

2018

HKTRANSPARENCY Report

香港資訊公開報告



February 2018

About the Hong Kong Transparency Report

The Hong Kong Transparency Report (HKTR) is a research and advocacy project hosted by the Journalism and Media Studies Centre of The University of Hong Kong. The project was launched in 2013 to document and monitor the Hong Kong government's practice of communications surveillance and content takedown in cyberspace. Through evidence-based reporting and research, HKTR seeks to promote transparency and to advance citizens' rights to privacy and freedom of expression.

Director

Keith Richburg

Academic Adviser

King-wa Fu

Project Manager

Benjamin Zhou

Authors

Benjamin Zhou

Tom Tsui

Special Thanks to

Korea University

Jiwon Sohn

Taiwan Association for Human Rights

Ming-hsuan Ho

The Chinese University of Hong Kong

Lokman Tsui

Office of the Hon Charles Mok,

Michelle Lam

Legislative Councillor (IT)

Published in February 2018 (Amended in May 2018)

Funding for this report was provided by Google. All opinions contained in this study reflect the independent views and analysis of the authors.



This report is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

HKTRANSPARENCY Report
a living report of the Government user data and content removal requests



<http://transparency.jmsc.hku.hk/>

Table of contents

Table of contents	2
Executive summary	3
1. Communications surveillance and transparency in the digital age	6
Introduction	6
Situation in Hong Kong	7
Situations in other jurisdictions	9
South Korea	9
Taiwan	11
Australia	13
The UK	14
The US	16
Observations	18
Recommendations	20
2. User data and content removal requests	22
Introduction	22
User data requests	23
Content removal requests	27
Appendix A: Government transparency reports	31
Appendix B: Questions raised by Legislative Council members on user data and content removal requests	33
Appendix C: ICT companies that release information about Hong Kong in their transparency reports	34

Executive summary

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 by covering 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%).

1. Communications surveillance and transparency in the digital age

Introduction

Background

The rise of multifaceted communications tools (e.g., emails, instant messaging applications and social media platforms) has widened the governments' aperture of surveillance all over the world, forcing a rethink of how to strike a balance between privacy and public security. Edward Snowden's global surveillance disclosure of the massive US spy programme in 2013 has prompted many jurisdictions to introduce legislations or amendments on current communications surveillance laws, contributing to better transparency.

In Hong Kong, a number of legislators and civil society groups have demanded to expand the scope of surveillance regulation. They recommended to add the access to user data and stored communications to the law during the deliberation of the Interception of Communications and Surveillance Amendment Bill 2015. However, the government refused to adopt the recommendation on the ground that surveillance law only regulated covert actions by law enforcement agencies¹.

Purpose

To enhance knowledge of Hong Kong's state of surveillance in cyberspace, the Hong Kong Transparency Report project has conducted a research on the matter, including a survey of the situations in South Korea, Taiwan, Australia, the UK and the US, with the hope that their experiences could help to shed light on potential solutions for Hong Kong.

¹ See 保安局局長動議恢復二讀辯論《2015 年截取通訊及監察（修訂）條例草案》發言全文（Chinese only），3 June 2016, “《條例》自二〇〇六年運作至今，依然有效地支援執法機關的運作，沒有「過時」或「涵蓋範圍不足」的情況，也不存在漏洞... 執法機關向網絡服務供應商索取用戶資料屬日常執法工作，不屬於《條例》規管範圍，兩者不應混為一談。”
<http://www.info.gov.hk/gia/general/201606/03/P201606030690.htm>

Definition

For the sake of consistency and convenience, this report will use the term “communications surveillance” to mean surveillance in cyberspace². Other terms frequently used in the report are defined as below:

- 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”.

Situation in Hong Kong

Surveillance

Surveillance by government agencies in Hong Kong is subject to the Interception of Communications and Surveillance Ordinance (Cap. 589, ‘ICSO’), which stipulates that a postal interception, telecommunications interception³ or data surveillance⁴ must be authorised by a panel judge⁵. In practice, the ICSO only covers the surveillance of real-time communications, while excluding contents and data that have already been stored.

For access to personal information and log records (metadata), government agencies usually issue user data requests to ICT companies, subject to the Personal Data (Privacy)

² “Communications surveillance” include postal mails, but this report only uses it to refer to surveillance targeting activities in cyberspace.

³ Section 2(1) of the Interception of Communications and Surveillance Ordinance (Cap.589) provides that “‘communication’ (通訊) means—(a) any communication transmitted by a postal service; or (b) any communication transmitted by a telecommunications system;”

⁴ Section 2(1) provides that “‘data surveillance device’ (數據監察器材)—(a) means any device or program used to monitor or record the input of information into, or the output of information from, any information system by electronic means; but (b) does not include an optical surveillance device;”

⁵ Section 8(1) provides that “An officer of a department may apply to a panel judge for the issue of a judge’s authorization for any interception or Type 1 surveillance to be carried out by or on behalf of any of the officers of the department.” Type 1 surveillance includes the use of data surveillance device.

Ordinance (Cap. 486)⁶. However, no detailed guidance or code of practice for a user data request has been found, while no court warrant is required. Companies may voluntarily comply with it.

To obtain the stored communications, law enforcement agencies are required to apply for a court warrant⁷ according to statutes including the Police Force Ordinance⁸. The High Court ruled in October 2017 that the police must obtain a warrant to inspect the content of a suspect's digital device seized during the arrest⁹.

Transparency

The Commissioner on Interception of Communications and Surveillance has published annual reports since 2007, which included the statistics of refused cases, people arrested, irregularities etc.¹⁰ However, the reports never broke down the figures by types of communications (e.g., phones, emails and instant messaging applications).

The government revealed the statistics of user data requests in its replies to questions by legislative council members from time to time¹¹, but no routine disclosure so far. Meanwhile,

⁶ See Paragraph 6 of the government response by Millie Ng for Secretary for Security, 8 May 2015, LC Paper No. CB (2)1391/14-15(01), "When investigating crime, LEAs may, depending on the nature of the cases and for the purpose of crime prevention and detection, request necessary information related to crime detection from the individuals or organisations concerned, including subscribers' information (such as account name and Internet Protocol address) and log records from local or overseas Internet service providers (ISPs), for locating witnesses, evidence or suspects. Such enquiries do not involve any request for records of the content of any non-public communications. LEAs are required to abide by the provisions of the Personal Data (Privacy) Ordinance (Cap. 486) when requesting personal data for the purpose of crime prevention and detection. Requesting subscribers' information from ISPs is part of LEAs' routine law enforcement efforts, and falls outside the scope of the ICSO."

⁷ See 010228-010842 of the minutes of meeting Bills Committee on Interception of Communications and Surveillance (Amendment) Bill 2015, 11 May 2015, LC Paper No. CB (2)1586/14-15, "(b) LEAs would apply for a court warrant when they intended to obtain information other than metadata from ISPs."

⁸ See Paragraph 9 of the government response by Millie Ng for Secretary for Security, 8 May 2015, LC Paper No. CB (2)1391/14-15(01), "Legislation that provides for an application for a court warrant includes: section 17 of the Prevention of Bribery Ordinance (Cap. 201), section 10B of the Independent Commission Against Corruption Ordinance (Cap. 204), section 50(7) of the Police Force Ordinance (Cap. 232), section 5 of the Organized and Serious Crimes Ordinance (Cap. 455), section 191 of the Securities and Futures Ordinance (Cap. 571), section 21 - 3 - of the Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405), section 123 of the Copyright Ordinance (Cap. 528) and section 56AA of the Immigration Ordinance (Cap. 115)."

⁹ See Sham Wing Kan v. Commissioner of Police, HCAL122/2014, ruled on 27 October 2017.

¹⁰ See Annual Report to the Chief Executive by The Commissioner on Interception of Communications and Surveillance, <http://www.info.gov.hk/info/sciocs/en/reports.htm>

¹¹ See LCQ10: Government's requests for information disclosure and removal made to information and communication technology companies, 1 March 2017, <http://www.info.gov.hk/gia/general/201703/01/P2017030100385.htm>

the Police Force, which is the largest user data requester, never disclosed key figures such as the number of court warrants they applied for.

With respect to access to stored communications by court warrants, the government said it had never maintained such statistics¹².

Situations in other jurisdictions

South Korea

Surveillance

There are four types of communications surveillance in South Korea: communication restricting measures (interception)¹³, acquisition of communications confirmation (metadata)¹⁴, provision of communications data (personal information), and search & seizure (stored communications)¹⁵.

¹² See Paragraph 6 of the government response by Millie Ng for Secretary for Security, 28 May 2015, LC Paper No. CB (2)1572/14-15(01), "LEAs do not maintain statistical figures on obtaining documents or information from any organisations, individuals or specific industries through application for court warrants."

¹³ "Content restricting measure" (interception) is a term appearing in the official English translation of South Korean law, and it is also called "censorship". See Article 3 of the Protection of Communication Secrets Act provides that "Any censorship of mail or any wiretapping of telecommunications (hereinafter referred to as 'communication-restricting measures') ..." Article 2 of the Act also provides that "6. The term 'censorship' means opening mail without the consent of the party concerned or acquiring knowledge of, recording or withholding its contents through other means;" http://elaw.klri.re.kr/eng_service/lawView.do?hseq=39120&lang=ENG

¹⁴ Article 2 of the Protection of Communications Secrets Act provides that "11. The term 'communication confirmation data' means the data on the records of telecommunications falling under any one of the following: (a) The date of telecommunications by subscribers; (b) The time that the telecommunications commence and end; (c) The communications number of outgoing and incoming call, etc. and the subscriber number of the other party; (d) The frequency of use; (e) The computer communications or Internet log records relating to facts that the users of computer communications or the Internet have used the telecommunications services; (f) The data on tracing a location of information communications apparatus connecting to the information communications networks; (g) The data on tracing a location of connectors capable of confirming the location of information communications apparatus to be used by the users of computer communications or Internet for connecting with the information communications networks;"

¹⁵ See page 3 of the Korea Internet Transparency Report 2017, October 2017, Korea University Law School, <http://transparency.kr/wp-content/uploads/2017/10/Korea-Internet-Transparency-Report-2017.pdf>

According to the Protection of Communication Secrets Act, a written permission by a court¹⁶ is required for conducting interception¹⁷ or acquisition of metadata¹⁸. Under certain circumstances concerning national security, the written approval must be issued by the president¹⁹. After the provision of metadata, the companies should report to the Ministry of Science and ICT²⁰.

For personal information including names, addresses, ID, etc., a public agency or judicial body may issue a request without a warrant to a telecommunication business operator pursuant to the Telecommunications Business Act²¹. The Act was introduced in 2010, providing detailed procedures for user data requests in its Article 83. Companies may voluntarily comply with such a request, but once the information provided, they should report to the Ministry of Science and ICT as well²².

¹⁶ The Act use the term “written permission” instead of “warrant”, Article 6 (5) provides that “The court shall, when it deems the application justified, grant permission for the communication-restricting measures to each suspect or person under investigation and then deliver a document attesting his/her granting such permission (hereinafter referred to as “written permission”) to the applicant.”

¹⁷ Article 6(1) provides that “Any prosecutor (including any public prosecutor; hereinafter the same shall apply) may ask a court (including a military court; hereinafter the same shall apply) to permit communication-restricting measures for each suspect or person under investigation when the requirements provided for in Article 5 (1) are met.”

¹⁸ Article 13(2) provides that “Any prosecutor or judicial police officer shall, when he/she asks for the provision of the communication confirmation data under paragraph (1), obtain permission therefor from the competent district court (including any ordinary military court; hereinafter the same shall apply) or branch court with a document...”

¹⁹ Article 7(1) provides that “2. Written approval shall be obtained from the President with respect to communications of countries hostile to the Republic of Korea, foreign agencies or groups and foreign nationals suspected of engaging in anti-national activities, or members of groups within the Korean Peninsula effectively beyond the sovereignty of the Republic of Korea and their umbrella groups based in foreign countries, and in the event of the proviso of paragraph (1) 1.”

²⁰ Article 13(7) provides that “When a telecommunications business entity provides any prosecutor, any judicial police officer or the head of any intelligence and investigative agency with the communication confirmation data, he/she shall make a report on the provision of the communication confirmation data twice a year to the Minister of Science, ICT and Future Planning and shall keep records in which necessary matters, including the provision of the communication confirmation data, are entered and other materials related to requests for the provision of the communication confirmation data, etc. for seven years from the date on which each of such communication confirmation data is provided.”

²¹ Article 83(3) of the Telecommunications Business Act provides the scope of data provision “1. Names of users; 2. Resident registration numbers of users; 3. Addresses of users; 4. Phone numbers of users; 5. User identification word (referring to the identification codes of users used to identify the rightful users of computer systems or communications networks); 6. Dates on which users subscribe or terminate their subscriptions.”

²² Article 83(6) of the Telecommunications Business Act.

To collect stored communications, law enforcement agencies must obtain a search & seizure warrant by a court in accordance with Article 215 of the Criminal Procedure Act²³. Such a warrant also allows them to access metadata and personal information stored in the devices they have searched or seized.

Transparency

The Ministry of Science and ICT publishes statistics of interception, acquisition of metadata and personal information biannually on its website²⁴, based on the reports submitted by telecommunications business entities.

The government report breaks down the numbers by agencies, types of accounts, communications methods (landline/mobile/internet, etc.). For Interception, the figures are categorised by normal/urgent measures.

The statistics of stored communications acquired by search and seizure warrants are not publicly available in South Korea²⁵.

Taiwan

Surveillance

In Taiwan, surveillance of both real-time and stored communications transmitted through telecommunication system are subject to the Communication Security and Surveillance Act²⁶. The methods include interception, sound and video recording, opening and checking, while excluding installation of surveillance devices²⁷. To conduct communications surveillance, an "interception warrant" shall be applied by a prosecutor to a judge²⁸.

²³ Korea's Supreme Court ruled in 2016 that it is illegal to obtain stored communications with an interception warrant (Supreme Court, 2016Do8137, 13 October 2016), and now a prosecutor would apply for a search and seizure warrant to access such contents.

²⁴ See the report of 1st half of 2017:

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

²⁵ See page 43 of the Korea Internet Transparency Report 2017.

²⁶ Article 6 of Communication Security and Surveillance Act provides that "The 'communications' as defined in this Act refer to: 1. Utilizing wired and wireless telecommunication equipment to send, store, transmit, or receive symbols, texts, images, sound or other types of information. 2. Mail and letters. 3. Speeches and conversations."

²⁷ See Article 13 of the CSSA.

²⁸ See Article 5 the CSSA. Article 6 provides that "in order to protect people's lives, bodies, or property from immediate harm...the judicial police authority may report to the prosecutor concerned, who will then verbally inform the enforcement authority to give priority to the communication surveillance." However, the prosecutor should report to the court within 24 hours and request the issuance of an interception warrant.

The 2014 Amendment created the “access warrant” for communications records (metadata) and user’s information (personal information)²⁹, with similar procedures of the interception warrant. Communications records include phone numbers, duration and locations, while user’s information include names, ID numbers and addresses³⁰.

In the meantime, the law enforcement authorities may issue a request to a telecommunications service provider to inquire users’ information, in accordance with the implementation measures promulgated under Article 7 of the Telecommunications Act³¹. The request must be signed by the head of a public or judicial authority, but service providers may voluntarily comply with it.

However, the requirements and procedures above do not apply to data transmitted or held by non-telecom service providers, such as internet platform, content and application service providers. For emails, the interception warrant only applies to communications in the course of transmission but not to stored email contents³².

To access stored communications and user data held by non-telecom service providers³³, law enforcement officers should obtain a search warrant issued by a judge pursuant to the Code of Criminal Procedure³⁴.

Transparency

Both the law enforcement and judicial authorities are obliged to disclose the statistics of surveillance regularly, according to the CSSA³⁵.

²⁹ See Article 11-1 of the CSSA.

³⁰ Article 3 of the CSSA provides that “The ‘communications records’ as defined in this Act refer to records such as the telecommunications numbers of the sender and the recipient, time of communication, length of use, address, service type, mailbox or location information generated by the telecommunications system after the telecommunications user uses the telecommunications services. The ‘communications user’s information’ as defined in this Act refers to the telecommunications user’s name, number of identification document, telecommunications number and information completed in the application, for any type of telecommunications service.”

³¹ 《電信事業處理有關機關(構)查詢電信使用者資料實施辦法》於 2007 年根據台灣《電信法》第七條 (Article 7) 訂立。Article 7 provides that “A telecommunications enterprise or its employees, including the retired, shall hold the existence and contents of communications in strict confidence. The preceding paragraph is not applicable to inquiries conducted in accordance with law. The Directorate General of Telecommunications shall promulgate rules governing operational procedures for telecommunications enterprises to handle inquiries for communications records and users’ data by relevant institutions.”

³² See an reply by the Ministry of Justice to Yahoo’s enquiry on 17 October 2014, 法檢字第 10300162120 號函, <http://www.moj.gov.tw/ct.asp?xItem=362736&ctNode=34731&mp=800>

³³ See “electronic record” in Article 122, Chapter XI “search and seizure”, Code of Criminal Procedure.

³⁴ See Article 128 of the CCP.

³⁵ See Article 16-1.

The Judicial Yuan, the highest judicial organ in Taiwan, has published annual statistical reports of communications surveillance since 2014³⁶, with a breakdown of warrants issued by local courts and the Supreme Court. The figures are categorised by communication methods, including landline, mobile, asymmetric digital subscriber line (ADSL), Skype, email, etc. Regarding access to metadata and user information, the report additionally provides a breakdown of crimes, such as theft, drugs, fraud, gambling.

The Ministry of Justice, which oversees law enforcement agencies and prosecutors' offices, publishes similar statistics but of different classifications³⁷.

Australia

Surveillance

In Australia, only a designated national security or law enforcement agency³⁸ may apply for a warrant from a judge to conduct interception or to access stored communications for investigation of serious offences³⁹. Otherwise, communications cannot be intercepted or accessed according to the Telecommunications (Interception and Access) Act 1979⁴⁰ (TIA Act).

Same as interception, the use of any surveillance device, including one to monitor the data input and output of a computer⁴¹, requires a court warrant pursuant to the Surveillance Devices Act 2004 (SD Act).

Only a number of designated law enforcement agencies have the mandate to access telecommunications data (metadata)⁴², including existing and prospective data, but the permission of each action must be made by an authorised senior officer⁴³.

³⁶ See 通訊監察統計年報, Judicial Yuan, <http://www.judicial.gov.tw/juds/>

³⁷ http://www.rjsd.moj.gov.tw/rjsdweb/common/WebList3.aspx?menu=INF_COMMON_O

³⁸ See page 1 of the Telecommunications (Interception and Access) Act 1979 Annual Report 2015-16, Attorney-General's Department, "During the reporting period, interception warrants were available to 17 Commonwealth, state and territory agencies (along with ASIO)...", <https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/Telecommunications-Interception-and-Access-Act-1979-Annual-Report-15-16.pdf>

³⁹ See page 2 of the TIA Act Annual Report 2015-16.

⁴⁰ See Chapter 2 "Interception of telecommunications" and Chapter 3 "Preserving and accessing stored communications" of the Telecommunications (Interception and Access) Act 1979.

⁴¹ See Chapter 1 of the Surveillance Devices Act 2004 Annual report 2015-16, Attorney-General's Department.

⁴² See page 37 of the TIA Act Annual Report 2015-16, "'Telecommunications data' is information about a communication—such as the phone numbers of the people who called each other, how long they talked to each other, the email address from which a message was sent and the time the message was sent."

⁴³ See chapter 4 "Access to telecommunications data" of the TIA Act.

To obtain personal information, government agencies may issue requests with or without a warrant to ICT companies. Such a request is subject to the Australian Privacy Principle 6 ("Use or disclosure of personal information")⁴⁴ of the Privacy Act 1988. Companies may voluntarily comply with a warrantless request.

Transparency

The Attorney-General's Department publishes annual reports under the TIA Act and SD Act⁴⁵.

The two reports not only provide statistics but also the legal grounds and procedures in plain language. They include the relevant legislations and legal development, agencies involved, types of warrants and surveillance devices, telecommunications data (metadata) and retained subscriber data (personal information)⁴⁶, numbers of prosecutions and convictions.

The UK

Surveillance

According to the Regulation of Investigatory Powers Act 2000, any interception of communications including access to stored communications⁴⁷ shall not be conducted without an authorisation, in most cases a warrant issued by a secretary of state⁴⁸.

⁴⁴ See Schedule 1 of the Privacy Act 1988.

⁴⁵ The two reports by the Attorney-General's Department are available on the webpage: <https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/default.aspx>

⁴⁶ See Table 43 in page 57 of the TIA Act Annual Report 2015-16.

⁴⁷ For the definition of "stored communications", see sections 2(7) and 2(8) of the Regulation of Investigatory Powers Act 2000. In addition, Section 3.23 of the Interception of Communications Code of Practice states that stored communications may also be accessed by means other than a warrant, for example, to be obtained by a production order under the Police and Criminal Evidence Act 1984.

⁴⁸ See page 33 of the Report of the Interception of Communications Commissioner Annual Report for 2016, "In practice, four Secretaries of State and one Scottish Minister consider most of the interception warrants. They are: The Defence Secretary; the Foreign and Commonwealth Secretary; the Home Secretary; the Secretary of State for Northern Ireland; and the Cabinet Secretary for Justice for Scotland." <https://www.gov.uk/government/publications/report-of-the-interception-of-communications-commissioner-annual-report-2016>

The acquisition of communications data (metadata and personal information)⁴⁹ is currently subject to the approval by a designated senior officer⁵⁰ of a public authority. A designated officer may also issue a notice to service providers, requiring them to obtain or disclose communications data⁵¹. The service providers must comply with the notice⁵².

However, the power to authorise access to user data may be transferred to a new authority under the investigatory powers commissioner, according to a government consultation paper published in November 2017⁵³.

For encrypted communications, a senior law enforcement officer may, upon the permission by a judicial authority, issue a notice to individuals or organisations, requiring them to decrypt the information⁵⁴.

Transparency

The United Kingdom has established a few codes of practice detailing the procedures on how to acquire and enforce the disclosure of communications. They include codes of practice for acquisition, disclosure and retention of communications data⁵⁵, interception of communications⁵⁶, and investigation of protected electronic information⁵⁷.

Currently, surveillance statistics (interception and communications data), errors and other issues can be found in annual reports published respectively by the offices of surveillance commissioners, interception of communications commissioner and intelligence services commissioner. From the reporting year of 2017, the three reports will merge into one to be published by the newly established investigatory powers commissioner⁵⁸.

⁴⁹ Collectively referred to as “communications data” in RIPA, and categorised by the Commissioner in his annual report into traffic data (e.g., the sender and recipient, location, time), service data (e.g., items on the bills of a user by a service provider) and subscriber information, see page 3 of the Annual Report for 2016.

⁵⁰ See sections 3.7-3.18 of the Code of Practice for the criteria of a “designated person”.

⁵¹ See Section 22 RIPA.

⁵² See Section 22(6) RIPA, introduced by the Protection of Freedoms Act 2012.

⁵³ See “UK police to lose phone and web data search authorisation powers”, 30 November 2017, The Guardian, <https://www.theguardian.com/technology/2017/nov/30/police-to-lose-phone-and-web-data-search-authorisation-powers>

⁵⁴ See part III “Investigation of electronic data protected by encryption etc.” and schedule 2 of the RIPA.

⁵⁵ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

⁵⁶ <https://www.gov.uk/government/publications/interception-of-communications-code-of-practice-2016>

⁵⁷ <https://www.gov.uk/government/publications/code-of-practice-for-investigation-of-protected-electronic-information>

⁵⁸ See “Investigatory Powers Commissioner establishes oversight regime”, 1 September 2017, Home Office, <https://www.gov.uk/government/news/investigatory-powers-commissioner-establishes-oversight-regime>

The UK government has been improving statistical reporting. In 2015, the Home Office added new provisions on statistical requirements to a code of practice⁵⁹, after the interception of communications commissioner raised recommendations such as recording the number of applications and items of data⁶⁰. The commissioner also issued a guidance on the statistical requirements⁶¹.

The US

Surveillance

The Fourth Amendment to the United States Constitution protects Americans against unreasonable searches⁶², and the definition of “search” in the Amendment was ruled by the Supreme Court to include monitoring and recording of private conversations⁶³. Generally, surveillance such as the interception of US citizens or people within the country requires a court warrant.

The Foreign Intelligence Surveillance Act (FISA), initially passed in 1978, created the Foreign Intelligence Court (FISC) to oversee surveillance warrants mainly targeting foreign powers and related agents. The Act was amended a few times including by the FISA Amendments Act of 2008 and USA Freedom Act of 2015.

The FISA sets out conditions and procedures for surveillance. For example, Title I requires a court warrant applied by a federal law enforcement or intelligence agency to conduct communications surveillance of people within the US⁶⁴. Section 702 of Title VII permits warrantless intelligence information acquisition targeting foreigners who are outside the US, subject to directives by the attorney general and the director of national intelligence,

⁵⁹ See paragraphs 6.5 and 6.6 of the Acquisition and Disclosure of Communications Data Code of Practice, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf

⁶⁰ See “Relationship between applications, authorisations, notices and items of data”, November 2014, Interception of Communications Commissioner’s Office, <http://www.iocco-uk.info/docs/Relationship%20between%20applications,%20authorisations,%20notices%20and%20items%20of%20data.pdf>

⁶¹ See Guidance on the Statistical Requirements in Paragraphs 6.5 and 6.6 of the Acquisition and Disclosure of Communications Data Code of Practice, 13 November 2015, IOCCO, [http://www.iocco-uk.info/docs/SRO%20Circular%20\(3\)%20Statistical%20Guidance%20Document%20for%20Annual%20Statistical%20Return.pdf](http://www.iocco-uk.info/docs/SRO%20Circular%20(3)%20Statistical%20Guidance%20Document%20for%20Annual%20Statistical%20Return.pdf)

⁶² The Amendment IV provides “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

⁶³ See *Katz v. United States*, <https://supreme.justia.com/cases/federal/us/389/347/>

⁶⁴ See 50 U.S.C. sections 1804 and 1823.

and oversight by the FISC. Communications service providers in the US are obliged to assist with authorised surveillance under Section 702⁶⁵.

Metadata, including tangible business records and call detail records, may be obtained upon a court order by the FISC. Meanwhile, the Federal Bureau of Investigation (FBI) has the mandate to issue compulsory National Security Letters (NSLs) to ICT companies in order to access both metadata and personal information⁶⁶ for national security investigations.

Transparency

IC on the Record (icontherecord.tumblr.com) is a website created by the Intelligence Community (IC) to increase transparency, posting declassified documents and statistics dated back to 2009.

In June 2013, after the Edward Snowden leaks, the then US President Obama directed the IC to make public as much information as possible about the surveillance programmes⁶⁷.

The Office of the Director of National Intelligence (ODNI) published the first transparency report in June 2014, explaining legal grounds and procedures of surveillance and disclosing statistics of various types of FISA orders and NSLs.

In June 2015, the USA FREEDOM Act was enacted, codifying the requirement of transparency reporting and extending the scope of statistics⁶⁸. The ODNI also published the Principles of Intelligence Transparency for the Intelligence Community⁶⁹ and its implementation plan⁷⁰ in the same year.

⁶⁵ See 50 U.S.C. section 1881a, and pages 5-6 of the Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016, https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016

⁶⁶ NSLs may be issued for telephone subscriber information and other electronic communication transactional records, and consumer-identifying information (names, addresses, places of employment, etc.), see page 22 of the Statistical Transparency Report 2016.

⁶⁷ See Remarks by the president in a press conference, Barack Obama, 9 August 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/08/09/remarks-president-press-conference>

⁶⁸ See 50 U.S.C. section 1873(b)

⁶⁹ The four principles are: 1. Provide appropriate transparency to enhance public understanding of the IC; 2. Be proactive and clear in making information publicly available; 3. Protect information about intelligence sources, methods, and activities; 4. Align IC roles, resources, processes, and policies to support transparency implementation, see <https://www.dni.gov/index.php/how-we-work/transparency>

⁷⁰ See The Implementation Plan for the Principles of Intelligence Transparency, 27 October 2015, <https://icontherecord.tumblr.com/transparency/implementation-plan-2015>

Observations

The situations of communications surveillance in Hong Kong and other jurisdictions are summarised below:

Warrant requirement

	Hong Kong	South Korea	Taiwan	Australia	UK⁷¹	US
<i>Interception</i>	✓	✓	✓	✓	✓	✓
<i>Stored communications</i>	✓	✓	✓	✓	✓	✓
<i>Metadata</i>	✗	✓	✓	○	○	✓
<i>Personal information</i>	✗	○	○	○	○	○

✓: yes

✗: no

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

For interception and access to stored communications, Hong Kong and other jurisdictions all require a warrant, either issued by a court or a ministry.

To access metadata and personal information in Hong Kong, there is neither requirement for a warrant, nor publicly available guidance or code of practice for law enforcement agencies.

South Korea, Taiwan and the US require a warrant for acquisition of metadata. Even though some jurisdictions do not have any warrant requirement to access user data, guidance and codes of practice can be easily found on their government websites.

⁷¹ In the UK, a secretary of state instead of a court judge issues such a warrant.

Routine disclosure

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

✓: yes

X: no

○: not specified but contained in numbers of a higher categorical rank, e.g., the report in Hong Kong only mentions the number of “judge’s authorisations for interception” but does not specify how many telecommunications or postal interceptions.

All six jurisdictions surveyed regularly disclose information about surveillance, including statistics and explanation of the mechanism in plain language. Such information is available in the commissioners’ reports in Hong Kong and the UK, and reports by the ministries in South Korea, Australia and the US. Both Taiwan and the US have publicly available portals for disclosing relevant statistics.

However, the commissioner’s report in Hong Kong does not specify telecommunications surveillance, and statistics of access to stored communications, metadata and user information are not disclosed on a routine basis.

Most of the jurisdictions other than Hong Kong provide information about the whole spectrum of communications surveillance, except that South Korea does not disclose the statistics of stored communications seized, and that Taiwan does not maintain the statistics of user data requests.

Legislation

The Interception of Communications and Surveillance Ordinance (Cap.589) in Hong Kong applies to telecommunications interception only, whereas surveillance laws with similar titles in other jurisdictions set procedures for access to stored communications, metadata and personal information as well.

The major laws are the Protection of Communication Secrets Act in South Korea, the Communication Security and Surveillance Act in Taiwan, the Telecommunications Interception and Access Act in Australia, the Regulation of Investigatory Powers Act in the UK, and the Foreign Intelligence Surveillance Act in the US.

Recommendations

Introduce legislation or amendments to current law

Article 30⁷² 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”⁷³.

However, the ICSO does not set out “legal procedures” as Article 30 requires, for the authorities to access user data and stored communications. These accesses are increasingly important for government investigations and law enforcement nowadays.

The government argued that the literal definition of “interception” prevented them from expanding the scope of the ICSO to cover these accesses⁷⁴. However, other jurisdictions did change their interception or surveillance laws, or introduced new acts in response to developing communications technologies.

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

Provided that the government accept or consider the first recommendation, making legislation may take years. Before a new statute is enacted, the government may issue guidance or code of practice based on the interpretation of current laws and court judgements.

The experiences of other jurisdictions show that, even though warrants may not be required in some circumstances, detailed guidance to law enforcement agencies is the norm.

⁷² Article 30 of the Basic Law provides that “The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.”

⁷³ Article 29 of the Basic Law provides that “The homes and other premises of Hong Kong residents shall be inviolable. Arbitrary or unlawful search of, or intrusion into, a resident’s home or other premises shall be prohibited.”

⁷⁴ See page 8 of Minutes of meeting, Panel on Security, 5 December 2017, LC Paper No. CB(2)647/17-18, <https://www.legco.gov.hk/yr17-18/english/panels/se/minutes/se20171205.pdf>

Improve routine disclosure to increase transparency

The Interception of Communications and Surveillance Ordinance (Cap.589) provides a transparency and accountability mechanism by establishing a position of commissioner and making his annual report publicly available, same as Australia and the UK.

The Hong Kong commissioner's report does not include details of communications surveillance in cyberspace due to the outdated Ordinance. However, the government may disclose such statistics without a statutory requirement. For example, it has already regularly disclosed figures regarding the Code on Access to Information on an official website since 2015. Another example is in South Korea: the Ministry of Science and ICT publishes statistics of interception, acquisition of metadata and personal information biannually without a legal requirement.

2. User data and content removal requests

Introduction

The subject

The internet and other forms of information technology are increasingly becoming necessary for daily life. Technology brings both convenience and risks: our personal information is vulnerable on the internet, and people can be prosecuted for what they say there. The Hong Kong Transparency Report (HKTR) project is concerned with how the Hong Kong government obtains citizens' personal information and takes down contents in cyberspace.

For crime prevention and other law enforcement actions, the Hong Kong government issues requests 1) for user data⁷⁵ and 2) to remove content⁷⁶ from the services of internet, communications and technology companies, which are collectively referred to as information and communication technology (ICT) companies in this report. A number of companies have published transparency reports and may include other types of government requests, or requests from courts or individuals. For instance, Apple also reports "device requests" relating to information about lost or stolen devices. For the convenience to make comparison, **this report only analyses user data and content removal requests**, and only focuses on requests from the government.

The sources

The Hong Kong government does not routinely disclose its requests for user data and content removal. HKTR obtained the data from two sources: 1) responses from the government to questions on the issue by Legislative Council members; 2) replies from access to information officers of government departments to HKTR's enquiries according to the Code on Access to Information⁷⁷.

⁷⁵ "User data" in this report refers to users' contact information, IP address, time and date of communications, locations, etc.

⁷⁶ "Content removal" in this report refers to requests to remove articles, web pages, hyperlinks, etc. published on the internet and other information held by service providers.

⁷⁷ The administrative Code stipulates the scope of government information that will be provided and how the information will be made available either routinely or by means of response to requests.

Since 2013, legislators including Charles Mok and James To have submitted questions in the Legislative Council on government requests, and therefore such statistics is available in the government replies (see **Appendix B**).

Meanwhile, 61 companies across the globe released transparency reports until the end of 2015⁷⁸, eight of which have revealed that they received requests from the Hong Kong government (see **Appendix C**). This report also includes additional information from these eight companies.

User data requests

Number of user data requests 2011 – 17

From 2011 to 2017, the Hong Kong 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 requests), and has come down to the lowest in 2017 (3,541 requests).

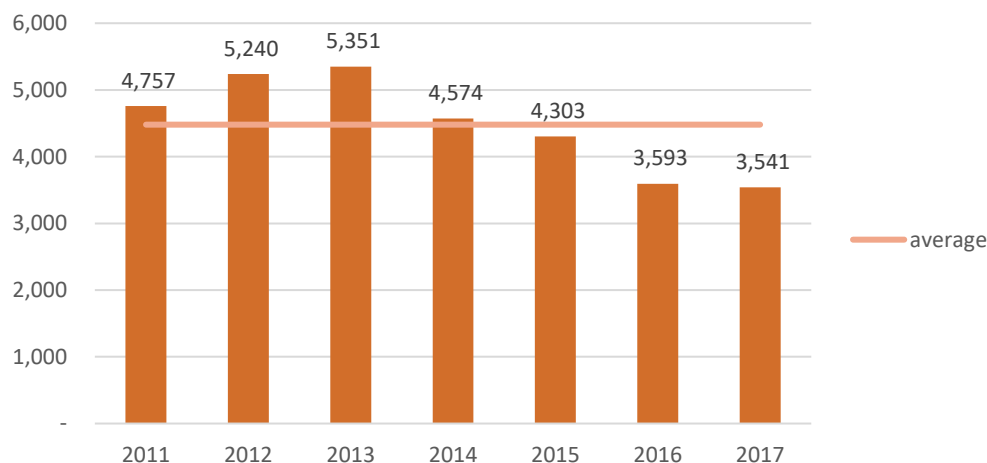


Chart 1 User data requests 2011 – 17

Comparison between figures from the government and ICT companies

As of 2017, eight ICT companies⁷⁹ have released regular transparency reports on user data requests from the Hong Kong government. However, their data is only comparable from 2013 onwards.

⁷⁸ Access Now. Transparency reporting index. <https://www.accessnow.org/transparency-reporting-index/>

⁷⁹ Google, Yahoo, Microsoft, Apple, Facebook, Twitter, Verizon and Line.

From 2013 to the first half of 2017, the number of user data requests sent to the companies comprised 42% (8,105 requests) of all such requests from the Hong Kong government. Both the absolute number and percentage decreased from 67% (1,722 requests, 1H2013) to 32% (572 requests, 1H2017), in line with the trend displayed by the government statistics.

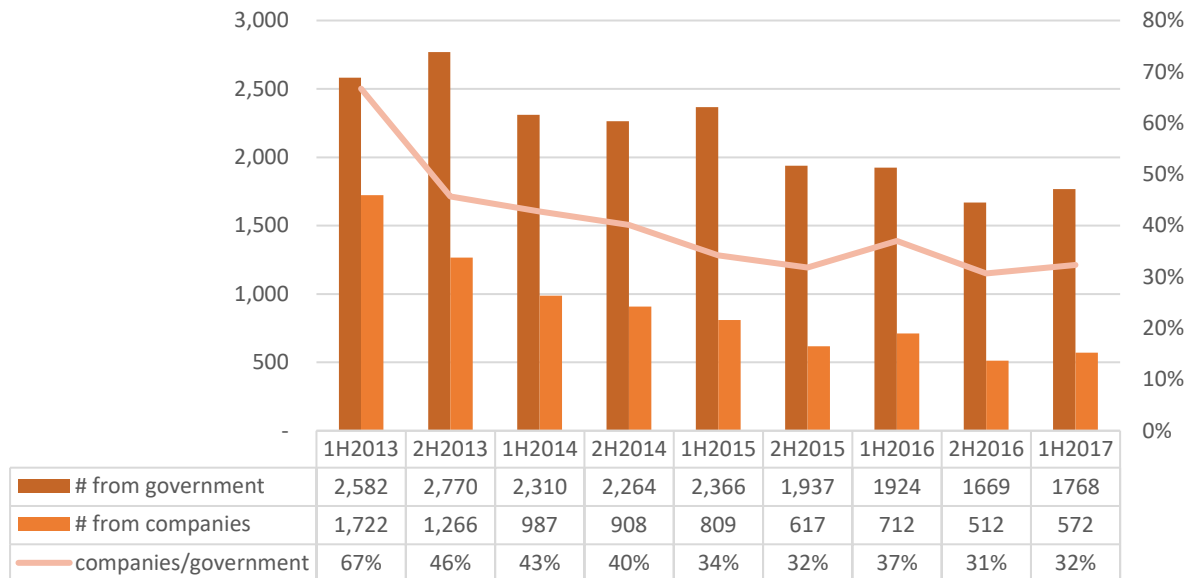


Chart 2 Comparison of user data request numbers released by the government and companies

Major sources of user data requests 2011 – 17

Of the seven government departments⁸⁰ that had issued user data requests between 2011 and 2017, three particular comprised 99% of all requests: the Hong Kong Police Force (88%), Customs and Excise Department (10%) and Office of the Communications Authority (1%).

⁸⁰ Agriculture, Fisheries and Conservation Department, Companies Registry, Customs and Excise Department, Home Affairs Department – Office of the Licensing Authority, Hong Kong Police Force, Inland Revenue Department, and Office of the Communications Authority.

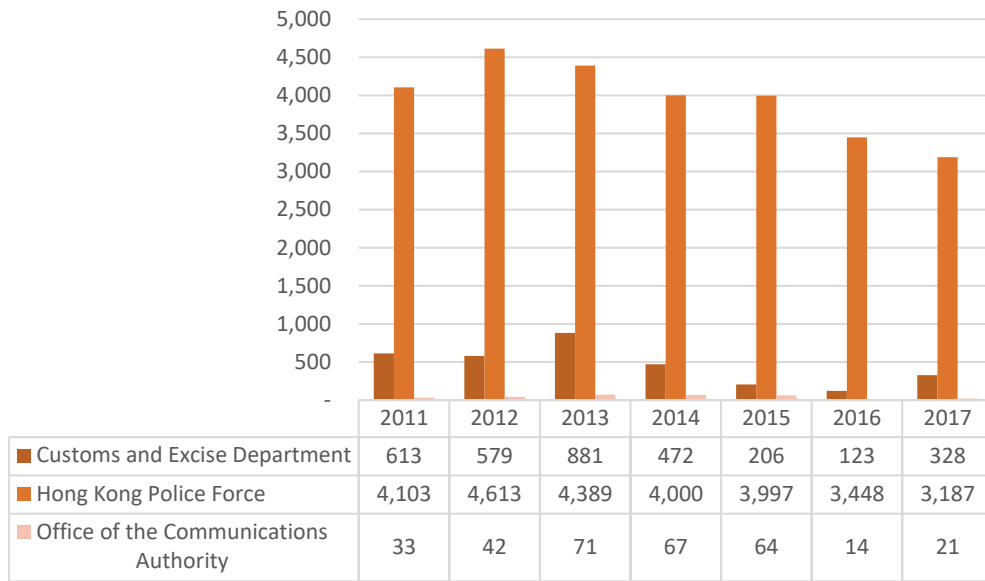


Chart 3 User data requests 2011 – 17 (comparison of government departments and years)

Reasons for user data requests

While details vary by departments, the reasons for user data requests between 2016 and 2017 can be generally classified into two categories:

- 1) **Crime prevention and detection** (99%, 7,086 requests): the Hong Kong Police Force (6,635 requests), Customs and Excise Department (451 requests).
- 2) **Law enforcement** (1%, 49 cases): the Office of the Communications Authority (35 requests), Inland Revenue Department (11 requests), Home Affairs Department - Office of the Licensing Authority (two requests), Companies Registry (one requests).

Reasons	2016	2017
Crime prevention & detection	3,571	3,515
Law enforcement	23	26

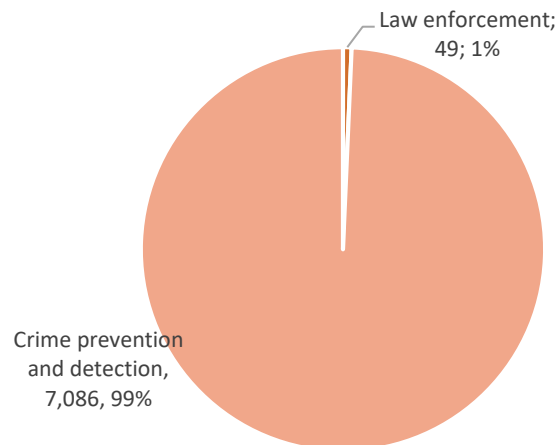


Chart 4 Reasons for user data requests 2016 – 17

User data requests acceded

Between 2016 and 2017, the government figures, excluding that of the Police, show that ICT companies complied with 99% of the government data requests.

The Police filed 88% of all such requests during the period, but never revealed the compliance rate.

	Companies Registry	Office of the Licensing Authority	Inland Revenue Department	Office of the Communications Authority	Customs and Excise Department	Hong Kong Police Force	Total*
# requests	1	2	11	35	451	6,635	500
# requests acceded	0	1	11	35	450	n/a	497
compliance %	0%	50%	100%	100%	99%	/	99%

*Excluding the Hong Kong Police Force

Chart 5 Comparison of user data requests acceded 2016 – 17 (released by the government)

However, the information released by the ICT companies shows that only 60% of the data requests from the Hong Kong government were acceded to from 2010 onward.

The compliance rate of Microsoft (77%) ranked the highest, followed by Apple (65%) and Yahoo (65%), Facebook (56%) and Google (42%). Twitter, Verizon and Line did not release such numbers.

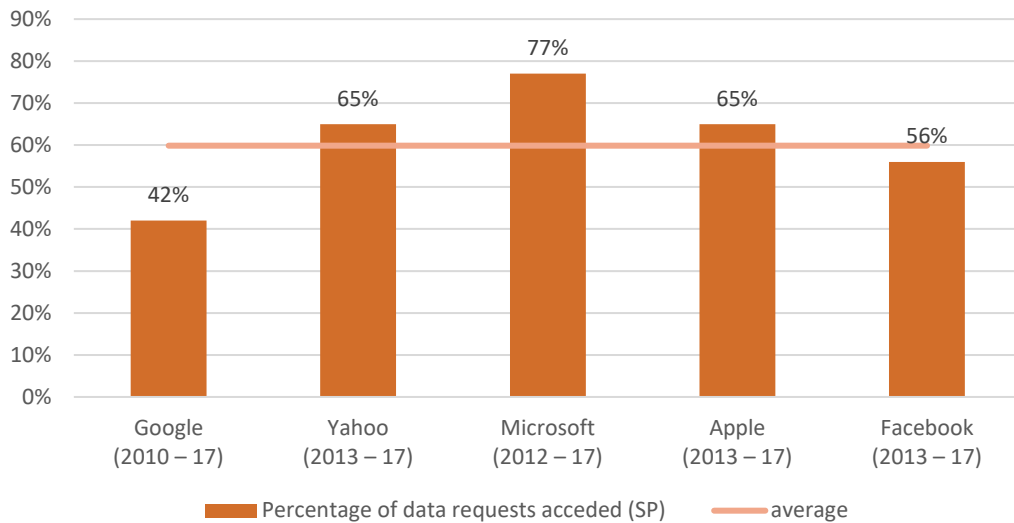


Chart 6 Comparison of percentage of user data requests acceded (released by companies)

User data requests without a warrant

Between 2016 and 2017, all government departments, other than the Police and Inland Revenue Department, had issued user data requests without any warrant. The Police⁸¹ and Inland Revenue Department⁸² refused to provide such figures.

Among the three requests rejected by ICT companies in the period, two (i.e. the Company Registries, and Office of the Licensing Authority) were attributable to a lack of warrant.

Content removal requests

Number of content removal requests 2011 – 17

From 2011 to 2017, the Hong Kong government had issued an annual average of 355 requests to ICT companies. The number has reached the highest in 2013 (657 requests), and has come down ever since, except for a rebound in 2017 (336 requests) from 2016 (194 requests)

⁸¹ The reason provided by the Police was that “relevant statistics are not available.”

⁸² The reason provided by the Inland Revenue Department was “due to the secrecy provisions under the Business Registration Ordinance (Cap. 310) and the Inland Revenue Ordinance (Cap.112).”

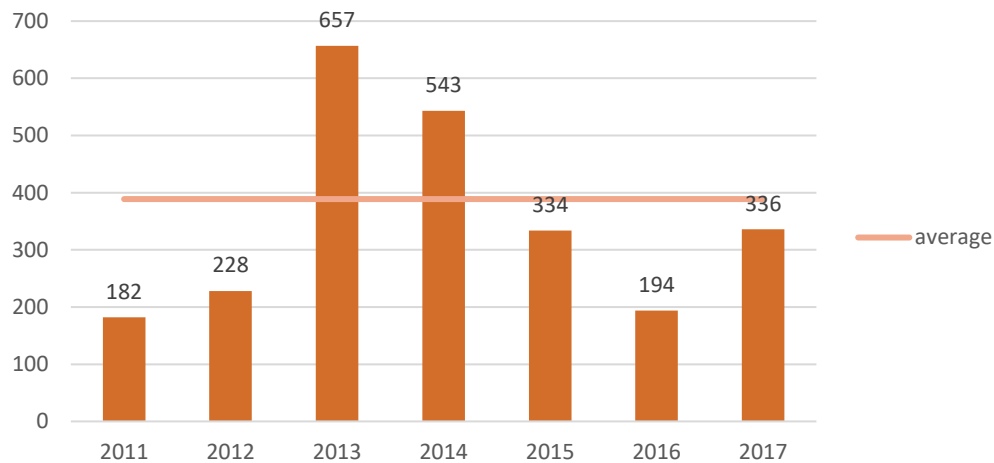


Chart 7 Content removal requests 2011 – 17

Major sources of content removal requests 2011 – 17

Of the 14 government departments which had issued content removal requests between 2011 and 2017, the Drug Office was the largest requester (40%, 1,004 requests), followed by the Customs and Excise Department (32%, 801 requests), Hong Kong Police Force (16%, 401 requests) and Chinese Medicine Division (8%, 211 cases).

If we combine data of the three divisions of the Department of Health (Drug Office, Chinese Medicine Division, and the Family Health Service), the department comprised 50% of all content removal requests from the Hong Kong government.

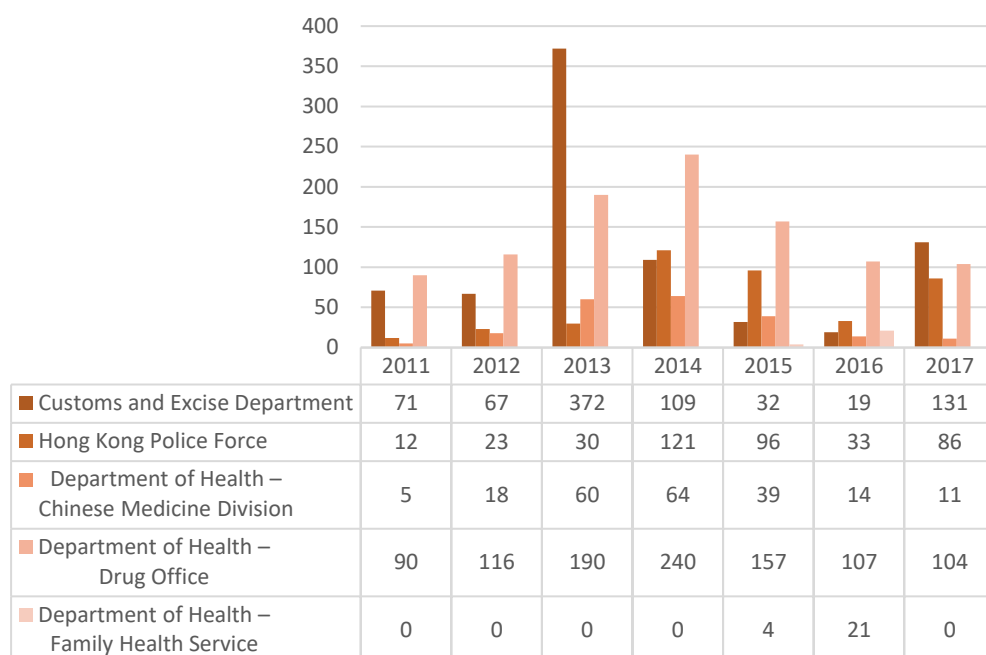


Chart 8 Content removal requests 2011 – 17 (comparison of government departments and years)

Reasons for content removal requests

Five types of reasons for content removal requests between 2016 and 2017

- 1) **Illegal sale of medicine** (44%, 236 requests): Department of Health – Drug Office (211 requests), Department of Health – Chinese Medicine Division (25 requests)
- 2) **Infringing activities** (32%, 171 requests): Customs and Excise Department (150 requests), Family Health Service (21 requests)
- 3) **Crime prevention & detection** (22%, 119 requests): Hong Kong Police Force
- 4) **Illegal advertisement** (2%, 11 requests): Housing Department
- 5) **Indecent content** (one request): Office of Communications Authority

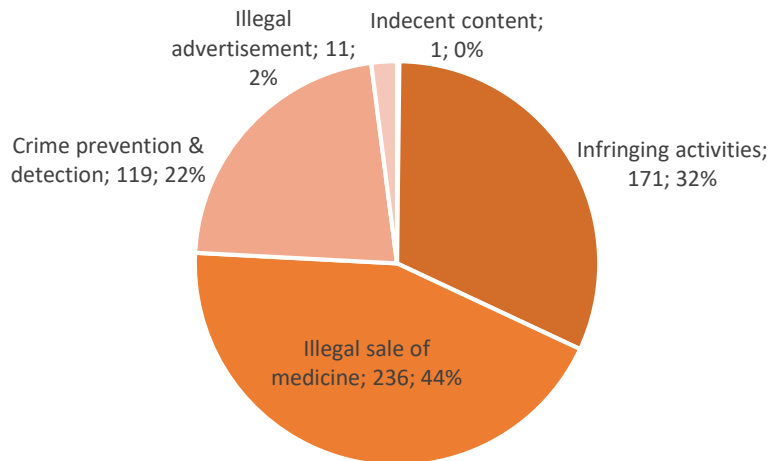


Chart 9 Reasons for content removal requests 2016 – 17

Content removal requests acceded

Between 2016 and 2017, the government figures, excluding that of the Police, show that ICT companies complied with all content removal requests.

The Police filed 16% of all such requests during the period, but never revealed the compliance rate.

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?catId=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_O

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) ⁸³	2013	2013	US	960	https://transparency.oath.com/
Apple ⁸⁴	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

⁸³ 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.

⁸⁴ 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.