

Hong Kong Transparency Report 2018

Executive Summary

(Read the full report: transparency.jmsc.hku.hk)

1. Communications surveillance and transparency in the digital age

➤ **Background**

- Edward Snowden's global surveillance disclosure of the massive US spy programme in 2013 has prompted many jurisdictions to introduce legislations or amendments on communications surveillance, contributing to better transparency.
- In 2016, the Hong Kong government refused to expand the scope of surveillance regulation to cover the access to user data and stored communications.
- HKTR conducted a survey on the matter in South Korea, Taiwan, Australia, the UK and the US, with the hope that their experiences could shed light on potential solutions for Hong Kong.

➤ **Findings**

- 1) The Interception of Communications and Surveillance Ordinance (Cap.589) fails to regulate access to user data in cyberspace by law enforcement agencies.
- The ICSSO, enacted in 2006, only regulates real-time surveillance including the interception of telecommunications and postal mails. However, surveillance laws in other jurisdictions also regulate access to communications, metadata and personal information (user data) that have been stored in electronic devices.

Definition:

- 1) "Interception" refers to the action of monitoring or recording private conversations in the course of transmission;
- 2) "Stored communications" refers to the contents of communications that are stored in service providers' servers or users' personal devices;
- 3) "Metadata" refers to business records produced and maintained by service providers (e.g., phone numbers of both senders and receivers, time and dates, locations);
- 4) "Personal information" is also referred to as "subscriber information", which describes personal identification (e.g., names, ID numbers, residential addresses);
- 5) "Metadata" and "personal information" may be collectively referred to as "user data".

- *Warrant requirement*

	Hong Kong	South Korea	Taiwan	Australia	UK	US
<i>Interception</i>	✓	✓	✓	✓	✓	✓
<i>Stored communications</i>	✓	✓	✓	✓	✓	✓
<i>Metadata</i>	✗	✓	✓	○	○	✓
<i>Personal information</i>	✗	○	○	○	○	○

○: No warrant required but detailed guidance to law enforcement agencies is available

In Hong Kong, if law enforcement agencies (LEAs) issue requests to ICT companies for their clients' data, the LEAs are not obliged to obtain a warrant in advance. There is no publicly available guideline detailing the procedures for such requests.

Some jurisdictions require a warrant to access metadata or personal information while some other do not. However, they all make guidance or codes of practice publicly available.

2) There is a lack of transparency in electronic communications surveillance: neither guidance to law enforcement agencies, nor routine disclosure to the public.

- *Routine disclosure*

	Hong Kong	South Korea	Taiwan	Australia	UK	US
<i>Interception</i>	○	✓	✓	✓	✓	✓
<i>Stored communications</i>	✗	✗	✓	✓	✓	✓
<i>Metadata</i>	✗	✓	✓	✓	✓	✓
<i>Personal information</i>	✗	✓	✗	✓	✓	○

○: Such information is not specified but contained in numbers of a higher categorical rank, e.g., the report in Hong Kong only mentions the number of judges' authorisations for interception but does not specify how many telecommunications or postal interceptions.

All six jurisdictions regularly disclose information about surveillance, including statistics and explanation of the mechanism in plain language. Both Taiwan and the US have publicly available data portals for disclosing relevant statistics.

In Hong Kong, the surveillance commissioner publishes numbers of interceptions conducted by LEAs every year, but the statistics does not include access to stored communications, metadata and user information.

➤ **Recommendations**

- Introduce legislation or amendments to the current surveillance law.

Article 30 of the Basic Law guarantees the “freedom and privacy of communication” as one of the citizens’ “fundamental rights”, and Article 29 protects Hong Kong residents from “arbitrary or unlawful search”. In the digital age, the Hong Kong government should introduce legislation or amendments to fulfil its obligation for protecting citizens’ privacy.

- Issue guidance to law enforcement agencies.
- Improve routine disclosure to increase transparency.

2. User data and content removal requests

➤ **User data requests**

- From 2011 to 2017, the HK government had issued an annual average of 4,470 user data requests to ICT companies. The number has reached the highest in 2013 (5,351), and come down to the lowest in 2017 (3,541).
- Eight international ICT companies have released statistics of user data requests from HK. The corporate data comprised 42% of all such requests made by the HK government since 2013. Their number has decreased from 1,722 in 1H2013 to 572 in 1H2017. The average compliance rate by the companies was 60%.
- The largest government requester was the Police (88%), and the major reason was for crime prevention and detection (99%).

➤ **Content removal requests**

- From 2011 to 2017, the HK government had issued an annual average of 355 requests to ICT companies. The number has reached the highest in 2013 (657), and come down ever since, except for a rebound from 2016 (194) to 2017 (336).
- The largest requester was the Department of Health (50%), and the major reason was to remove online content related to illegal sale of medicine (44%).

Appendix A: Government transparency reports

Hong Kong

Annual Report to the Chief Executive by the Commissioner on Interception of Communications and Surveillance, Commissioner on Interception of Communications and Surveillance

<http://www.info.gov.hk/info/sciocs/en/reports.htm>

South Korea

Status of communications confirmation data and provision of communications data etc. (상반기 통신자료 및 통신사실확인자료 제공 등 현황), Ministry of Science and ICT

(For 1H2017)

<http://www.msip.go.kr/web/msipContents/contentsView.do?catelId=mssw311&artId=1368236>

Taiwan

Annual statistics report on communications surveillance (《通訊監察統計年報》), Judicial Yuan

<http://www.judicial.gov.tw/juds/>

Cases of applications for interception warrants/access warrants (《通訊監察書/調取票聲請案件》), Ministry of Justice

http://www.rjtd.moj.gov.tw/rjtdweb/common/WebList3.aspx?menu=INF_COMMON_0

Australia

Telecommunications (Interception and Access) Act 1979 - Annual report, Attorney-General's Department

Surveillance Devices Act 2004 – Annual report, Attorney-General's Department

<https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/default.aspx>

The UK

Report of the Interception of Communications Commissioner: annual report, Interception of Communications Commissioner

(For 2016) <https://www.gov.uk/government/publications/report-of-the-interception-of-communications-commissioner-annual-report-2016>

Office of Surveillance Commissioners annual report, Office of Surveillance Commissioners

(For 2016) <https://www.gov.uk/government/publications/office-of-surveillance-commissioners-annual-report-2016>

Report of the Intelligence Services Commissioner, Intelligence Services Commissioner

(For 2016) <https://www.gov.uk/government/publications/report-of-the-intelligence-services-commissioner-for-2016>

(The three commissioners' reports will merge into one by the Investigatory Powers Commissioner established in 2017)

The US

Statistical transparency report regarding the use of national security authorities, Office of the Director of National Intelligence

(For 2016)

https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016

Appendix B: Questions raised by Legislative Council members on user data and content removal requests

Date	Question raised by (legislator)	Reply by (government official)	Reporting period	URL
6 February 2013	Charles Mok	Gregory So (Secretary for Commerce and Economic Development)	2010 – 2012 (aggregated numbers)	http://www.info.gov.hk/gia/general/201302/06/P201302060424.htm
19 February 2014	Charles Mok	Godfrey Leung (Acting Secretary for CED)	February 2013 – January 2014	http://www.info.gov.hk/gia/general/201402/19/P201402190281.htm
15 October 2014	James To	Gregory So	February – October 2014	http://www.info.gov.hk/gia/general/201410/15/P201410150422.htm
11 February 2015	Charles Mok	Gregory So	2011 – 2014 (annual)	http://www.info.gov.hk/gia/general/201502/11/P201502110755.htm
27 January 2016	Charles Mok	Nicholas W Yang (Secretary for Innovation and Technology)	2011 – 2015 (biannual)	http://www.info.gov.hk/gia/general/201601/27/P201601270385.htm
1 March 2017	Charles Mok	Nicholas W Yang	2015 – 2016 (biannual)	http://www.info.gov.hk/gia/general/201703/01/P2017030100385.htm
31 January 2018	Charles Mok	Nicholas W Yang	2017 (biannual)	http://www.info.gov.hk/gia/general/201801/31/P2018013100456.htm

Appendix C: ICT companies that release information about Hong Kong in their transparency reports

Company	Year of first release of transparency report	Year of first release of HK requests	Country where headquarters is located	Average annual number of requests	URL
Google	2010	2010	US	490	https://www.google.com/transparencyreport/userdatarequests/HK/
Microsoft	2012	2012	US	662	https://www.microsoft.com/en-us/about/corporate-responsibility/lerr
Twitter	2012	2013	US	1	https://transparency.twitter.com/
Yahoo (Oath)¹	2013	2013	US	960	https://transparency.oath.com/
Apple²	2013	2013	US	820	http://www.apple.com/hk/en/privacy/transparency-reports/
Facebook	2013	2013	US	62	https://transparency.facebook.com
Verizon	2013	2014	US	1	http://www.verizon.com/about/portal/transparency-report/international-report/
Line	2016	2016	Japan	1	https://linecorp.com/en/security/transparency/top

¹ Verizon acquired Yahoo in 2017, and the new holding company Oath started to release its transparency reports of 1H2017, which contained statistics of Yahoo, Tumblr, Aol, among others.

² The numbers from Apple include device requests. The vast majority of the requests Apple receive from law enforcement relate to information about lost or stolen devices. Device requests may also include requests for customer contact information provided to register a device with Apple or the date(s) the device used Apple services.

