

# Hong Kong Transparency Report

# 2014

---

Hong Kong Transparency Report (HKTR), a project run by Journalism and Media Studies Centre, The University of Hong Kong, researches and tracks government data and content removal requests towards Internet service providers, Internet platforms and websites.

## Contents

Introduction .....	1
Key findings of the 2014 data.....	2
User data requests .....	2
Content removal requests.....	3
Key findings of the 2013 data.....	3
User data requests .....	4
Content removal requests.....	6
A general review of the 2010-2013 data.....	8
User data requests .....	8
Content removal requests.....	10
Recommendations .....	13
Make public the current internal guidelines and monitoring mechanism .....	13
Set up an independent oversight body.....	13
Introduce a standard request logging system.....	14
Regular disclosure .....	15
Extend the scope of disclosure .....	15
User notification.....	16
Work with service providers .....	16
Annex I: Exemptions.....	17
Personal Data (Privacy) Ordinance.....	17
Annex II: data source.....	18

## Introduction

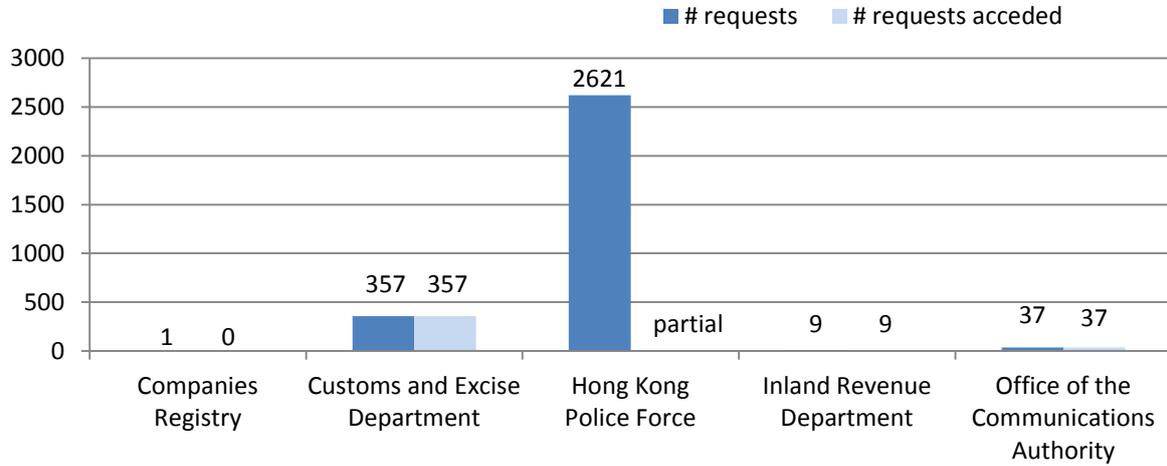
We believe that Hong Kong Internet users have the right to know how their data is being accessed and handled by other parties, and that the government has the obligation to respect users' privacy and regularly disclose its data and removal requests made to service providers during criminal investigations and other law enforcement activities.

Based on this belief, HKTR actively seeks new information from the access to information officers under the Code on Access to Information. During our research and request process, we identified a series of issues that cast shadows over government legitimacy and accountability, such as the lack of judicial review and an independent oversight body during the government request-making process. At the end of this report, we propose recommendations to improve the current request-making mechanism.

## Key findings of the 2014 data

### User data requests

2014 government data requests

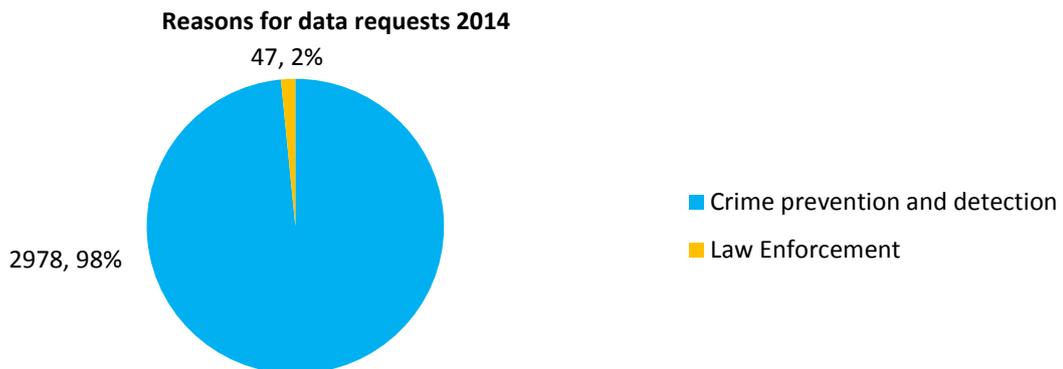


**Data Source:** Dataset the government disclosed upon James To’s requests

From 2014 February to October 15, five government departments made a total of 3,025 user information requests (requests for users’ names, address, contact details etc) to service providers.

The Police Force accounts for 86% (2,621 cases) of the total user information requests, followed by the Customs and Excise Department with 12% (357 cases).

Companies Registry said its request (only one case) is being handled by the service provider.



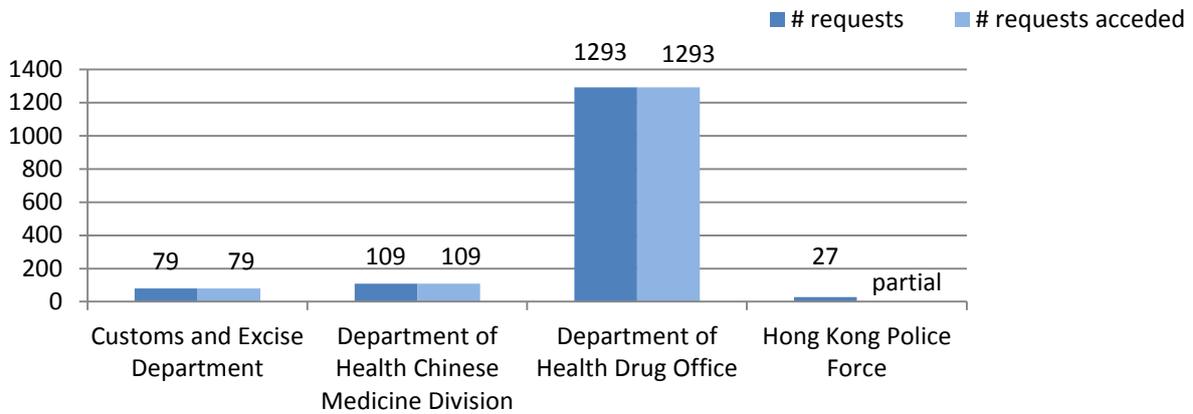
**Data Source:** Dataset the government disclosed upon James To’s requests

Two major reasons for government data requests:

- **Crime prevention and detection:** Police (2,621 cases) and Customs (357 cases)
- **Law enforcement:** Office of the Communications Authority (37 cases), Inland Revenue Department (9 cases) and Companies Registry (1 case)

## Content removal requests

2014 government removal requests



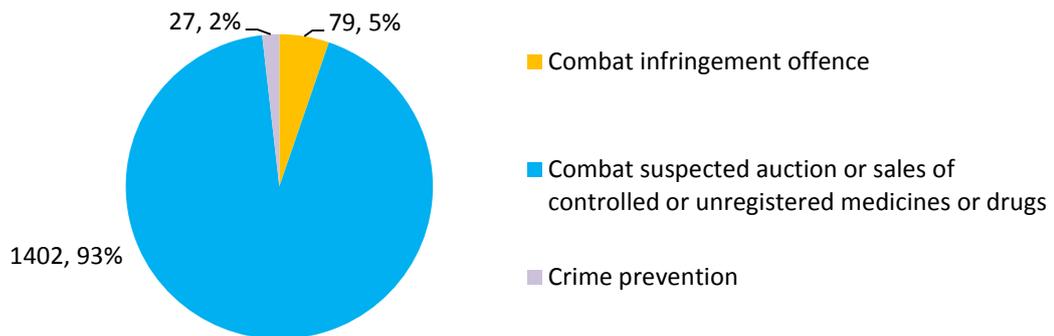
Data Source: Dataset the government disclosed upon James To’s requests

From 2014 February to October 15, four government departments made a total of 1,508 content removal requests (requests to remove articles, web pages, hyperlinks, etc) to service providers, almost all of which were acceded to.

The Department of Health accounts for 93% (1,402 cases) of the total content removal requests, followed by the Customs and Excise Department with 5% (79 cases).

The Police Force did not provide an exact number of its request compliance rate.

Reasons for removal requests 2014



Data Source: Dataset the government disclosed upon James To’s requests

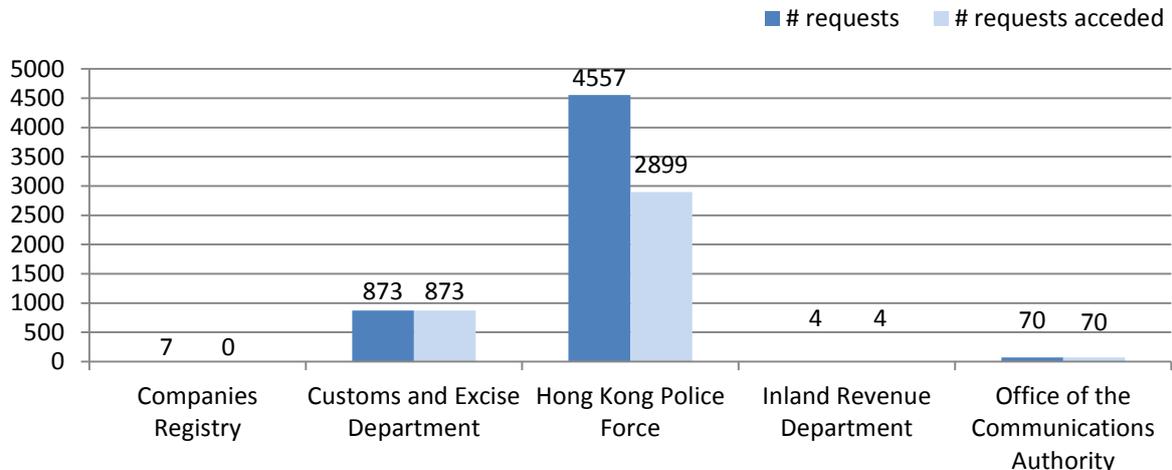
The three major reasons for government content removal requests:

- **Suspected auction or sales of unregistered products:** Department of Health (1,402 cases)
- **Infringement offences:** Customs and Excise Department (79 cases)
- **Crime prevention:** Police Force (27 cases)

## Key findings of the 2013 data

User data requests

2013 government data requests



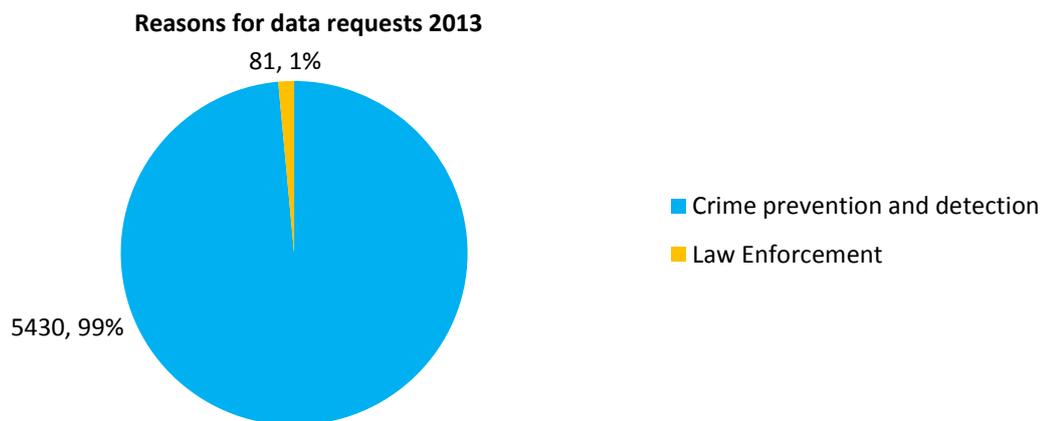
Data Source: Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

In 2013<sup>1</sup>, five government departments made a total of 5,511 user information requests (requests for users’ contact information, IP address, etc.) to service providers, out of which 3,846 requests (70%) were granted.

The Police Force accounts for 83% (4,557 cases) of the total user information requests, followed by the Customs and Excise Department with 16% (873 cases).

Only 64% of the Police Force’s requests were complied with by service providers.

None of the Companies Registry’s requests (in total 7 cases) was acceded to by service providers.

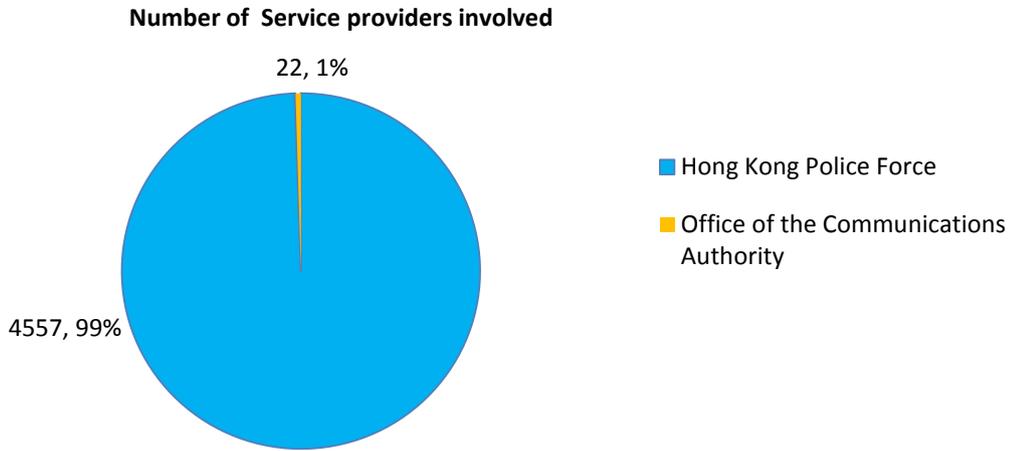


Data Source: Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

<sup>1</sup> The official reporting period for the 2013 data is from February 2013 to January 2014.

Two major reasons for government data requests:

- **Crime prevention and detection:** Police (4557 cases) and Customs (873 cases)
- **Law enforcement:** Office of the Communications Authority (70 cases), Companies Registry (7 cases), and Inland Revenue Department (4 cases)

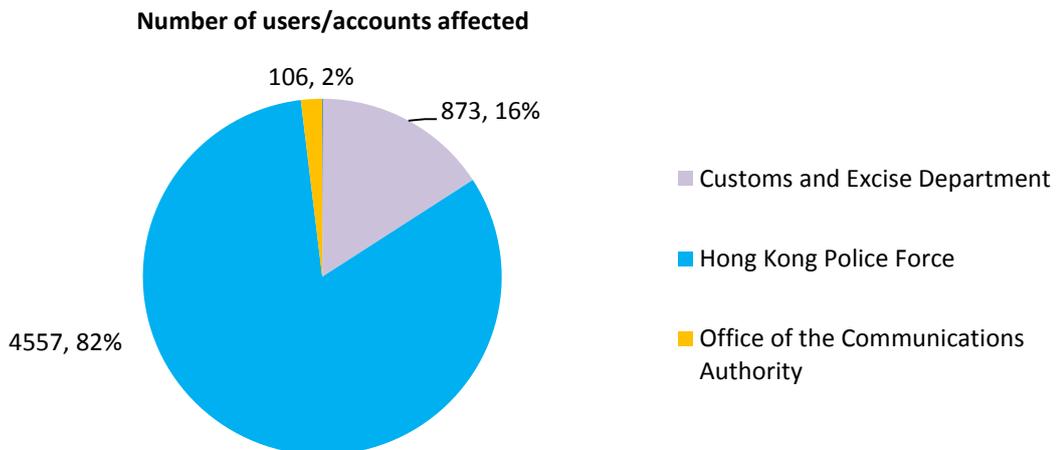


**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

Police requests involved the biggest number of service providers (4557), followed by OFCA (22), and Inland Revenue (4).

The Customs and Excise Department said it did not have any statistics of the number of service providers.

HKTR has sent a separate request to Companies Registry for the number of service providers involved on September 2, 2014. So far the department has not provided the information we requested.



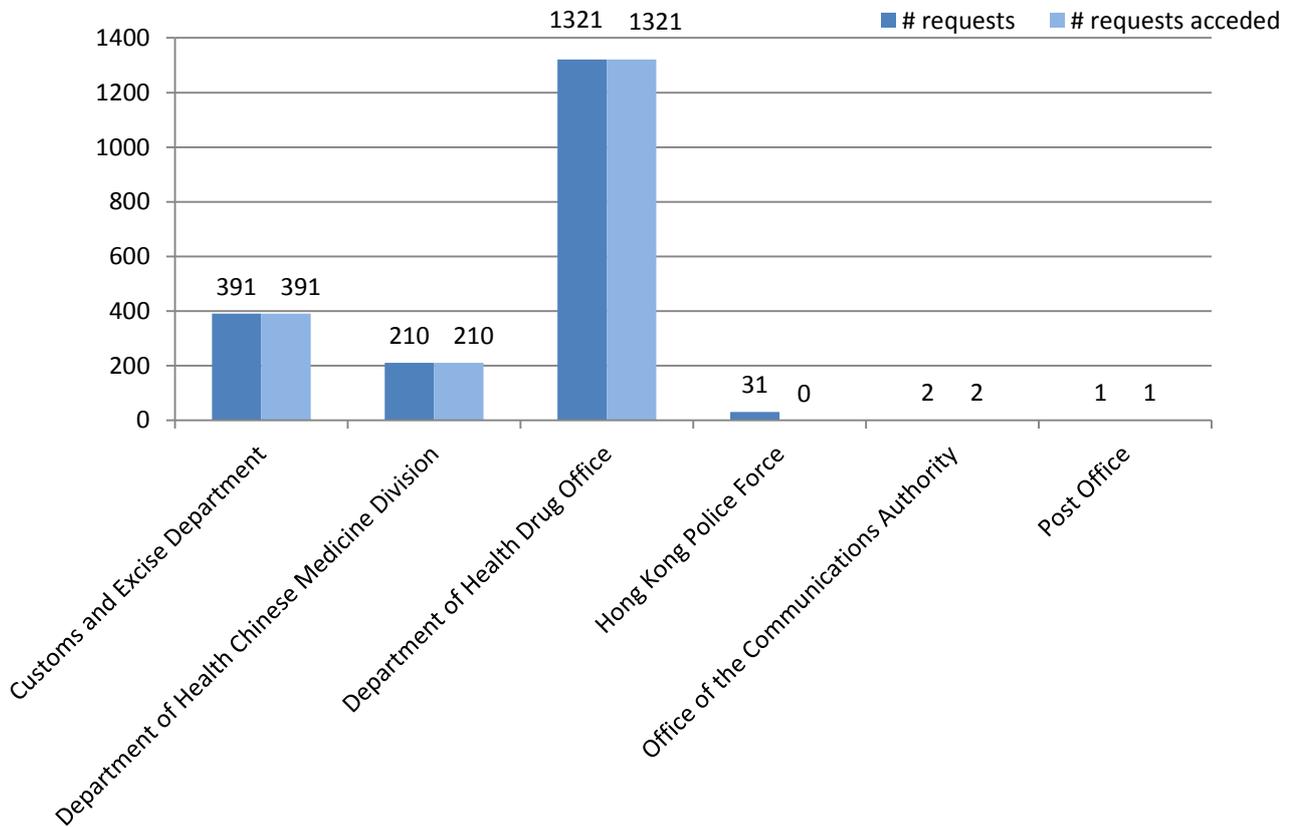
**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

The Police requests affected the largest number of users/accounts (4557), followed by Customs (873), OFCA (106), and Companies Registry (5).

Inland Revenue told HKTR that such information “cannot be provided due to the secrecy provisions under the Business Registration Ordinance and the Inland Revenue Ordinance”.

### Content removal requests

2013 government removal requests



**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

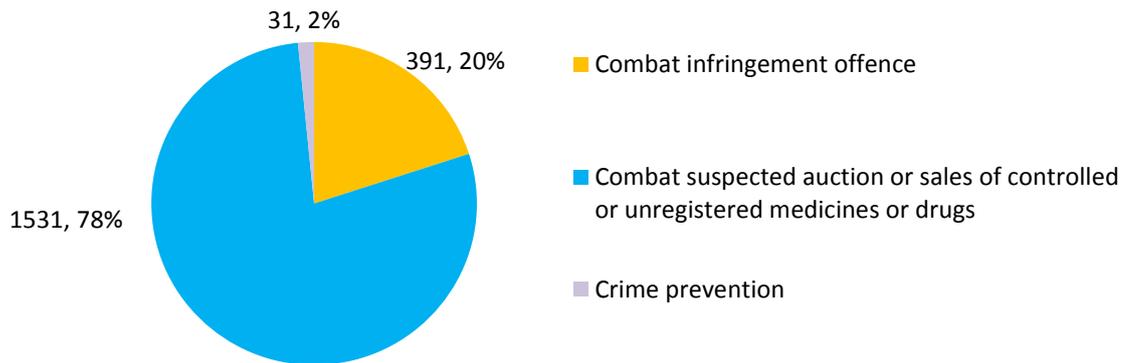
In 2013<sup>2</sup>, five government departments made a total of 1,956 content removal requests (requests to remove articles, web pages, hyperlinks, etc) to service providers, almost 100% of which were acceded to.

The Department of Health accounts for 78% (1,531 cases) of the total content removal requests, followed by the Customs and Excise Department with 20% (391 cases).

The Police Force did not provide an exact number of its request compliance rate, as some of the service providers did not respond to police requests.

<sup>2</sup> The official reporting period for the 2013 data is from February 2013 to January 2014.

Reasons for removal requests 2013

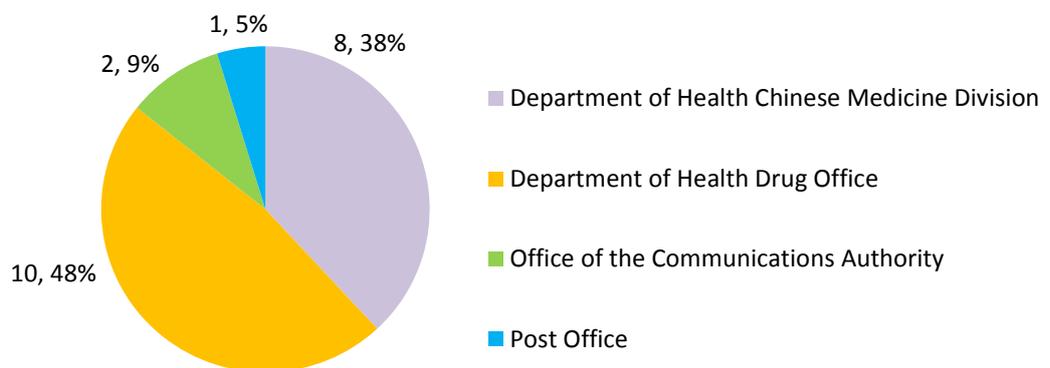


Data Source: Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

The three major reasons for government content removal requests:

- **Suspected auction or sales of unregistered products:** Department of Health (1,531 cases)
- **Infringement offences:** Customs and Excise Department (391 cases)
- **Crime prevention:** Police Force (31 cases)

Number of service providers involved



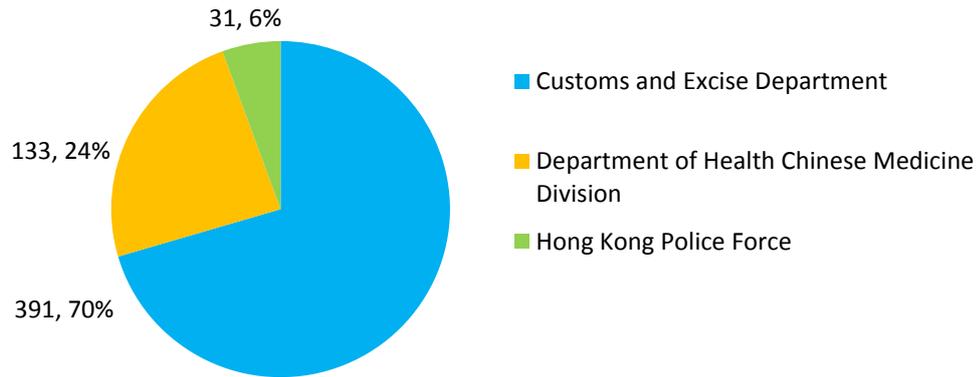
Data Source: Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

The Department of Health’s requests involved the biggest number of providers (18 in total), followed by OFCA (2), and Post Office (1). Data from Customs and Police are not available.

Office of the Communications Authority revealed the name of one of the websites that the authority asked to remove indecent text and photos.

The other departments did not disclose the names of the service providers due to legal or operational restrictions.

Number of users/accounts affected



**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

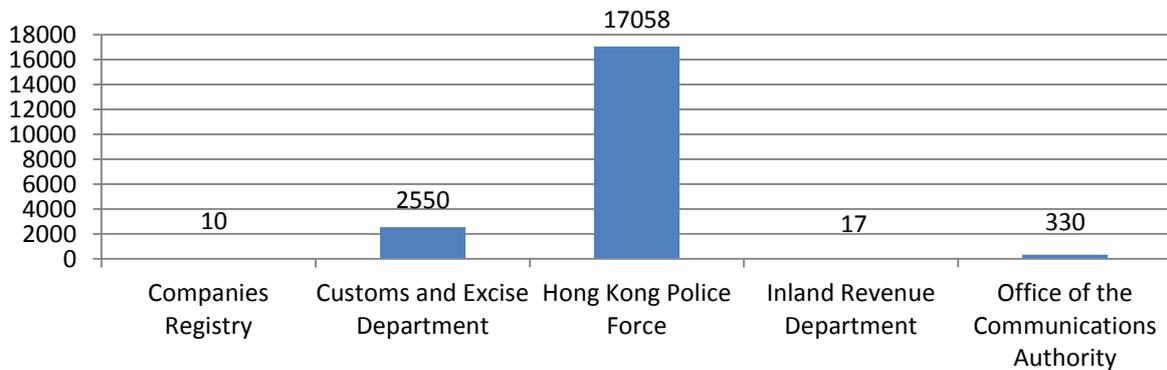
Customs’ requests affected the largest number of users/accounts (391), followed by the Chinese Medicine Division of the Department of Health (133), Police (31), OFCA (2) and Hongkong Post (1).

The Drug Office told HKTR it does not keep a record of the accounts affected and therefore cannot provide such information.

**A general review of the 2010-2013 data**

**User data requests**

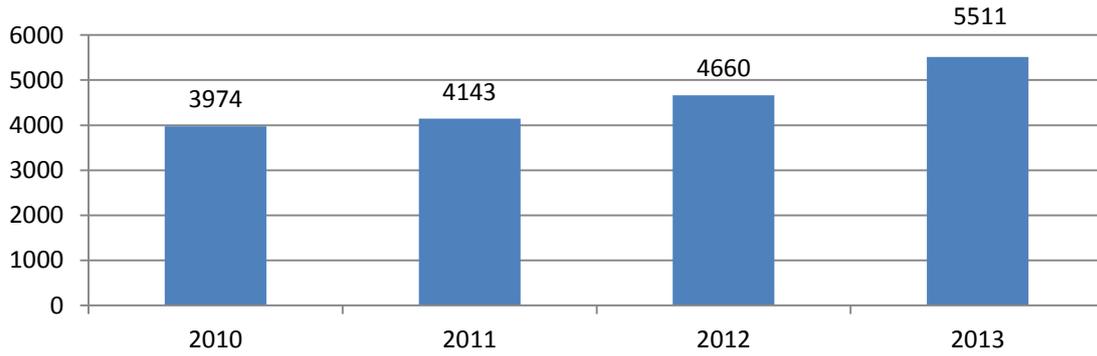
2010-2013 government data requests



**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

For the four-year period from 2010 to 2013, six government departments made a total of 19,965 user information requests. Of these, the Police Force made 85%, or 17,058 cases, followed by the Customs and Excise Department with 13%, 2550 cases.

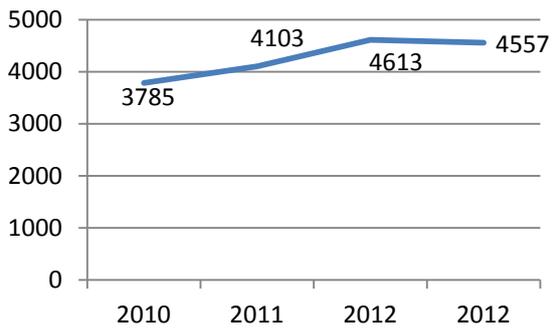
**Government data requests by year**



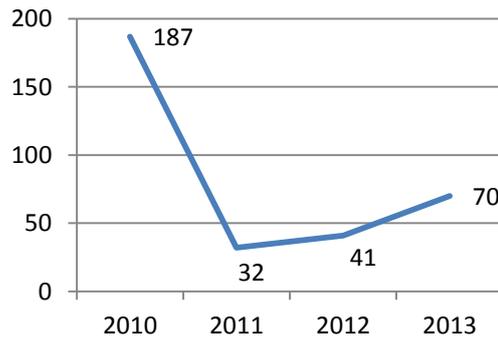
**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

Note: Data input from Customs between 2010 and 2012 is missing from the above chart. The Customs told HKTR that it did not have the annual breakdown of the data from 2010 to 2012. The Customs made a total of 1,677 requests from 2010 to 2012.

**2010-2013  
Police data requests**

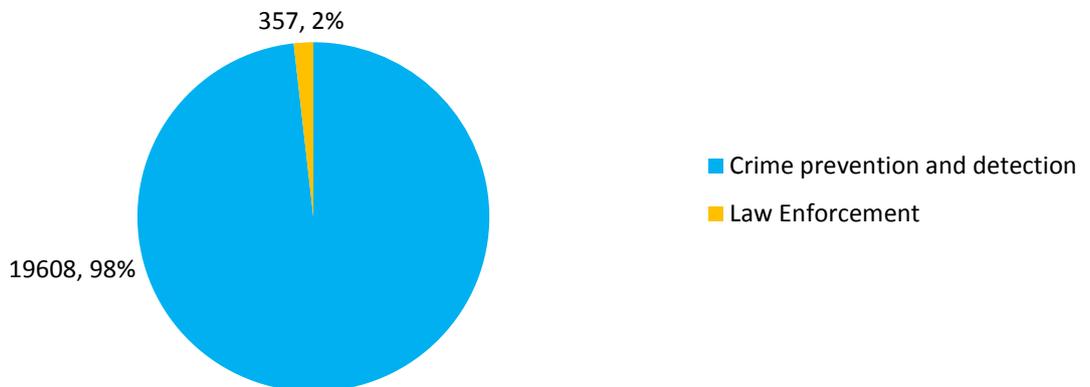


**2010-2013  
OFCA data requests**



**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

**Reasons for data requests 2010-2013**

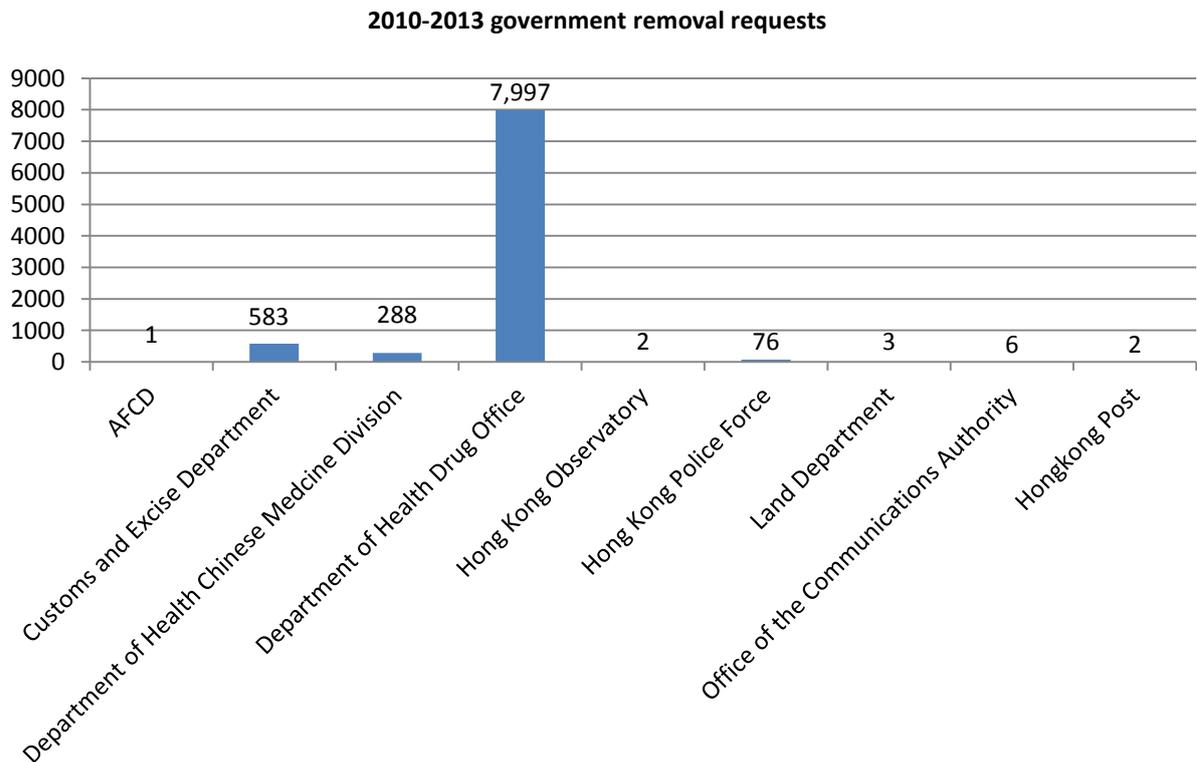


**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

The two major reasons for government data requests:

- Crime prevention and detection: Police Force (17,058 cases) and Customs (2550 cases)
- Law enforcement: Inland Revenue (17 cases), OFCA (330 cases), and Companies Registry (10 cases)

### Content removal requests

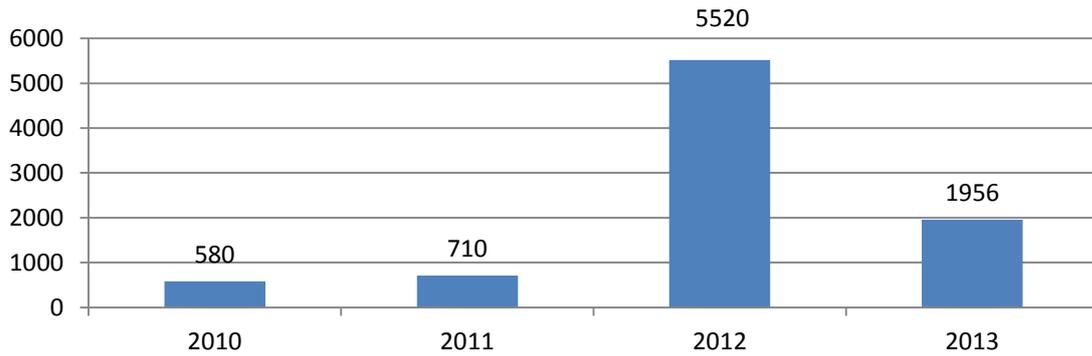


**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

For the four-year period from 2010 to 2013, eight government departments made a total of 8,958 content removal requests to service providers.

Over 92% of such requests came from Department of Health’s Drug Office and Chinese Medicine Division (8,285 cases). The Customs and Excise Department accounted for 7% (583 cases).

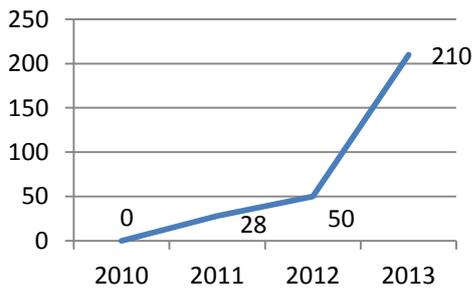
**Government removal requests by year**



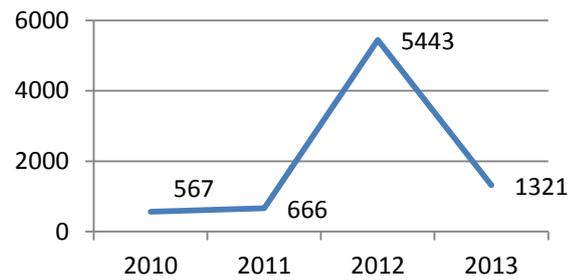
**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

**Note:** Data input from Customs between 2010 and 2012 is missing from the above chart. The Customs told HKTR that it did not have the annual break down data from 2010 to 2012. The Customs made a total of 193 removal requests from 2010 to 2012.

**Chinese Medicine Division  
removal requests  
2010-2013**

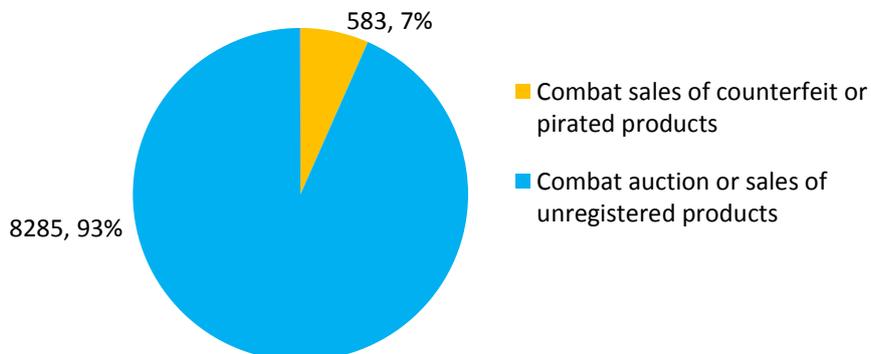


**Drug Office  
removal requests  
2010-2013**



**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

**Reasons for removal requests 2010-2013**



**Data Source:** Dataset the government disclosed upon Charles Mok’s requests, and new data HKTR obtained

The three major reasons for content removal requests during this four-year period are:

- **Suspected auction or sales of unregistered medicine or drugs:** Department of Health (8,235 cases);
- **Suspected sales of counterfeit or pirated goods:** Customs (583 cases),
- **Crime prevention:** the Police Force (76 cases);

Other reasons include: combatting sales of endangered species suspected by AFCD (1 case); combatting copyright infringement reported by Hong Kong Observatory (2 cases) and the Land Department (3 cases); combatting indecent content by OFCA (6 cases) and combatting inappropriate content by Hongkong Post (2 cases).

## Recommendations

### Make public the current internal guidelines and monitoring mechanism

At the 15 October 2014's Legislative Council meeting, Legislator James To raised the question "of the discrepancies in the procedural guidelines or contents of the forms used by various government departments for making requests to service providers for disclosure or removal of information of their users", and whether the government "will consider standardising such guidelines and forms".

Regrettably, Secretary for Commerce and Economic Development Gregory So said in his written reply that "Since the existing mechanism functions effectively, we do not think it is necessary to establish a separate set of procedures for Internet service providers".

Previously, Legislator Charles Mok asked twice about the details of the government's internal guidelines and monitoring mechanism in 2013 and 2014. But Secretary for Commerce and Economic Development Gregory So and Acting Secretary for Commerce and Economic Development Godfrey Leung chose to keep this crucial information shrouded in secrecy.

Leung said in a general reply to Mok in February 2014 that the government departments will ensure that they only make requests when necessary for the purpose of performing duties, and since the existing mechanism functions effectively, he did not think it is necessary to review the relevant procedures/guidelines. Leung's self-reassuring answer, however, is far from informative and convincing from the public standpoint.

Since the government is keeping its request-making procedures in the dark, the public has no way to know how the government makes requests to service providers, whether the reasons provided by the government agencies (crime prevention and detection, and law enforcement) can be sufficiently justified for accessing users' personal information, whether there are alternative investigation methods without breaching users' privacy, and what would happen if the service providers did not respond to or rejected government requests. In fact, only 70% (3,846) of the 5,511 user information requests issued by the various government agencies in 2013 were granted by service providers.

The lack of transparency on these critical questions risks eroding the public's trust in government operations. The government should reveal its internal guidelines and monitoring mechanism as soon as possible for public review for greater transparency and accountability in the government request-making process.

### Set up an independent oversight body

From February to 15 October 2014, five government departments made 3,025 user data requests, only partially were made under court orders. During the same period, four government agencies made 1,508 data removal requests, none were done under court orders.

At the 15 October 2014's Legislative Council meeting, Legislator James To questioned "whether the authorities will consider reviewing the existing legislation with a view to requiring that a government department must obtain a court order before it may make a request to a service provider for disclosure or removal of its users' information, so as to prevent abuse of personal information and to safeguard the privacy of the members of the public".

Sadly, Secretary for Commerce and Economic Development Gregory So repeatedly replied that "since the existing mechanism functions effectively, we do not think it is necessary to review it."

In 2013, only 'partial' of the government's 5,511 user information requests were issued under a court order, which raises the concern whether the government power is left unchecked when it is trying to access or remove users' online data.

An independent body is needed to challenge requests issued by the government and to judge if such requests are appropriate and necessary before they are sent to service providers. In other words, a due process should be established to oversee the government request-making activities. Correspondingly, there should be an independent agency responsible for examining the results of requests in order to detect problems and defects in the current government request-making mechanism.

Furthermore, there should be different levels of access to user information that the government can apply for based on different levels of importance and urgency of the government departments' criminal investigation and law enforcement activities. In the US, the Electronic Communications Privacy Act sets out three legal processes that government agencies can use to obtain a certain level of user account information from service providers: subpoena, court order and search warrant. These three procedures serve as thresholds to make sure government agencies perform their duties within legal boundaries.

### **Introduce a standard request logging system**

HKTR discovered through our correspondence with government agencies great discrepancies in government departments' request logging systems, which makes it difficult for meaningful comparison and analysis across the board. And there is no sign that the government is making an effort to establish a standard request logging system.

Certain government departments did not keep a record of their individual requests and request results. For example, the Police Force did not keep the numbers of requests it sent to individual companies or the compliance rates of its requests.

Some government agencies did not keep the number of service providers involved in their requests. For instance, the Customs and Excise Department said it did not have

statistics on the number of service providers it made requests to for its 2010 - 2013 user information requests.

Certain departments did not keep the record of the accounts/users affected by their requests. For instance, the Drug Office of the Department of Health did not keep a record of the accounts/users affected for its 2013 data removal requests.

In addition, between 2010 and 2012, some departments did not keep the annual breakdown data. For instance, although the Customs published the lump sum request data from 2010 to 2012 (1,677 data requests, 193 removal requests), it told HKTR that it did not have any statistics on the yearly breakdown of the lump sum data.

The Police, the Customs and the Department of Health are among the largest issuer of user information and content removal requests in the past four years. But none of them have managed to keep a proper record of the requests they issued and the request results.

Proper record management increases government transparency and accountability and is a precondition of open government. It is the obligation of the government to keep a proper record management system for the benefit of the government itself and the public alike. The valuable information held on the request records will not only facilitate government agencies' internal reference, but also give the public an accurate picture of the scale and scope of government's access to their information.

### **Regular disclosure**

At present, the government data and content removal requests were disclosed upon the requests of Legislative Council member Charles Mok. Rather than publishing such information upon request, the government should consider disclosing it on a regular basis, just like the way it publishes on a quarterly basis the statistics on the access to information requests. Furthermore, given the nature of this information, it could be disclosed in an open data format, which would enable easier auditing and analysis.

The government has the chance to be transparent and act in a responsible way by taking the initiative of informing its citizens what it is doing with their private data. Meanwhile, proactive data release can also help improve the government's efficiency and effectiveness, since the public accessibility of the data will reduce the workload of civil servants attending to the public requests, and foster collaboration between the government and social groups to improve the existing mechanism.

### **Extend the scope of disclosure**

The current government disclosure only covers the requests it made to Internet service providers, Internet platforms and websites. But there is a high chance that the government also makes requests to telecom companies. If this is the case, HKTR hopes the government can consider incorporating telecom companies into its request

disclosure mechanism, to give the public a more comprehensive picture of the scale and scope of its data and removal requests.

### **User notification**

Currently there is no law or regulation that allows or prohibits service providers to notify their users of the government requests. As users have the right to know how their personal information is accessed and handled by the government, a user notification system should be duly introduced to allow service providers to tell their users about the relevant government activities, provided such notification won't impede crime investigation or law enforcement.

### **Work with service providers**

During HKTR's correspondence with the government officers, we encountered a few cases where the government told us details of the requests, such as the names of service providers, and on what dates it made individual requests. But in most cases, the government agencies cited business, legal or operational restrictions as reasons for keeping the names, or even the dates, secret.

But there are also cases where the government has to wait for the consent of service providers before revealing their names to HKTR, a process HKTR believes can be improved.

For instance, after HKTR asked Hongkong Post on 22 May 2014 about the name of the website that it made a content removal request to, in the following three months, Hongkong Post's officer for access to information sent a number of emails to the website in question seeking consent for the disclosure. However, HKTR learned on 11 August that the service providers never responded to the government request. As a result, Hongkong Post was unable to release the name of the website.

In another case, both the Companies Registry and the Customs and Excise Department told HKTR that since the question involves the commercial information of a large number of service providers, it is rather impossible for the government to obtain consent from all relevant organisations. Hence, the names of individual service providers were not made public.

In light of the time and effort that government officers need to spend in seeking service providers' consent to reveal their names, it is recommended that the government could work with service providers at the early stage, for instance, when it issues requests to service providers, to come up with a list of what can be and cannot be disclosed.

## Annex I: Exemptions

### Personal Data (Privacy) Ordinance

Hong Kong Data Protection Principle 3 (DPP3) stipulates “unless the data subject has given prior consent, personal data shall be used for the purpose for which they were originally collected or a directly related purpose.”

Pursuant to the Personal Data (Privacy) Ordinance (hereinafter referred to as “the Ordinance”), a data user who contravenes the data protection principles may face level 5 (HKD50,000) or level 6 (HKD100,000) fine and imprisonment for 2 years.

However, Section 58 (1) & (2) of the Ordinance promulgates that personal data is exempt from the provisions of DPP3 if personal data held is for the purpose of

(a) the prevention or detection of crime;

(d) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;

That said, the Ordinance and the privacy commissioner’s website make it clear that the data requests issued by law enforcement (such as the police and the customs) are not legally binding, and it is up to the data user (in this case the Internet/online service providers) to decide whether the data requested by law enforcement agencies is directly related to the agencies’ criminal investigation purposes. If the relevancy is not clear, the data user has the right to decline law enforcement’s data requests. As Section 51 of the Ordinance stipulates:

“Where any personal data is exempt from any provision of this Ordinance by virtue of this Part, then, in respect of that data and to the extent of that exemption, that provision neither confers any right nor imposes any requirement on any person, and the other provisions of this Ordinance which relate (whether directly or indirectly) to that provision shall be construed accordingly.”

#### *Case study*

The case study below was an excerpt from the Office of the Privacy Commissioner for Personal Data, Hong Kong. For more information on this case please refer to the privacy commissioner’s website.

“A bank disclosed a data subject's bank account information to the Police without the data subject’s prescribed consent and without carefully considering whether the exemptions of sections 58(1)(d) and (2) were applicable.

...

The privacy commissioner was of the view that the Bank could not believe that provision of the Data to the Police complied with section 58(1)(d) by simply relying on the letter of the Police, and could not reasonably believe that it would be likely to prejudice the purpose referred by the Police if DPP3 was applicable so that the exemption of section 58(2) of the Ordinance could be relied on. Hence, the Commissioner opined that the Bank's act of providing the Data to the Police had contravened DPP3.”

## Annex II: data source

### Government release

Data below was released by the government upon requests by Legislative Councillor Charles Mok and James To

[2014 data and removal requests](#)

[2013 data requests](#)

[2013 content removal requests](#)

[2010-2012 data requests](#)

[2010-2012 content removal requests](#)

### New data HKTR obtained

The number of acceded data requests from Inland Revenue in 2013: 4

The number of acceded data requests from Police Force in 2013: 2899

The number of service providers involved data requests from Office of the Communications Authority in 2013: 22

The number of service providers involved data requests from Inland Revenue in 2010-2012: 6

The number of acceded data requests from Inland Revenue in 2010-2012: 13

The annual breakdown of 2010-2012 data requests from Hong Kong Police Force, Companies Registry, Inland Revenue, and Office of the Communications Authority

The annual breakdown of 2010-2012 content removal requests from Hong Kong Police Force, Agriculture, Fisheries and Conservation Department, Department of Health, Hong Kong Observatory, Hongkong Post, Lands Department, Office of the Communications Authority

The service providers breakdown of 2010-2013 content removal requests from Drug Office

The service providers breakdown of 2010-2013 content removal requests from Chinese Medicine Division

Names of service providers involved in 2011-2013 content removal requests from Office of the Communications Authority

Names of service providers involved in 2012 content removal requests from Agriculture, Fisheries and Conservation Department

Names of service providers involved in 2011-2012 content removal requests from Companies Registry, Hong Kong Observatory, Lands Department and Hongkong Post

### **Report update log**

Published: 26 September 2014

First update: 16 October 2014 (added new data released by the government on 15 October 2014)

### **Note:**

Hong Kong Transparency Report would not exist if the government were more transparent and voluntarily disclosed information about these requests. To find out more about our project, please check out our website: <http://transparency.jmsc.hku.hk/>

-End-