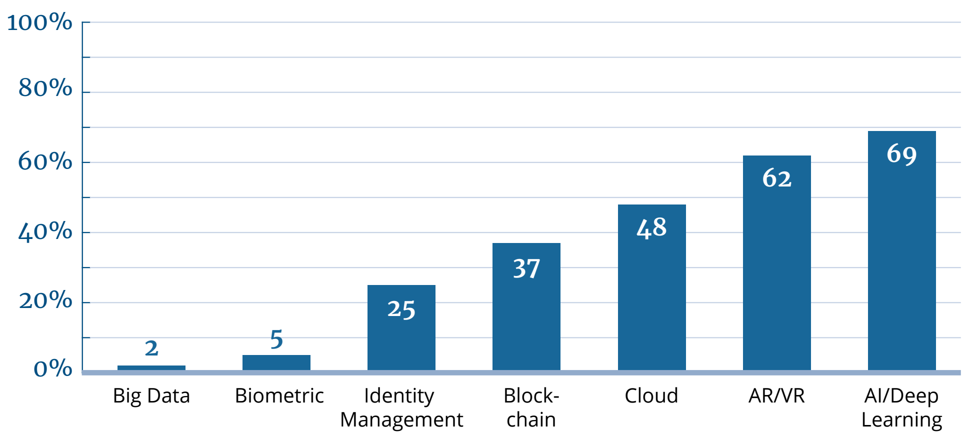
Hong Kong has a flourishing fintech ecosystem, and many companies have integrated fintech solutions in their business models (see Table 1). Of these, 67% use a B2B model (Business to Business), 45% B2B2C (Business to Business to Consumer), and 39% use a B2C (Business to Consumer) model.

Table 1: Hong Kong's Fintech Major Players in Different Sectors

Sectors	Major Players
Financing	Lending Club, Monexo Innovations Limited, WeLab Bank
Payments and Infrastructure	Octopus, Faster Payment System (FPS), Alipay, Payme (HSBC), WeChat Pay
Operations and Risk Management	Wolters Kluwer, Infosys, Credissimo
Data Security Monetisation	Atcipher, Rook Security, Axtria
Customer Interface	Apple Pay, Facebook, Xiaomi

Source: Hong Kong FinTech White Paper V3.1, 2019.

Figure 1: Technologies Used by Fintech Startups in Hong Kong



Source: Hong Kong FinTech White Paper V3.1, 2019.

Similar to London and New York, Hong Kong is one of the leading fintech players in the world. In 2019, there was US$376 million private capital raised for fintech industries, which is twice as much as in 2018. Hong Kong has more than 160 banks and insurers, and 800 wealth and asset management companies. About 86% of the traditional banks adopt fintech solutions in Hong Kong, and there are 8 virtual banks and 4 virtual insurers. With its access to Mainland China and international markets, 44% of the fintech founders come from overseas, while the remainder come from Mainland China and Hong Kong. Regtech, Blockchain, and Insurtech were the top three fastest-growing fintech categories in 2019. According to the 2019 Hong Kong fintech white paper, four out of 9 unicorns have been classified as the fintech unicorns in Hong Kong, namely WeLab (virtual banking), BitMEX (cryptocurrency trading), TNG Wallet (e-wallet), and AirWallex (e-payment solution).

Fintech Regulatory Landscape

To better understand the regulatory and fintech development landscape in Hong Kong. Here is a list of the key stakeholders.

1. **Hong Kong Monetary Authority (HKMA)** is a central banking institution in Hong Kong. Founded in April 1993, it maintains currency stability and the stability of the financial system. Another vital function is to maintain the city's status as the international financial center by cultivating fintech innovation. The Fintech Supervisory Sandbox, which is under the HKMA, is an important initiative for fintech startups to test their products before launching.

2. **Office of the Privacy Commissioner for Personal Data** serves as the main authority for data protection issues. It was established to administer and enforce the Personal Data (Privacy) Ordinance (Cap. 486), which is the primary data protection law in Hong Kong.

3. **InvestHK** is a department operating under the Government of Hong Kong. It strives to attract foreign direct investment and enhance the city's international business status. It also works with different stakeholders, including entrepreneurs, to enlarge and support their business by providing advice and services.

Regulating Data Privacy in Hong Kong: The Personal Data (Privacy) Ordinance

In Hong Kong, the privacy of personal data is protected under the Personal Data (Privacy) Ordinance, or PDPO (2012). Based on the OECD Privacy Guidelines 1980, the PDPO was passed in 1995, following a Law Reform Commission Report published the year prior. The Ordinance regulates the collection and use of personal data, and applies to both the private and public sectors.

In 2012, significant amendments were made to the PDPO by the Personal Data (Privacy) (Amendment) Ordinance 2012, for example, the establishment of direct marketing provisions.

Key definitions under the PDPO include:

- **Personal Data:** information which relates to a living individual and can be used to identify that individual.
- **Data Subject:** the individual who is the subject of the personal data.
- **Data User:** a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data.

The main provisions of the Ordinance are the Data Protection Principles, or DPPs. These principles give direction on how personal data should be collected and handled, and must be complied with by all data users. There are six DPPs (Community Legal Information Centre, 2020):

- **Purpose and Manner of Collection:** Personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user. The data should be collected in a lawful and fair manner, and should be necessary and adequate without being excessive for such purpose.
- **Accuracy and Duration of Retention:** Data users must take all practicable steps to ensure that personal data is accurate. Additionally, data users should not keep data longer than necessary to fulfil the purpose for which it was obtained.
- **Use of Data:** Personal data may not be used for any purpose other than the one mentioned at the time of data collection. Informed consent from the data subject is required for personal data to be used for a new purpose, for example, transferring data to a third party for direct marketing.
- **Data Security:** Data users must take appropriate security measures to protect the personal data that they store. Potential security threats include the unauthorised or accidental access or erasure of data.
- **Openness and Transparency:** Data users must take all practicable steps to ensure openness of their personal data policies and practices. They must publicly disclose the kind of data held by them and how it is handled.

- **Access and Correction:** Data subjects have the right to ask data users if they hold any of their personal data. They can also request a copy of their personal data and request inaccurate data to be corrected.

The contravention of a DPP is not an offence per se, however, the breach of certain provisions of the PDPO can amount to an offence. For example, the failure to comply with direct marketing requirements can result in a fine up to $500,000 and imprisonment for 3 years. Complaints relating to the PDPO can be made to the Office of the Privacy Commissioner for Personal Data. Following an investigation of the claim, the Commissioner may issue an enforcement notice to the data user, directing remedial or preventative steps to be followed. Failure to comply with an enforcement notice is an offence and may result in a fine of up to $50,000 and imprisonment for 2 years, with a daily penalty of $1,000. There are certain derogations to the requirements of the PDPO, such as crime prevention and security reasons.

In January 2020, the Constitutional and Mainland Affairs Bureau published a paper suggesting further reform of the PDPO. At the time of writing, the reform proposals are at a preliminary stage (Koo & Chung, 2020).

Data-Driven Innovation and Fintech in Hong Kong

Part A: Collection and use of data and the impact on innovation capacity

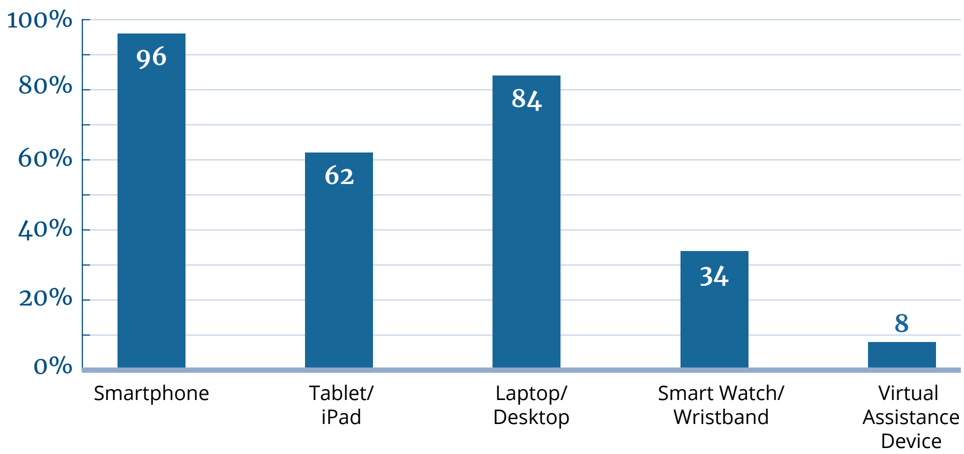
The fintech industry significantly benefits from Hong Kong being one of the leading international financial centers. A large and dynamic financial industry and coupled with world-class tertiary education institutions provide a fertile ground for the development of the fintech ecosystem.

According to our interviewees, various stakeholders attach great importance to collected data. For instance, a project manager working on blockchain solutions described collected data as the "lifeblood of the global economy", which assists them in developing artificial intelligence (AI) solutions, for instance by training machine learning algorithms. Collection and use of data from customers also help to improve the efficiency of their business operations.

There are several reasons to consider that the ordinance is effective. Firstly, the common law system in Hong Kong enables flexibility to adapt to the new change in the economy and the financial sector. Judges can make decisions based on the latest developments in the industry because of case law. Secondly, Hong Kong has balanced rather well the business interests and citizen's data privacy protection. Compared with the opt-in approach adopted in Europe, Hong Kong adopts an opt-out approach, in which data will be collected and used automatically unless the person actively disagrees with data collection (Understanding Patient Data, 2018). Given that the person does not have to actively declare their willingness for data collection and use, data collectors have more opportunities to use personal data. A legal scholar commented that the balance between encouraging innovations and protecting citizens' basic rights has been achieved successfully in Hong Kong. Considering the opt-in and opt-out approaches, a fintech professional raised concerns towards innovation flourishing by comparing the user experiences in China and Hong Kong. He observed that most citizens in China are willing to give data collection consent to government and private organizations since they want to enjoy services provided by them, while Hongkongers are more reluctant to sacrifice their privacy as they are concerned about individual rights. The opt-in approach requires everything to be granted with permission from users, consequently decreasing the volume of data that can be collected, at least in principle. Nonetheless, the opt-in approach provides a way to decline collection permission (for example using the unsubscribe option), which balances the needs of data collection and individual rights.

On the other hand, there are also several reasons for considering the ordinance to be ineffective. First, uncertainty arises when it comes to the definition of personal data, although the legal language written in the ordinance is quite clear. A scholar who did research in this area showed a controversial opinion towards the qualification of personal data among different stakeholders. For instance, researchers believe that geo-location data and IP addresses of personal devices should be considered as personal data while the experts who work in telecommunication sectors do not think so. This is an issue, as a vast majority of Hong Kong residents use multiple digital devices to access the internet – smartphones, tablets, laptops, smart watches and virtual assistance devices (See Figure 2). This situation highlights the need to clarify what type of data should be considered personal and/or sensitive. Nevertheless, the cost of clarification within the Hong Kong legal system is high since the issue has to be addressed by the courts. Second, there is a certain lack of coverage within the data collection governance framework, for example, regarding facial recognition. Indeed, there are thousands of surveillance cameras collecting facial data in shopping malls, commercial buildings around Hong Kong, which could imply that the data is being collected for commercial purposes without people's knowledge and consent.

Figure 2: Ownership of Digital Devices in Hong Kong



Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

These problems are not unique to Hong Kong, however. Similar problems with the legal interpretation are also reported in Taiwan. The data privacy law in Taiwan is called the Personal Information Protection Act (2015). One of our interviewees conducted focus groups with telecommunication professionals in Taiwan, who emphasized the difficulties in striking a right balance between data protection and innovation. Indeed, it is crucial to ensure the user's information is being protected so that users feel safe and willing to trust the system. A significant concern for them is the identification of the data subject. In the Personal Information Protection Act, data refers to "a natural person's name, date of birth, ID Card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial conditions, data concerning a person's social activities and any other information that may be used to directly or indirectly identify a person." The data subject is not clearly interpreted in the law, mentioned by the data controllers in Taiwan. Although it is believed that the laws are set to protect consumers and users, the lack of interpretation leads to difficulty in using big data. Also, there is no specific government department such as the Privacy Commissioner for Personal Data in Hong Kong, to regulate and execute the law in Taiwan.

The General Data Protection Regulation (GDPR) in the European Union and the European Economic Area is also worth examining. Scholars and lawyers in Hong Kong agreed that the GDPR is a heavy-handed piece of regulation. Although it performs well in protecting individual rights, it may negatively affect the dynamism of the economy and undermine future innovation and business efficiency. Still, they recommended several lessons of GDPR for Hong Kong:

1. **Transparency:** Businesses should declare what data they collect and how they use the data. The transparency should also consider the protection of business efficiencies.

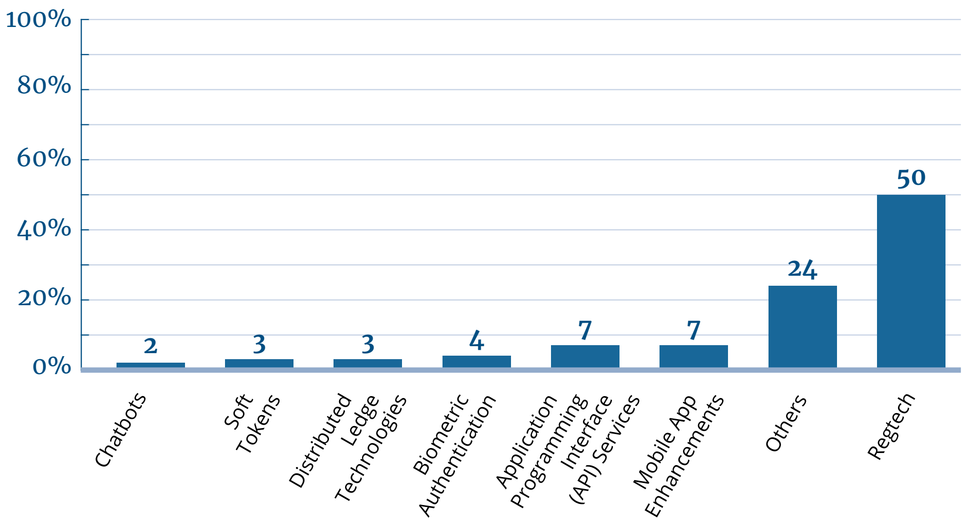
2. **More specific definition of personal data:** According to the PDPO, personal data refers to "information which relates to a living individual and can be used to identify that individual. It must also exist in a form in which access to or processing of is practicable". In contrast, the long list of data types introduced in the GDPR, with a specific definition of names, IP addresses, and geo-location, provides a higher level of clarity. A fintech professional added that specific examples should be added to the Guidance on Collection and Use of Biometric Data (2020), such as dealing with fingerprint and facial recognition on smartphone devices.

Speaking about the future amendment of PDPO, Our interviewees predict further changes in the Ordinance, suggesting the following revisions to the code. Firstly, the law should be tightened on the monetization and the commercial use of data, while the use of data from the personal perspective should remain flexible. Secondly, the government should pay more attention to the importance of data flow, telecommunication, and virtual banking issues. At the time of writing, the Chief Executive of Hong Kong, Carrie Lam mentioned the government was working on revising the ordinance in early February 2021, tackling the dissemination of "fake news" and hate speech, and considering putting doxing as a criminal offense.

A question that triggers a debate among stakeholders is about striking the right balance between aiding the innovation capabilities of firms and protecting personal privacy rights. Interviewees stressed the importance of noting that different countries and territories have their own motivations for promulgating their data privacy laws. Even if the privacy ordinance framework in Hong Kong was not as strong as GDPR, the regulations are written clearly. Nonetheless, a legal expert noted that although the framework of privacy laws in different places could look similar, the interpretations and practices could differ significantly. When authorities try to enforce their data privacy laws, the same language can be interpreted in a different way, potentially hindering cross-border innovation in business models.

A fintech expert working for the government suggests that the current legal framework in Hong Kong strikes the right balance. Regulations are needed to protect the right of residents, and the Ordinance gives heads-up if an organization has a problem in violating data protection principles. Moreover, the government has been proactive about providing support to fintech startups, including setting up frameworks for implementation and testing of their solutions. For example, the Fintech Supervisory Sandbox launched by the Hong Kong Monetary Authority in September 2016, allows fintech companies to conduct trials to receive data and feedback from a limited number of participants, under the supervision of the Hong Kong Monetary Authority. The Sandbox enables fintech companies to refine their initiatives before launching under four safeguards – boundary, customer protection measures, risk management controls, readiness, and monitoring. There are 203 fintech initiatives that used the Sandbox as of the end of February 2021, including biometric authentication, soft tokens, chatbots, distributed ledger technologies, API services, Regtech, and mobile apps enhancement (Figure 3).

Figure 3: Distribution of Technologies Involved in Pilot Trials in Hong Kong



Source: Hong Kong Monetary Authority, FinTech Supervisory Sandbox (FSS), February 2021. 203 cases considered.

From our interviews, several recommendations on how to improve the existing laws related to data and privacy protection have emerged:

1. An expert in blockchain solutions commented that "existing laws/regulations are quite loose." This means that there are no solid and explicit laws to protect data extraction, collection, utilization, leading the companies to use the data rather easily, with few restrictions. For example, organizations can harvest and pass users' information across different industries. Concrete regulations are needed to protect the data security.

2. Citizens need to trust the system, in order to agree with the collection of personal data; they are aware that their personal data may be used for unethical or even criminal activities, including blackmail. A scholar elaborated the quality of data provided by citizens is highly dependent on their trust in the technological systems and organizations collecting and managing the data. Enhancing people's trust in data collection procedures increases the quality and the quantity of data being collected, benefitting innovation consequently.

3. Apart from balancing the interests, regulators should improve the clarity of the existing laws. There should be clearer rules specifying how the regulators should stop the behavior if it is in breach of the regulation.

4. While there are unintentional grey areas, the Fintech Facilitation Office can help entrepreneurs interpret rules and fill those gaps. The Fintech Facilitation Office is a platform established by the Hong Kong Monetary Authority in 2016 for fintech stakeholders to exchange ideas and enhance their understanding of the fintech regulatory landscape in Hong Kong. It also helps fintech initiatives to minimize potential risks and nurture future fintech talents.

5. From a commercial perspective, data collection and data analysis create numerous opportunities for companies to use and collect consumer data, thus creating business value. The fintech industry hopes for light regulation of digital industries, especially blockchain and AI in order for the industry to flourish in the future.

> From a commercial perspective, data collection and data analysis create numerous opportunities for companies to use and collect consumer data, thus creating business value. The fintech industry hopes for light regulation of digital industries, especially blockchain and AI in order for the industry to flourish in the future.

China's Role in Hong Kong's Fintech Industry: A Curious Case of the Ant Group's Cancelled IPO

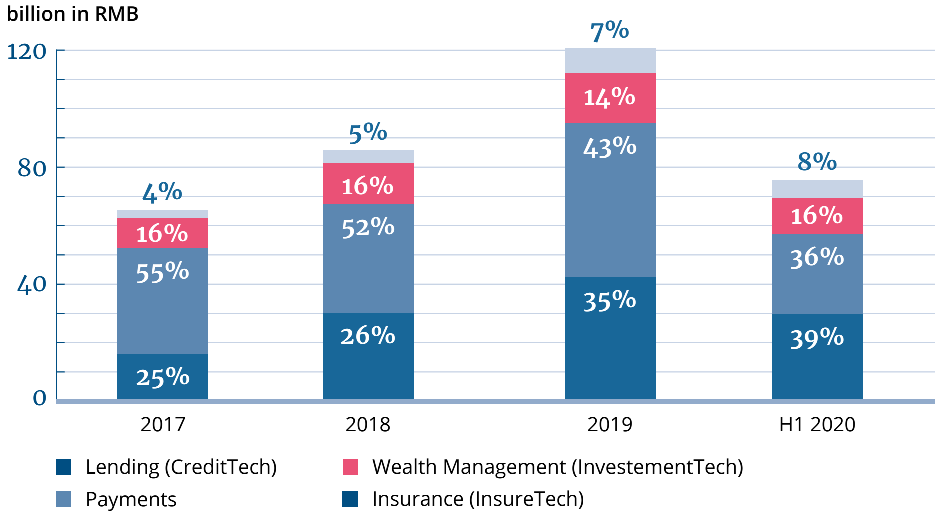
Many of the fintech startups incorporated in Hong Kong are primarily looking to focus on a vast emerging "datascape" of Mainland China to serve its customers, while benefiting from low taxes, common law protections, and business friendly environment in Hong Kong. While such ventures are generally supported by both national and local authorities, there are some recent cases which demonstrate the difficulties that may emerge from such "cross-border" arrangements. One of the events that has captured public attention in the late 2020, was a failed IPO at the Hong Kong Stock Exchange of the fintech giant Ant Group.

Jack Ma's Alibaba Group built a payment system Alipay in China in 2004, and the system enable users to make payments easily and instantly. Not surprisingly, the system proved to be very popular, and currently, Alipay today has around a billion users, with more than 730 million users active each month. Consequently, Alibaba Group spun off Alipay and recapitalized its services to a company called Ant Group in 2014.

Ant Group is a fintech company that provides a variety of services. Apart from the digital payments and merchant services (for example, Alipay), it also provides new services including CreditTech (for example, Huabei), InvestmentTech (for example, Ant Fortune), InsureTech (for example, Xiang Hu Bao). Spun off from Alibaba in 2011, the four segments of services brought Ant Group US10.3 billion in revenues in 2020. Alipay, which is the centralized platform consolidating the four services, is the largest digital payment platform and credit services provider in China. Ant Group's IPO aimed to raise around US$34.5 billion in late 2020, compared with that of Aramco's US$29.4 billion and Alibaba's own IPO at US$25 billion and would value Ant Group at US$313 billion, given its growing share of revenues accrued from lending business (see Figure 4).

Figure 4: Ant's Growing Share of Revenue from Lending

Revenue share by business line



Source: Company Data published in Financial Times.

The Ant Group's Artificial Intelligence measures credit limits and interest rates based on the borrower's use history from Alibaba services, such as paid utility and whether the borrower has paid bills on time, resulting in a low loan delinquency rate of 1–2%. In China, mobile payment accounts must be linked to both personal details and bank accounts. The users of the services in China are generally eager to disclose personal information such as address and annual income in order to improve their credit scores in Ant's credit system, Sesame Credit.

Ant Group's IPO was considered to be a shining example of the bright future of fintech industry in China and Hong Kong, demonstrating the potential of innovation in the financial sector using consumer data. However, the IPO was called off two days before its debut at the Hong Kong Stock Exchange. According to the statement made by The Financial Stability and Development Committee (FSDC) – a financial regulatory body under the China's State Council, the IPO was suspended to limit any systemic financial risk, aiming to provide the right balance in the future between encouraging innovation and sound regulation. The regulator followed-up with the tightened regulations on the finance and online microloan sectors, slashing individual loans and tightening the capital contribution requirement for online platforms. The rules required Ant Group to fund more than 30% of the loans, instead of 2%, which leads to the disruption of the current business model run by Ant Group. After a meeting with Ant Group and the regulators in China, the Shanghai Stock Exchange stopped the IPO on Nov 3, 2020, given that requirements were not fulfilled.

Although initially surprising, this move by the financial regulator was prompted by the rising levels of debt in China. The household debt-to-income ratio in China reached 128% at the end of 2019, posing a serious risk to financial stability. The IPO would put Ant Financial to a worth of US$359 billion, which is larger than the Industrial and Commercial Bank of China (ICBC) – a bank owned by the Chinese government. The Chinese government worried that Ant Financial, the private company, would bring more foreign investors, and that its potential failure could be disastrous for the whole economy. There is a need to protect the interest of banks owned by the government. Fintech companies in China, for example, ant group, lufax.com, put 2–4% of their capital for loans. The new regulations increased the percentage to 30%, which reclassifies the nature of becoming a bank instead of a private company.

“Every participant in the market must follow the laws, and no one can make exceptions,” Xinhua, a Chinese news agency, commented. The new rules introduced by Chinese regulators reflect a stricter regulatory stance towards fintech firms. Ant Group has arguably been a victim of its own success, and its failed IPO demonstrates that the future growth of the data-driven financial services in Hong Kong is likely to be increasingly determined by the regulatory climate in Mainland China.

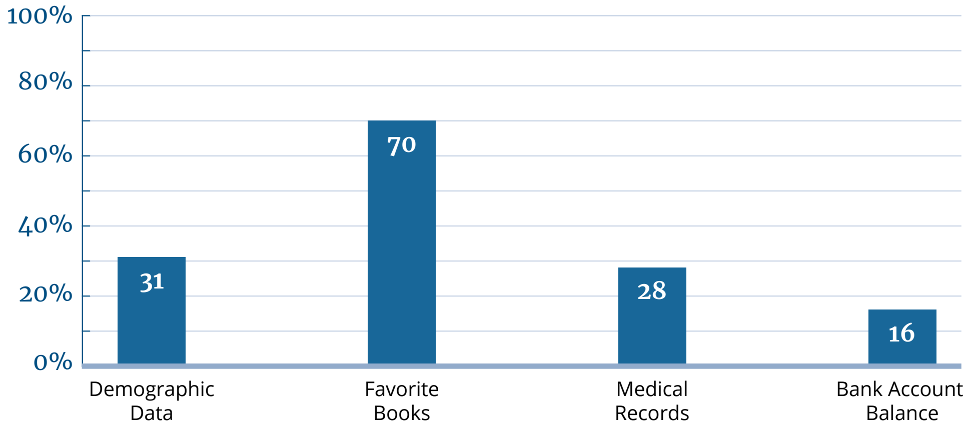
Part B: Perceptions Around Data and Innovation

In Hong Kong, personal data is defined as “information which relates to a living individual and can be used to identify that individual”. A similar understanding as in many other jurisdictions, examples of this information includes an individual’s name, address or date of birth among many others.

Regarding the attitudes of the general public, one of our interviewees, a journalist in a prominent newspaper, suggested that “Hongkongers are quite sensitive about data privacy”. A potential cause of this may be the fact that Hong Kong can be thought of as a relatively small society where the threshold for anonymity is lower – although being a global metropolis with more than 7 million residents, it is geographically small and separated from the rest of China with a “hard” border. Still, Hong Kong consumers are pragmatic and accept some common business practices involving the collection of personal data, for example, leaving behind their names and phone numbers to get membership in supermarkets, department stores and other retail businesses. In a conversation with a cybersecurity expert, it was mentioned that “most individuals in Hong Kong hold a more pragmatic sense”, and that people accept the exchange of basic personal data for convenience. Our survey findings show that while most Hongkongers do not mind sharing the data on their favorite books, the number drop dramatically as the nature of data sharing moves towards more sensitive personal information, including demographics, medical and financial (see Figure 5).

> A journalist in a prominent newspaper, suggested that “Hongkongers are quite sensitive about data privacy”.

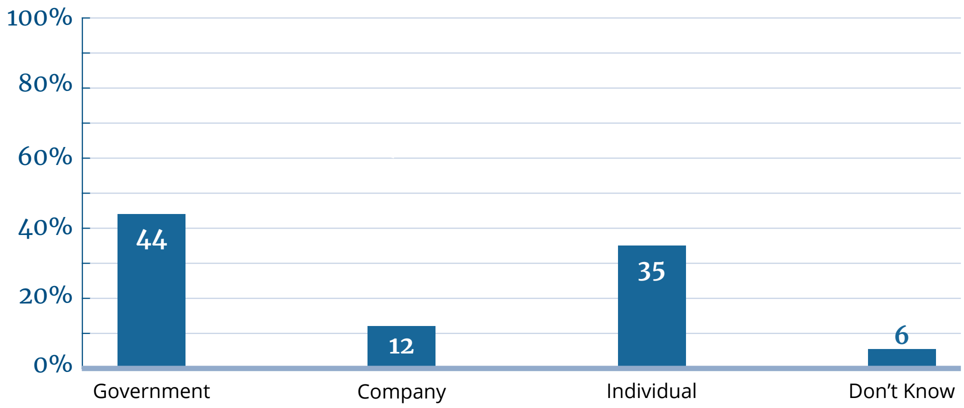
Figure 5: Willingness to Disclose Personal Data



Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

There are ongoing debates regarding the ownership and control of the vast amounts of data generated by the digital mediation of most aspects of everyday life. As observed by industry professionals, different citizens apportion responsibility on the agencies tasked to control the access to a user's data. Accordingly, a majority of citizens presume that it is the duty of the government to monitor and control access to their data, whereas some think it is a company's or an individual's responsibility. In Hong Kong, over 40% of the surveyed respondents apportioned data protection responsibility to the government compared to the 12% that entrusted the responsibility to companies. Although 6% of the respondents didn't know whose duty it was to control/protect their data, 35% apportioned it to individuals (see Figure 6).

Figure 6: Citizens' Perception on Data Protection Responsibility

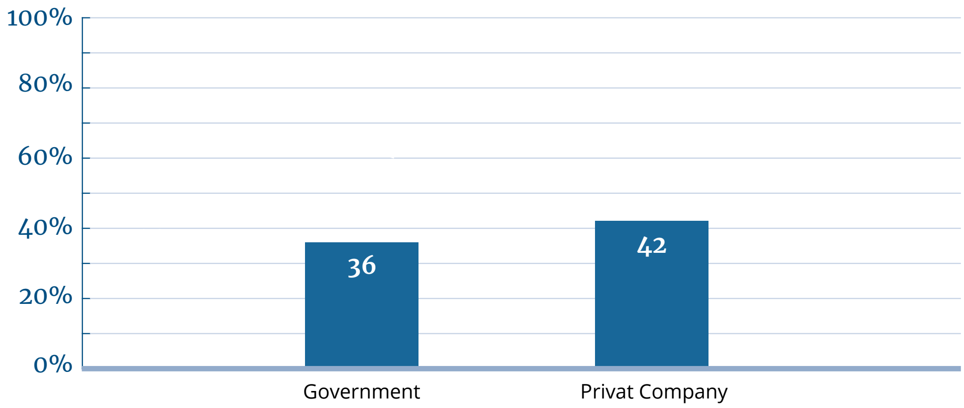


Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

Therefore, our respondents also emphasize the importance of individual responsibility for ensuring one's data is protected despite also entrusting the government to do so. In Hong Kong, the government controls personal data access through enacted laws, in particular, PDPO (Cap. 486) entrusts the government or its agencies such as the Office of the Privacy Commissioner the responsibility of protecting, monitoring and regulating access or use of citizens' data. In addition, it creates means or procedures through which an individual can access or amend their personal data. Under the Ordinance's Article 18 – it stipulates the procedures followed to request/access any such data by any individual, thus evidencing the importance of individual citizens' responsibility in data regulation processes.

What about trusting the government vs. the private sector with their data? Its proper use by private companies enhances client needs whereas the same data is vital in enabling the government to easily allocate resources aimed at improving its citizens' socio-economic status and livelihoods in general. Interestingly, the findings show that Hong Kong citizens trust private companies a little more to use their personal data appropriately when compared to the government (see Figure 7).

Figure 7: Trust in Appropriate Data Use



Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

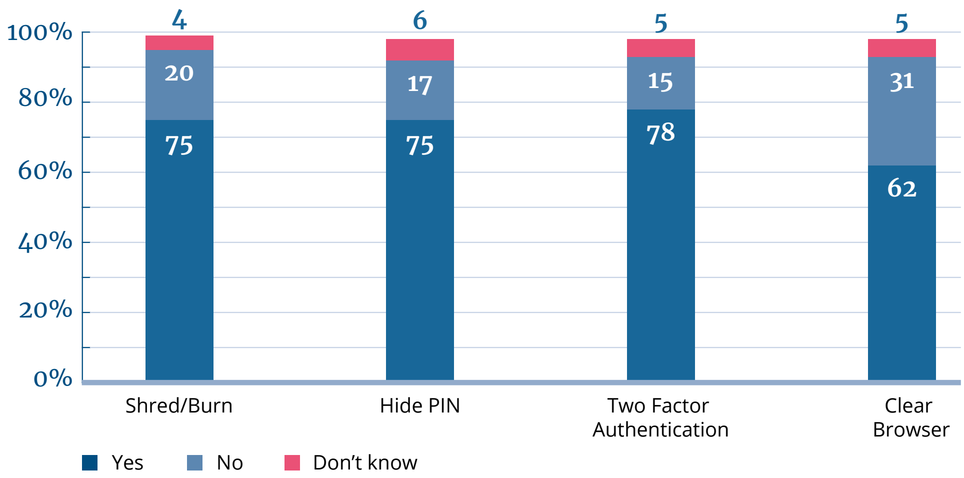
With a combination of the importance of data and concerned consumers, it is evident that "businesses need to work within the rules", according to a journalist. Data governance is a real and serious issue and companies cannot freely harvest whatever data they want, especially with increasingly vigilant consumers. In a recent presentation at the Fintech Fair in November 2020, Yi Gang, Governor of the People's Bank of China, noted "consumer privacy protection and firms' commercial secret protection" as the biggest concerns in the field of fintech. The driving forces of government rules and pressure for protection from consumers can nudge companies to react in order to maintain market competitiveness. In circumstances where regulations or public perception mean that certain practices become socially unacceptable, companies will have to be more creative in how they collect data and create value from it.

Stronger Hong Kong Government involvement may be an appropriate response to satisfy both privacy and business concerns. In a recent speech by Paul Chan Mo-po, Financial Secretary of Hong Kong, it was made clear that "enabling a robust regulatory environment is essential if fintech is to flourish." If governance and supervision of data protection is good enough, individuals consequently feel safer and more confident to provide their personal data to firms and service providers, which in turn leads to great benefits for businesses. A notable developing initiative by the HKMA is the establishment of the Commercial Data Interchange, or CDI. The CDI provides a rigorously regulated framework, rooted in user consent, for data to be more freely transferred.

Eddie Yue, Chief Executive of the HKMA announced that the "secure transfer of data is a priority" for the project. The initiative aims to establish a consent-based common standard for data owners and addresses inefficiencies in the status quo regarding the sharing and transfer of data in Hong Kong. Ultimately, individuals can make complaints about companies' duties of enterprise social responsibility to their community, however, the primary driving force should be the local rule of law enforced by the government, and also individuals taking precautionary measures in ensuring their personal data is protected. As aforementioned, over 40% of our respondents apportioned data protection responsibility to the government compared to the 12% that entrusted the responsibility to companies.

Our survey findings show that most Hong Kong residents take active steps to protect their personal data. Although clearing of browser histories is the least practiced data protection form in Hong Kong, over 75% of Hong Kong practice a two-factor-authentication, hide their personal identification numbers (PIN) and shred or burn personal documents (See Figure 8).

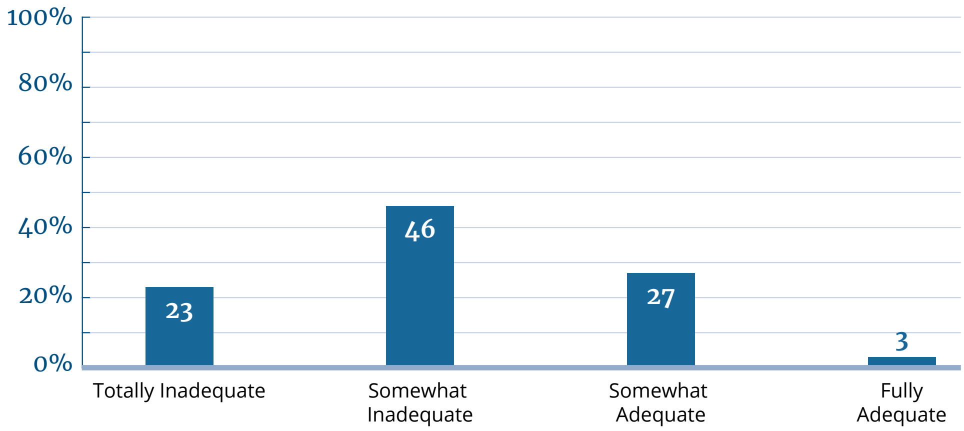
Figure 8: Data Protection Practices in Hong Kong



Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents, 1.9% missing not shown.

Nonetheless, data regulation in Hong Kong continues to generate debates despite having the Office of the Privacy Commissioner for Personal Data which has played a positive role in dealing with current data privacy issues. To further nurture innovation, government officials could look at how other jurisdictions are approaching the matter of data protection. Hong Kong could also enhance its data culture by putting more resources into data education. With a focus on explaining these fundamental issues, the mishandling of data may be more effectively dealt with than with the usual financial threats of large fines. This will enable Hong Kong to amend its data protection related regulations so as to enhance citizens' confidence in the adequacy of regulations, given that 69% of the surveyed respondents acknowledged that existing regulations were inadequate or somewhat inadequate (Figure 9).

Figure 9: Personal Data Privacy and Security Regulation in Hong Kong



Source: Survey by Rakuten Insight for City University of HongKong. 1,170 respondents.

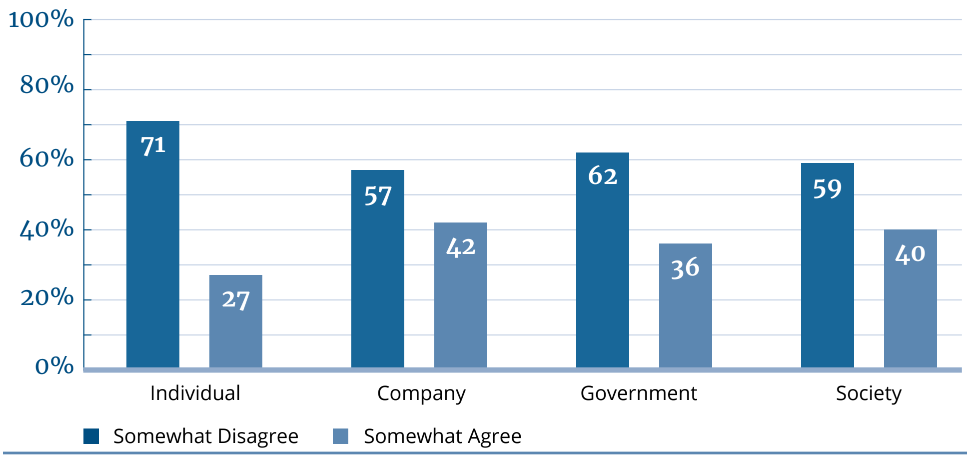
Part C: Data and Value Creation

It is undeniable that data is an increasingly important resource for financial companies. For example, Eddie Yue, Chief Executive of the HKMA, recently remarked that "data will be vital to the future of banking." Further, organisations that are able to take advantage of their data create a multitude of benefits, not only at an internal level but also potentially for a wider society. On an individual level, convenience is a key advantage. In the context of online shopping on e-commerce websites, user preferences are inferred based on pre-existing searches and other interactions with the platform. The processing of this data leads the right items to be recommended, saving time and money for the consumer.

The usefulness of shared or collected data has generated debates among different stakeholders – individuals, companies, government and civil society. In Hong Kong, only 42% of the surveyed respondents agreed companies that collected data about consumers were able to make appropriate offers to their customers compared to 36% agreeing the same when the government is concerned (Figure 10).

> The usefulness of shared or collected data has generated debates among different stakeholders – individuals, companies, government and civil society.

Figure 10: Citizens' Perceptions on Data Usefulness to Stakeholders



Source: Survey by Rakuten Insight for City University of Hong Kong. 1,170 respondents.

A legal scholar argues that when looking at a broader picture of our highly globalised and interconnected world, companies that successfully process and analyse cross-border transfers of data are able to better integrate different geographical markets. Cross-border data flows continue to grow, and overall, the ability to leverage data has positive results with respect to business efficiency and cross-border trade.

One of our interviewees, a senior civil servant working on the fintech industry promotion in Hong Kong, emphasized that a new breed of financial intermediaries, powered by large consumer datasets could level the playing field for many young people and startup companies that do not have extensive credit histories and are therefore at a disadvantaged position when it comes to obtaining loans and financial guarantees. By virtue of knowing their customers better than traditional banks, fintech companies would be able to better manage the risks, while providing an improved customer experience.

From the perspective of major international companies that put a large emphasis on analyzing the data that they collect, data can be a major source of competitive advantage. For example, by leveraging large-scale data analysis, international retail giants can understand consumer trends in individual countries better than smaller local businesses in those countries who might not have access to the breadth of data, let alone the analytic capability. The company with the benefits of consumer data therefore accrues a significant first movers' advantage. When asked about the influx of data available in the last few years (sometimes referred to as the "data explosion"), an economist expressed that the surge of data "is a huge goldmine…to be exploited."

For example, by leveraging large-scale data analysis, international retail giants can understand consumer trends in individual countries better than smaller local businesses in those countries who might not have access to the breadth of data, let alone the analytic capability.

A potential barrier to digital trade and cross-border data flows is the trend of data localisation – the idea of countries preferring to store data locally, as opposed to freely sharing in a global capacity. In conversation with a blockchain expert, it was emphasized that this is “a growing trend in recent years”, in which governments prohibit local companies from sharing data with foreign countries on the basis of protecting national security. Although this may be a valid concern, it is important to strike a reasonable balance between governments and companies that commercialise the use of data to maintain business efficiency.

> A potential barrier to digital trade and cross-border data flows is the trend of data localisation – the idea of countries preferring to store data locally, as opposed to freely sharing in a global capacity.

Considering a framework like the GDPR, constraints are placed on the use of data and transmission across different countries, which may affect the aforementioned aspects of consumer convenience and business efficiency. Ultimately, there is a challenging balancing act between the protection of fundamental rights with the growth of businesses. This legislation leans more towards for former, with emphasis placed on individual privacy. As it is still a new law, scientific-base empirical data is necessary to more accurately describe how effective the framework is.

In summary, this study provides one of the first evidence-based analyses of the role of the data in the emerging fintech ecosystem in Hong Kong. Over the decades, with its unique advantages as a special administrative region, Hong Kong has been successfully maintaining its status as the Asia's premier financial center. While personal data is generally well-protected under the existing legal and regulatory frameworks, the Government maintains a pro-business stance and encourages new modes of data utilization, including offering companies a regulated "sandbox" for testing their products and services by using data innovation models. These measures help fintech startups to grow and attract global talents to develop their ideas in Hong Kong.

In addition, regarding the data protection laws, Hong Kong residents, although not necessarily satisfied with the existing laws and mechanisms, assign a significant portion of responsibility to individuals, who they believe should decide on whether they want to share their personal data or not. This shows that Hong Kong residents are generally aware of their data rights. Although the study shows that people trust the private sectors slightly more than the government in terms of appropriate data usage, most of the people are still sceptical and concern about how their data being used. On the other hand, the interviewed experts generally pointed out that greater clarity is needed when it comes to definitions of personal data and its uses in the existing law framework, while suggesting that the Government should maintain a neutral stance when it comes to future regulation of data protection. As people are getting more concerned about protecting their privacy and data rights, it is becoming more challenging for the Hong Kong government to balance the interest of the public and private companies when introducing new regulations.

Given the tightening of data protection laws and practices as applied to fintech organizations in Mainland China as reflected by the case of Ant Group's cancelled IPO, it is likely that spillover effects will be seen in Hong Kong in the near future, particularly as many China-based fintech companies decide to proceed with their IPOs on the Hong Kong Stock Exchange. Surely the effect of the tightening rules will be observed closely by investors and global companies, as it can pose an impact on the willingness of foreign investment and ultimately the status of Hong Kong as an international financial hub.

> Surely the effect of the tightening rules will be observed closely by investors and global companies, as it can pose an impact on the willingness of foreign investment and ultimately the status of Hong Kong as an international financial hub.

A **Arner, D., & Barberis, J.** (2015, March 26). FinTech and Regulation: Recent Developments and Outlook. Retrieved from https://www.slideshare.net/FinTechHk/FinTech-regulation-by.

B **Aryan, A.** (2020, November 06). Explained: What is the Ant Group, and why is their IPO suspended? Retrieved from https://indianexpress.com/article/explained/explained-what-is-the-ant-group-why-is-their-ipo-suspended-6943919/.

C **Calhoun, G.** (2020, November 22). Why China Stopped The Ant Groups IPO (Part 2): Ants Dangerous Business Model. Retrieved from https://www.forbes.com/sites/georgecalhoun/2020/11/16/why-china-stopped-the-ant-groups-ipopart-2-ants-dangerous-business-model/?sh=2b4bc05358bf.

Census and Statistics Department (2021). Population – Overview: Census and Statistics Department. Retrieved from https://www.censtatd.gov.hk/hkstat/sub/so20.jsp.

Cho, Y. (2020, November 02). How AI and vast data support Ant Groups financial empire. Retrieved from https://asia.nikkei.com/Business/Finance/How-AI-and-vast-data-support-Ant-Group-s-financial-empire.

Community Legal Information Centre (2020, February 26). The meaning of "personal data" and the six data protection principles. Retrieved from https://www.clic.org.hk/en/topics/personalDataPrivacy/6_data_protection_principles.

E **Education Bureau** (2020). Facts and Figures. Retrieved from https://www.studyinhongkong.edu.hk/en/why-hong-kong/facts-and-figures.php.

I **InvestHK** (2019). Why Hong Kong. Retrieved from https://www.investhk.gov.hk/en/why-hong-kong.html.

K **Koo, C., & Chung, A.** (2020, March 30). Reform to Hong Kongs data protection law finally on the horizon. Watch this space! Retrieved from https://www.lexology.com/library/detail.aspx?g=a2aa3c58-4621-48ae-a181-5b3a4939ebb2.

P **Personal Data Protection Act Art 2, The Personal Data Protection Act of the National Development Council of Taiwan** (2015).

Pham, S. (2020, November 04). Analysis: Beijing just yanked Ant Group's IPO to show Jack Ma who's really in charge. Retrieved from https://edition.cnn.com/2020/11/04/tech/ant-ipo-beijing-china-intl-hnk/index.html.

Privacy Commissioner for Personal Data (2020, August). *Guidance on Collection and Use of Biometric Data* (Hong Kong, Privacy Commissioner for Personal Data). Retrieved from https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf.

S **SCMP Research** (2020). *China Fintech Report 2020* (Publication). Hong Kong: SCMP Research.

T **The Personal Data (Privacy) Ordinance, Cap 486, Laws of Hong Kong** (2012).
Understanding Patient Data. (2018, May 25). Why an opt-out rather than an opt-in or consent? Retrieved from https://understandingpatientdata.org.uk/news/why-an-opt-out.

W **WHub** (2019). *Hong Kong FinTech White Paper 2019* (Vol. 3.1, Rep.). Hong Kong. Retrieved from https://www.whub.io/fintech-toolbox-download.

Sample of Questions

Semi-structured interviews were conducted with questions broadly aligned with three themes:

1. How the regulation of data affects innovative capacities
2. Data cultures, or perceptions around data and innovation
3. How data creates value or values

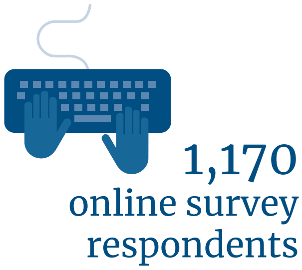
A sample of questions for each theme follows:

Regulation	• To what extent do you think the laws and regulations around data protection have been helping or hindering the innovation capabilities of firms and organizations? • Do you see the legal landscape, as in the laws and regulations in specific, or the legal framework, changing in the next few years? • How can the current laws and regulations, including the legal framework, be improved so that the innovation capabilities of organizations can be further enhanced?
Data Cultures	• How is personal data seen in Hong Kong? For example, do people see it as something that they need to protect? Or as byproducts of economic transactions? • How might perceptions of personal data and privacy have an impact on innovation? For example, what types of data would be considered taboo to share, and in what contexts?
Data and Value Creation	• What do you think is the value that organizations bring when they are successful in managing their data, including analysing, storing, protecting, and sharing their data? • How do you think frameworks like the GDPR affect domestic and trans-border operations, and to what extent do you think a similar framework would be feasible in Hong Kong?

Methodology

This study was conducted using a triangulation of four different methods: semi-structured interviews, desk research, attendance of Hong Kong FinTech Week 2021, and finally an online survey of Hong Kong residents conducted by a reputable market research firm.

10 interviews were conducted with members of the public and private sectors, with different areas of expertise such as fintech, cyber security, enterprise blockchain, law, and policy. All of the interviews were conducted through online video conference calls due to pandemic restrictions. Interview questions were modified based on the expertise of each interviewee, but largely focused on three major concerns: collection and use of data and how they affect innovation capacity, perceptions around data and innovation, and data and value creation. A total of 1,170 respondents across Hong Kong took part in the online survey conducted by Rakuten Insight from February 4–21, 2021. The survey respondents were selected via a proprietary online panel and are broadly representative of the Hong Kong general population.



Relevant documents such as whitepapers, news, and reports were gathered according to themes such as values associated with data, data governance principles, and partnerships in data sharing. We also attended the Hong Kong FinTech Week 2021, featuring a series of fintech talks and seminars that brings the latest insights from various stakeholders and explores how fintech can further impact financial services and society.

AUTHORS

Marko M. Skoric is an Associate Professor at the Department of Media and Communication, City University of Hong Kong. His research interests are focused on new media and social change, with a particular emphasis on the civic and political implications of new communication technologies.

Chun Hong Tse is a Research Assistant at the Department of Media and Communication, City University of Hong Kong. His research interests are focused on journalism with a particular emphasis on citizen journalism, computer-mediated communication and political communication.

Jeremy Pui is a Law LLB Student at King's College London. His research interests are focused on blockchain, legal technology, and consumer protection.

Juma Kasadha is a postdoctoral fellow at the Department of Media and Communication, City University of Hong Kong. His research interests are new media technologies and social change with a particular emphasis on citizen political engagement, and civic and political implications of new media technologies in sub-Saharan Africa.

Editors
Christian Echle
Director Regional Programme
Political Dialoge Asia
christian.echle@kas.de

Ming Yin Ho
Programme Manager for Digital Transformation
mingyin.ho@kas.de

Konrad-Adenauer-Stiftung e. V.
Regional Programme
Political Dialogue Asia
Arc 380
380 Jalan Besar, #11-01
Singapore 209000
www.kas.de/singapore

Imprint

Published by:
Konrad Adenauer Stiftung Regional Programme
Political Dialogue Asia, Singapore, 2021

Design and typesetting: yellow too Pasiek Horntrich GbR
Pattern: iStock by Getty Images/lasagnaforone

Printed with financial support from the German Federal Government.

ISBN 978-981-18-4822-3

Data fuels digital change. The ability to collect, process, and make available ever-increasing amounts of data is a key to innovation and growth.

This report is one of the series surveying seven different Asian territories to deepen understandings of innovation and data policies, and contribute to debates about data governance and data protection. The study was carried out in collaboration with the National University of Singapore (NUS). We selected Hong Kong SAR, India, Japan, the People's Republic of China, Singapore, South Korea, and Taiwan as the contexts to be examined. We looked at the areas of transport, finance, administration, health and smart cities to understand how innovation is driven in the context of relationships among key stakeholders such as citizens, civil societies, government agencies, private sectors and research institutions.

This report describes and analyses one of the key fields of the data innovation landscape in Hong Kong – the emerging financial technology (fintech) industry, through the lens of innovation and data policies, as well as citizens attitudes towards data sharing.

Konrad-Adenauer-Stiftung e. V.

DATA AND
INNOVATION
IN ASIA-PACIFIC