BÁNKI KÖZLEMÉNYEK --- BÁNKI REPORTS
VII. ÉVFOLYAM 2. SZÁM --- VOLUME VII NO. 2

Regulatory environment for IoT in Hong Kong

Az IoT szabályozási környezete Hongkongban

Gellért Miklós

Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary
gellert.miklos@gmail.com

Abstract — **Governments and regulators around the world have realized the potential benefits of a digital economy and are now developing a regulatory environment that incentivizes IoT (Internet of Things) device manufacturers and service providers to enter the market, while also supporting the adoption of these solutions by the economy. Although IoT undoubtedly leads to increased efficiency, reduced waste, and smarter ways of working, it also introduces heightened data privacy and cybersecurity risks. Hong Kong is one of the leading regions in the development of the digital economy and the adoption of IoT technologies. A new IoT code of practice has been released to increase data security awareness among end users while also raising the security level of the IoT devices entering the market. This paper aims to provide an overview of the code of practice, the most relevant privacy provisions, and the dedicated wireless IoT licensing regime developed by the regulatory authority.**

Keywords: IoT, Hong Kong, data security, data privacy, code of practice

Összefoglalás — **A kormányok és a szabályozó hatóságok világszerte felismerték a digitális gazdaság potenciális előnyeit, és jelenleg olyan szabályozási környezetet alakítanak ki, amely piacra lépésre ösztönzi az IoT- (*Internet of Things*-) eszközök gyártóit és szolgáltatóit, továbbá támogatja a gazdaságot ezen megoldások alkalmazásában. Az IoT nagyobb hatékonyságot, kevesebb hulladékot és intelligensebb munkamódszereket eredményez, ugyanakkor megnövekedett adatvédelmi és kiberbiztonsági kockázatokhoz vezet. Hongkong az egyik vezető régió a digitális gazdaság fejlesztésében és az IoT-technológia átvételében. Új IoT gyakorlati kódex jelent meg, amely növeli a végfelhasználók adatbiztonsági tudatosságát, miközben a piacra kerülő IoT-eszközök biztonsági szintjét is emeli. A jelen írás célja, hogy áttekintést nyújtson a gyakorlati kódexről, a legfontosabb adatvédelmi rendelkezésekről és a szabályozó hatóság által kidolgozott vezeték nélküli IoT-engedélyezési rendszerről.**

Kulcsszavak: IoT, Hongkong, adatbiztonság, adatvédelem, gyakorlati kódex

1 INTRODUCTION

IoT devices are generally used for automated machine-to-machine (M2M) communications. With new wireless technologies such as the fifth-generation (“5G”) mobile technologies and new IoT applications, such as smart cities, precision agriculture, and autonomous vehicles, continuously being developed, it is expected that in Hong Kong a large number of IoT devices will connect to the public telecommunications networks in the near future. The list of potential use cases includes mission-critical applications that are fundamental to the functioning of society and economy. This proliferation of IoT devices and the processing of vast amounts of data by IoT devices has brought new challenges for data protection and security. In 2019, Hong Kong issued a Code of Practice (CoP) for IoT to ensure that IoT networks and applications are protected against emerging new security threats.

2 IOT CODE OF PRACTICE

The CoP is a dedicated, voluntary collection of best practices and measures addressed to IoT device manufacturers and service providers to ensure the provision of satisfactory service, strengthen consumer protection, and enhance user confidence in the use of IoT devices. Licensed telecommunications service providers offering communications services and platforms forIoT devices are required to provide a high-quaility, efficient, and continuous service as required by the Communications Authority (CA), the telecommunications regulatory authority of Hong Kong. In the code of practice, the CA has identified four challenges related to the increasing number of IoT devices connected to networks: (a) privacy, (b) identity, (c) security, and (d) availability. Privacy risk refers to a risk of end-user personal data being unlawfully processed, which may cause harm for individual end-users or their families. Identity-related challenges pertain to the ability to authenticate IoT devices, services and the end-user operating thems. From a security perspective, the challenge is to ensure the system integrity of IoT devices to prevent and withstand cyber-attacks while the associated data can be verified, tracked, and monitored. The availability risk means a risk to the uninterrupted connectivity between the IoT devices and services.

The measures and best practices listed in the CoP address these identified challenges. Although voluntary, IoT device manufacturers and IoT service providers are encouraged to implement as many of the measures as possible when entering the Hong Kong market. Additionally, the CoP encourages device manufacturers and vendors to study the referenced documents when developing their own operational and management policies. The referenced documents include guidelines, and policies issued by governments, industry associations and nonprofit organizations. [1]

The CoP recommends that only those manufacturers of IoT devices may deploy IoT devices in Hong Kong who implement appropriate security policies and resilient measures. In this context, resiliency means that IoT devices are designed in such a way that they are able to run independently, securely, and safely with basic functions even in the event of a failure of IoT platform or network connection loss. These documents should be complemented with a suitable testing process to verify the functions and features of the devices. Security should also include data security.

One of the basic security measures is to implement unique usernames and strong passwords for IoT devices. Usually, the industry standard is to use generic usernames and passwords, which can be changed later by the end-user. However, this poses the risk of the device being restored to factory default settings, thereby enabling access to it using default credentials. For this reason, it is not recommended using IoT devices with hard-coded usernames and passwords in their software. As an additional measure, multi-factor authentication – namely,, using an electronic token in addition to a username and password – and identity management technology, including SIM card, are also recommended to increase security.

Usernames and passwords, personal data, and device identifiers should also be stored securely, encrypted on the IoT device to prevents unauthorized access or modification by third parties. If such data needs to be transmitted over the network, it is recommended to apply end-to-end encryption. Further security measures should include, if possible, anti-virus, anti-malware, network firewalls, and access control lists.

Usernames and passwords may be considered as personal data, just as much of the data gathered by IoT devices in certain cases including smart watches, smart cameras. Manufacturers should comply with the data protection requirements and should also ensure that personal data can be permanently erased from devices by the end-user. This is especially important in case of a transfer of ownership or disposal of IoT devices. The devices and applications should process personal data in compliance with the local data protection regulations, and users should be informed about how their data will be used for each IoT device.

Users should have the option to delete any personal data permanently from the devices. According to the CoP, manufacturers should configure the security and privacy settings of IoT devices to the highest possible level by default. Users should only be provided with the minimum set of rights necessary for operating IoT devices. This minimizes the risk of users unknowingly modifying the settings, making it easier for third parties to compromise the devices. The recommendation is that only essential network interfaces should be open for access, while other parts, such as camera, loudspeaker, and microphone, should be enabled only when in use.

Software updates may open up new possible threat vectors for malicious third parties to gain access to an IoT device and the data stored. For this reason, it is recommended that users should be notified in advance of the need for an update and that IoT devices should be updated as soon as possible in a way that does not impact the functioning of the device. At the end of the device lifecycle, when the IoT devices are no longer updatable, they should be replaced. Software integrity verification is a measure that also helps to defend against malicious attacks. If during the verification process any unauthorized change is found, then the device should be able to alert users and disconnect from any network automatically. This may prevent further access to network elements.

Depending on the use case, IoT devices may have sensors to measure specific values, such as temperature, humidity, brightness, or time, and then execute actions depending on those measurements. For example, a smart thermostat automatically regulating temperature and activating the heating system when the temperature reaches a certain value. IoT device manufacturers should develop devices in such a way that enables devices to validate formats, types, and values of data from any source including data entered by users, collected by the devices themselves or transmitted via the network. If any anomalies are detected, the devices should be able to initiate appropriate mitigating measures. Taking the example of the smart thermostat, a malicious third-party gaining access to the device would be able to control the thermostat and set the temperature to values so high or low that it may cause physical harm, system damage or financial loss for the owners of the devices.

Bug reporting is an important measure to fix any zero-day vulnerabilities and develop timely bug fixes. For this reason, the CoP recommends that manufacturers and operators should maintain a point of contact where users can report security issues and bugs to minimize the security risks. In case the information is reported to the vendors, it should be shared with the manufacturers or operators of the device. The CoP also recognizes that secure devices are necessary, but not sufficient, and users should be educated as well. Adequate guidance should be provided and made available on the installation, configuration, and use of IoT devices. Manufacturers and operators should also share best practices for users to follow.

IoT devices usually serve a function in a wider system, therefore ensuring the security of the network and its elements is not a single action done upon installation, but an ongoing process. The CoP recommends that operators of IoT devices to frequently conduct assessment of potential risks on the relevant risks arising from device operation. In Annex B, the CoP also provides a template checklist for providers of IoT devices to help with the risk assessment. [1] In December 2022, the Telecommunications Regulatory Affairs Advisory Committee (TRACC) proposed an update to the CoP. The update – although still voluntary for providers of IoT – aims to improve the security of IoT services and devices. Based on the update, IoT providers should conduct regular assessments of compliance with best practices published by the CA as part of Annex C, as well as risk assessment based on Section 5 and Annex B of the CoP. IoT device manufacturers and service providers should submit the relevant information and documents to the CA every year. To encourage compliance, the CA will publish the names of those operators that have conducted the compliance check and made a risk assessment on thematic webpage of the CA for public information [2].

3 Data privacy

Data privacy in Hong Kong is regulated by the Personal Data (Privacy) Ordinance (PDPO) and the Data Protection Principles (DPPs). The PDPO is one of the longest-standing data protection laws in Asia, which took effect in December 1996. It was inspired by the OECD Privacy Guidelines and was amended in 2012 and 2021. The PDPO is the data privacy law in effect in Hong Kong, therefore it applies to both the private and the public sectors.

Under the PDPO, the DPPs set the framework for data users on how personal data should be collected, processed, and stored. The DPPs are listed in Schedule 1 of the PDPO, and there are six of them. In addition to the PDPO and the DPPs, the Privacy Commissioner has released several guidance notes to guide data users on lawful personal data processing. Although there are guidance notes on various topics, there is no dedicated guidance note on IoT. This means that manufacturers and providers of IoT services need to follow the general principles and requirements set out by the PDPO. To help data users with compliance, the Privacy Commissioner has released the Privacy Management Programme, a framework aimed to develop a privacy infrastructure with a monitoring and reporting process. The recommendations are similar to the mandatory requirements set by the European General Data Protection Regulation (GDPR) as they also include the nomination of a Data Protection Officer, the development of personal data processing policies and data breach notification procedures.

The main difference is that while the GDPR is mandatory, adherence to the Privacy Management Programme is entirely voluntary for data users [4]. This does not mean, however, that data users are not liable for the processing of personal data. In an increasingly digitized world, data is rarely retained within a single country. Data users may contract with other data users or employ data processors located outside Hong Kong; however section 33 of the PDPO imposes restrictions on cross-border data transfer, unless the transfer is exempted by law or the data subject has previously consented to such transfer.

One way for any IoT device manufacturer or service provider to comply with cross-border data transfer restrictions is to include Recommended Model Contractual Clauses (MMCs) in the contracts. The MCCs are developed by the Privacy Commissioner and are shared in a guide with the general public. [5] The clauses are drafted for free use in any contract between two parties. Outsourcing data processing by data users has become common practice across all industries, including IoT.

This means that if a data user contracts with a data processor for processing personal data – including collection, storage, usage, and so forth. – outside Hong Kong then the IoT manufacturer or service provider, as a data user, must adopt contractual or other measures to ensure that the data is kept only as long as it is necessary for the purpose of the processing (under DPP2(3)) and prevent unauthorized or accidental access (under DPP4(2)). Similar to the liability established by the GDPR, under the PDPO the data user is liable for any act committed by the data processor.

4 Data Security

Cyber threats are among the main threats to the IoT industry. For regulators, IoT manufacturers, and IoT service providers data security is a top priority and main concern. The reason is that IoT devices are used in various industries and use cases, besides it gathers a wide range of data. Any unauthorized access to the data through hacking, malware, or data breaches may have severe consequences for end users. Consequences may include monetary loss, reputational damage, physical harm, or even death.

DPP4 of the PDPO requires all data users to take all practicable steps to ensure that any personal data held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use [6].

In practice, this means that if an IoT manufacturer or service provider, as a data user, enters into a data processing relationship with a data processor, such as a cloud service, platform, or analytics provider, the data user must ensure the security of the data. Under Section 65(2) of the PDPO a data user is liable for any data processor engaged as an agent. Therefore, data users should ensure that the data processors and any other data users comply with the PDPO and apply robust and resilient security measures to protect the personal data processed.

The Privacy Commissioner is responsible for the enforcement of the requirements. If the Commissioner receives a complaint or has reasonable grounds to suspect a contravention of PDPO, the Commissioner may conduct an investigation of the suspected contravention and publish a report setting out the investigation results and recommendations, if it is in the public interest [7]. The Commissioner may issue an enforcement notice to the data user, directing remedial or preventive steps to be taken. Contravention of an enforcement notice issued by the Commissioner is also an offence, which may result in fines or imprisonment. The possible penalties for disclosure of personal data without consent can reach HK$1,000,000 or five years imprisonment. End-users who suffer loss or damage because of a data breach are also entitled to pursue civil claims.

5 Licensing

For a functioning IoT market not only device manufacturers and service providers are needed, but also telecommunications operators that maintain the necessary network infrastructure. The Office of the Communications Authority (OFCA) developed a new licensing regime for the Wireless Internet of Things (WIoT) services on 1 December 2017, allowing telecommunications service operators to provide platforms and services for IoT using the shared frequency band of 920–925 MHz.

This type of IoT license is subject to less stringent regulatory control and lower license fees to encourage the growth of the IoT market and to incentivize telecommunications operators to provide IoT services. Under the WIoT License, licensees are entitled to establish, maintain, and operate wireless networks and systems for the provision of wireless IoT services in Hong Kong, based on wireless technologies operating in the 920–925 MHz band [8].

This frequency band is an unlicensed frequency band used by various low-power, wide-area network (LPWAN) technologies. For cellular connectivity-based IoT solutions, an operator requires a different type of license to provide the necessary network and connectivity services that enable the communication between IoT devices.

The WIoT license allows the licensees to provide wireless data communications services for automated data-only machine-to-machine communications between network elements and IoT devices. M2M communications are defined as communications between machines or devices in which data can be exchanged in an automatic or scheduled manner with little or no human intervention [9]. The license does not permit the provision of any services that allows real-time voice communications or any other service that is subject to separate licensing requirements.

6 Conclusion

The Internet of Things (IoT) is becoming ubiquitous, transforming industries, improving efficiency, and offering new ways of working. Adopters of IoT technology may gain advantages over the competition and, as a result, an increasing number of countries are developing regulatory frameworks to foster development and incentivize the implementation of IoT solutions. However, besides clear advantages, there are also significant risks associated with IoT. The main risks include cyber security and data privacy. Governments and regulators are issuing frameworks, guides, and codes of practices to shape and guide the market.

The code of practice issued by the OFCA serves the same purpose. It serves to guide IoT manufacturers and service providers while protecting end users and enhancing data security and awareness. The collection of best practices and recommendations may increase the security of devices and their users. However, the voluntary nature of the document may limit its effectiveness. Moreover, as additional countries and regions develop similar documents and frameworks with varying requirements, this results in increased complexity and cost to market entry, ultimately raising the prices of the IoT devices and services leading to slower adoption and digitalization.

References

[1] "Code of Practice on the Operation and Management of Internet of Things Devices", Office of the Communications Authority, Hong Kong, China, Issue 2, April 2023, available here: https://www.coms-auth.hk/filemanager/statement/en/upload/619/cop-iot_e.pdf

[2] Proposed Update of the "Security Guidelines for Next Generation Networks" and "Code of Practice on the Operation and Management of Internet of Things Devices", Telecommunications Regulatory Affairs Advisory Committee, Hong Kong, China, TRAAC Paper No. 4/2022, 19 December 2022, available here: https://www.ofca.gov.hk/filemanager/ofca/en/content_757/traac4_2022.pdf

[3] Privacy Protection and Data Governance in the Internet of Things, Hong Kong Academy of Law, Office of the Privacy Commissioner for Personal Data, Hong Kong, China, 5 June 2019, available here: https://www.pcpd.org.hk/english/news_events/speech/files/AcademyofLaw_0605.pdf

[4] Privacy Management Programme – A Best Practice Guide, Privacy Commissioner for Personal Data, Hong Kong, China, March 2019, available here: https://www.pcpd.org.hk/english/publications/files/PMP_guide_e.pdf

[5] Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data, Privacy Commissioner for Personal Data, Hong Kong, China, May 2022, available here: https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_model_contractual_clauses.pdf

[6] Personal Data (Privacy) Ordinance, Hong Kong, China, accessible here: https://www.elegislation.gov.hk/hk/cap486?xpid=ID_1438403261084_001

[7] Office of the Privacy Commissioner for Personal Data, Hong Kong, China, accessible here: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

[8] Guidelines for Submission of Applications for Wireless Internet of Things Licence, Office of the Communications Authority, Hong Kong, China, Issue 2, 29 June 2021, available here: https://www.coms-auth.hk/filemanager/statement/en/upload/566/gn132021.pdf

[9] Numbering Arrangement for Machine-to-Machine Communications, Telecommunications Regulatory Affairs Advisory Committee, Hong Kong, China, 20 November 2014, available here: https://www.ofca.gov.hk/filemanager/ofca/en/content_757/traac5_2014.pdf