The “Taiwan Internet Transparency Report” (TITR) is a research project on internet freedom and online privacy conducted by Taiwan Association for Human Rights (TAHR). This project investigate and track the personal data requests and content removal request situation done by government units.

Publisher：Taiwan Association for Human Rights

Author：Ming-Syuan Ho （Project officer for TITR）

Advisors (Name Sort by A-Z):
Ching-Yi Liu (Professor of Graduate Institute of National Development in National Taiwan University, Boardmember of TAHR), Jo-Fan Yu (Head of Policy and Government Relations in Google Taiwan & Hong Kong), Kuo-Wei Wu (CEO of National Information Infrastructure Enterprise Promotion Association), Wen-Tsong Chiou (Associate Research Fellow of Institutum Jurisprudentiae in Academia Sinica, Vice President of TAHR), Tyng-Ruey Chuang (Associate Research Fellow of Institute of Information Science in Academia Sinica)

Cooperative Partners (Name Sort by A-Z):
Eeling Chiu (Secretary-General of TAHR), Kiang, Liwen, Nchild, Pofeng Lee (Chairman of Open Culture Foundation), Ronny Wang, TH Schee (Representative of Open Knowledge Foundation Taiwan), Yu-Tsang Lin (Executive Secretary of Judicial Reform Foundation)

Special Thanks：The Office of Legislator Mei-Nyu You

The URL to download this report is below:
© Taiwan Association for Human Rights 2015
Overview
Introduction

The “Taiwan Internet Transparency Report” is a research project on internet freedom and online privacy conducted by Taiwan Association for Human Rights (TAHR).

According to a news release published on August 27, 2015 by Taiwan Network Information Center (TWNIC), the internet penetration rate in Taiwan has reached 80.3% and the penetration rate of the population aged from 18 to 30 is 100%. The massive internet population means that Taiwan has entered the internet age and that internet has become a must-have tool in people’s everyday lives. However, while enjoying the convenience brought by the internet, are the people in Taiwan fully aware of the risks that they are facing in terms of their internet activities? Do they know how their data is handled (whether provided voluntarily or used involuntarily and unconsciously)? Do they know if their online expressions are categorized as appropriate or inappropriate and how they are treated?

Since 2009, we have incorporated the “International Covenant on Civil and Political Rights” (ICCPR) into our domestic laws. Article 17 of the ICCPR specifies that “No one shall be subjected to arbitrary or unlawful interference with his privacy”. In December 2014, the United Nations General Assembly (UNGA) approved resolution A/RES/69/166 “The right to privacy in the digital age”. In addition to reiterating the importance of the ICCPR’s Article 17, the resolution points out that the government’s approach to collecting personal data may infringe the human rights. In May 2015, David Kaye, a UN Special Rapporteur to the Human Rights Council, illustrated the relations between online privacy and freedom of expression in his report on the promotion and protection of the right to freedom of opinion and expression in the digital age (A/HRC/29/32).
As such, we believe that internet users in Taiwan have the right to know how their data stored in the internet service providers’ database due to internet activities is collected, used, and kept; and which government units would use which mechanisms to discern whether an online expression is appropriate or not and then handle it.

To protect people’s right to know, our government stipulated “The Freedom of Government Information Law” in 2005. The law allows people to request the government to provide related administrative data relating to people’s rights and interests. Therefore, for this TITTR project, we took the initiative to request government organizations to provide us the legal bases, standard operating procedures (SOPs), and statistics of their requests based on the aforementioned law. We hope to obtain the data from the government organizations. Furthermore, we look forward to having positive communications with the government through the request-reply process to let the government know our suggestions for the internet management policy, which protects people’s rights and interests.

We deeply believe that information transparency is the foundation for a government to build its credibility. Particularly since Edward Snowden, a former contractor of the US National Security Agency, revealed the global surveillance programs in 2013, people around the world have been concerned about whether their governments would proactively disclose the information on their collection and use of personal data as well as management on online expressions. We hope that the ROC government can lead the world and set a good example for others by responding to people’s demands and even take the initiative to regularly disclose such data when most nations are uncertain about the information disclosure.

1. Please see the news release in the following link: http://www.twnic.net.tw/download/200307/20150901a.pdf.

---

### Goals

The goals of this TITTR project are categorized based on the timeline and content:

**Short-term goals:**
- To request government units to release related data in recent years.
- To propose suggestions for future improvements based on the existing.
- To ask the government to establish statistics compiling formats data.

**Long-term goals:**
- The government units could proactively announce related data.
- The government units could establish SOPs and internal audit operating.
- To establish an independent organization to supervise the government’s related activities.
## Implementation

### Selection of units

For this project, we sent letters to 42 government and private organizations (institutions), asking them to publish the data on requests for internet personal data and content removal.

<table>
<thead>
<tr>
<th>Organizations</th>
<th>Level</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>National security organization</strong></td>
<td>Level 1</td>
<td>Executive Yuan</td>
</tr>
<tr>
<td></td>
<td>Level 2 or independent</td>
<td>Ministry of the Interior (MOI), Ministry of Justice (MOJ), Ministry of National Defense (MND), Ministry of Finance (MOF), Ministry of Economic Affairs (MOEA), Ministry of Education (MOE), Ministry of Transportation &amp; Communications (MOTC), Ministry of Culture (MOC), Ministry of Foreign Affairs (MOFA), Ministry of Labor (MOL), Ministry of Health and Welfare (MOHW), National Communications Commission (NCC), Coast Guard Administration (CGA), Environment Protection Administration (EPA), Mainland Affairs Council (MAC), Central Election Commission (CEC), Council of Agriculture (COA), Fair Trade Commission (FTC), Financial Supervisory Commission (FSC)</td>
</tr>
<tr>
<td><strong>Central administrative organizations</strong></td>
<td>Level 3</td>
<td>National Immigration Agency (NIA), National Police Agency (NPA), Agency Against Corruption (AAC), Investigation Bureau, Military Police Command, Military Intelligence Bureau, Taxation Administration, Customs Administration, Intellectual Property Office (TIPO), Industrial Development Bureau (IDB)</td>
</tr>
<tr>
<td></td>
<td>Level 4</td>
<td>Criminal Investigation Bureau, 2nd Special Police Corps, 3rd Special Police Corps, Taipei City Police Department, New Taipei City Police Department, Taoyuan City Police Department, Taichung City Police Department, Tainan City Police Department, Kaohsiung City Police Department,</td>
</tr>
<tr>
<td><strong>Judicial Organization</strong></td>
<td></td>
<td>Department of Statistics, Judicial Yuan</td>
</tr>
<tr>
<td><strong>Private organizations entrusted by the government</strong></td>
<td></td>
<td>Institute of Watch Internet Network (iWIN)</td>
</tr>
</tbody>
</table>
Among the 42 units that we enquired, apart from the National Security Bureau, Department of Statistics of the Judicial Yuan, and iWIN, all other units are under the Executive Yuan. Therefore, for the data’s integrity and reference value, we selected not only the Executive Yuan and most of its Level 2 subsidiaries, but also some other Level 2 organizations expected to have related statistics as well as some representative prosecutors and police units for the surveys.

The TTTR survey was conducted via letters. During the process, we also received some additional information, which helped ensure the accuracy. On November 22, 2012, the “Essential Norm and Division of Work Principle for Internet Content Management”, (hereinafter called the “Principle”) was adopted at the 23rd committee meeting of the National Information and Communication Security Taskforce (NICST). The Principle specifies that “Internet platform, content and application services providers are not telecommunications companies so they are not supervised by the National Communications Commission. Any competent authority finds any internet contents or activities violate its regulations, it may directly contact the internet services providers, requesting them to remove inappropriate content immediately and provide the personal data of the publisher.” Furthermore, the Principle even listed the internet content governed by each competent authority. Hence, we include all the authorities listed on the Principle in our mailing list of the survey.

## Selection of data scope

The statistics that we asked the government to provide regarding their requests for internet personal data and content removal covers the followings:

**Request for internet personal data**
- data not voluntarily provided to government organizations by internet users.
- data provided from internet services providers after “direct” requests from government organizations.
- data comprises 1) substantive content (email text, instant messaging text) and metadata in terms of the content (which were not divided in this report) or 2) history data and real-time data in terms of storage.

**Requests for content removal**
- Internet users’ involuntary content removals.
- Content removals due to “direct” requests from government organizations to internet services providers.
- Content including symbols, characters, photos, music, and images.

---

4. Please see the full text of the “Essential Norm and Division of Work Principle for Internet Content Management” in the following link: https://drive.google.com/file/d/0B6XXC2kUbblDV3RaMzNTZ0p6dU-U/view?usp=sharing
Implementation phases

For the implementation of the TITR project, there are basically four phases as listed below:

1. TAHR sent mails to government organizations to survey their requests for internet user data, requests for content removal, and related legal bases and SOPs.

2. TAHR sent mails to these organizations again to follow up on the survey results gained in Phase I, asking for further details about the statistics, SOPs, internal audit operations, and standard documents.

3. TAHR sought a legislator’s assistance, asking the legislator to send mails to the organizations which provided us insufficient data or refused to provide us data in Phase II.

4. TAHR held a press conference or a seminar to release the annual report and also posted the annual report on the internet.
Report
2012-2014 internet personal data requests

Legal bases and procedures

According to Subparagraph 2 of Paragraph 1 of Article 5 of the “Central Regulation Standard Act”, provisions concerning the rights or obligations of the people should be stipulated by a statute. Therefore, government organizations’ requests for internet personal data or content removal due to administrative needs are considered as activities interfering people’s privacy and freedom of speech. Therefore, based on the Act, the government should stipulate relevant provisions as legal bases for government organizations to follow.

During the first two phases of the project, we asked the organizations this part in our mails in hopes to clarify their duties and responsibilities. Below is what we obtained from the organizations in terms of their requests for internet personal data:

<table>
<thead>
<tr>
<th>No.</th>
<th>Unit</th>
<th>Legal bases for internet personal data requests</th>
</tr>
</thead>
</table>
| 1   | National Police Agency                                               | • The Communication Security and Surveillance Act  
• Regulations for government organizations to assist the national intelligence work |
| 2   | Investigation Bureau, Ministry of Justice                            | • Articles 3-1, 11-1, 15, 16 of the Communication Security and Surveillance Act and related enforcement rules |
| 3   | Agency against Corruption, Ministry of Justice                       | • Articles 229-231 of the Code of Criminal Procedure  
• Communication Security and Surveillance Act  
• Directions for prosecutor authorities to implement communication surveillance measures |
| 4   | National Police Agency, Ministry of the Interior                     | • Laws and regulations database  
• MOJ’s web page of “Communication Security and Surveillance” |
| 5   | Criminal Investigation Bureau, National Police Agency                | • Laws and regulations database  
• MOJ’s web page of “Communication Security and Surveillance” |
| 6   | 2nd Special Police Corps (IPR Police)                                | • TIPO’s web page of “Laws”  
• MOJ’s web page of “Communication Security and Surveillance” |
<table>
<thead>
<tr>
<th></th>
<th>2nd Special Police Corps (IPR Police)</th>
<th>• NCC’s web page of “Legal Affairs”</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Coast Guard Administration, Executive Yuan</td>
<td>• Communication Security and Surveillance Act</td>
</tr>
</tbody>
</table>
| 8 | National Communications Commission | • Paragraph 2 of Article 55 of the Telecommunications Act  
• According to Paragraph 2 of Article 7 of the Telecommunications Act, the “Rules Governing Operational Procedures for Telecommunications Enterprises to Handle Inquiries for Communications Records” and the “Rules Governing Operational Procedures for Telecommunications Enterprises to Handle Inquiries for Users’ Data” were stipulated. |
| 9 | National Communications Commission | • Article 24 of the Meteorological Act, and Article 40 of the Administrative Procedure Act |
| 10 | Ministry of Finance | • Paragraph 1 of Article 30 of the Tax Collection Act  
• Paragraphs 1 and 2 of Article 13 of the Customs Act |
| 11 | Ministry of Economic Affairs | • Articles 49 and 50 of the Commodity Inspection Act  
• Articles 42 and 43 of the Weights and Measures Act |
| 12 | Ministry of Health and Welfare | • Paragraphs 1 and 2 of Article 3 and Article 5 of the “Rules Governing Operational Procedures for Telecommunications Enterprises to Handle Inquiries for Communications Records”  
• Paragraphs 1 and 2 of Article 33 of the Mental Health Act  
• Article 26 of the Medical Care Act  
• Article 29 of the Act Governing Food Safety and Sanitation  
• Article 66 of the Pharmaceutical Affairs Act |
| 13 | National Immigration Agency, Ministry of Interior | • Article 89 of the Immigration Act  
• “Rules Governing Operational Procedures for Telecommunications Enterprises to Handle Inquiries for Users’ Data” |
| 14 | Fair Trade Commission | • Subparagraph 2 of Paragraph 1 of Article 27 of the Fair Trade Act  
• Article 40 of the Administrative Procedure Act |
Statistics

Statistics from various units

Below are the replies on statistics from the aforesaid 14 units which claimed to have authorities:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Replies with statistics</th>
<th>Replies without statistics</th>
<th>Never execution in recent 3 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Police Agency, Criminal Investigation Bureau</td>
<td>National Security Bureau</td>
<td>Coast Guard Administration, Executive Yuan</td>
<td></td>
</tr>
<tr>
<td>National Immigration Agency, Ministry of Interior</td>
<td>Investigation Bureau, Ministry of Justice</td>
<td>National Communications Commission</td>
<td></td>
</tr>
<tr>
<td>Ministry of Transportation and Communications</td>
<td>Agency Against Corruption, Ministry of Justice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ministry of Finance</td>
<td>National Police Agency, Ministry of Interior</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ministry of Economic Affairs</td>
<td>Fair Trade Commission</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ministry of Health and Welfare</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd Special Police Corps</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Each unit claimed that the data provided to us has comprised the statistics of the unit and its subsidiaries.
### 2012-2014 internet personal data requests from Criminal Investigation Bureau

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of requests</th>
<th>No. of successful requests</th>
<th>No. of affected users</th>
</tr>
</thead>
<tbody>
<tr>
<td>1H12</td>
<td>302</td>
<td>271</td>
<td>N/A</td>
</tr>
<tr>
<td>2H12</td>
<td>374</td>
<td>339</td>
<td>N/A</td>
</tr>
<tr>
<td>1H13</td>
<td>315</td>
<td>278</td>
<td>N/A</td>
</tr>
<tr>
<td>2H13</td>
<td>341</td>
<td>301</td>
<td>N/A</td>
</tr>
<tr>
<td>1H14</td>
<td>467</td>
<td>388</td>
<td>N/A</td>
</tr>
<tr>
<td>2H14</td>
<td>438</td>
<td>370</td>
<td>N/A</td>
</tr>
</tbody>
</table>

* In 2012-2014, the Criminal Investigation Bureau had 2,237 requests and received 1,947 positive responses so the success rate of 87%.

* The CIB did not provide us the number of affected users in the requests.\(^7\)

---

6. For the above statistics, please see the CIB’s letter Xing-Zi-Zi No. 1041400360 dated March 25, 2015.

7. “N/A” in this report means no data was provided.
### 2012-2014 internet personal data requests from National Immigration Agency

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of requests</th>
<th>No. of successful requests</th>
<th>No. of affected users</th>
</tr>
</thead>
<tbody>
<tr>
<td>1H12</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>2H12</td>
<td>1</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>1H13</td>
<td>1</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>2H13</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>1H14</td>
<td>18</td>
<td>18</td>
<td>N/A</td>
</tr>
<tr>
<td>2H14</td>
<td>2</td>
<td>2</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- In 2012-2014, the National Immigration Agency had 22 requests and received 22 positive responses so the success rate is 100%.
- The National Immigration Agency did not provide us the number of affected users in the requests.

---

8. For the above statistics, please see the National Immigration Agency’s letter Yi-Shu-Zi-An-Yan-Zi No. 1040038924 dated March 27, 2015.
In 2012-2014, the Ministry of Transportation and Communications had 4 requests and received 2 positive responses so the success rate is 50%.

The Ministry of Transportation and Communications provided us the reasons why two of the requests were rejected: 1) The data relating to operations and maintenance was not available because it was in charge by the parent companies based overseas; and 2) The data that the organizations received was not enough for statistics compiling and analysis.

---

9. For the above statistics, please see the MOTC’s letter Jiao-You-Zi No. 1040004037 dated March 25, 2015.
2012-2014 internet personal data requests from Ministry of Finance

In 2012-2014, the Ministry of Finance (MOF) had 60 requests and received 59 positive responses so the success rate is 98.83%.

The MOF provided us the reason why one of the requests was rejected: ISP didn't provide any data.

In 2012-2014, the Ministry of Finance (MOF) had 60 requests and received 59 positive responses so the success rate is 98.83%.

10. For the above statistics, please see the MOF’s letter Tai-Cai-Fa-Zi No. 10413915320 dated March 23, 2015
### 2012-2014 internet personal data requests from Ministry of Economic Affairs

---

**Box5**

For the above statistics, please see the MOEA’s letter Jing-Fa-Zi No. 10404644530 dated March 06, 2015.

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of requests</th>
<th>No. of successful requests</th>
<th>No. of affected users</th>
</tr>
</thead>
<tbody>
<tr>
<td>1H12</td>
<td>137</td>
<td>137</td>
<td>137</td>
</tr>
<tr>
<td>2H12</td>
<td>182</td>
<td>182</td>
<td>182</td>
</tr>
<tr>
<td>1H13</td>
<td>137</td>
<td>137</td>
<td>137</td>
</tr>
<tr>
<td>2H13</td>
<td>176</td>
<td>176</td>
<td>176</td>
</tr>
<tr>
<td>1H14</td>
<td>127</td>
<td>127</td>
<td>127</td>
</tr>
<tr>
<td>2H14</td>
<td>302</td>
<td>302</td>
<td>302</td>
</tr>
</tbody>
</table>

- In 2012-2014, the Ministry of Economic Affairs (MOEA) had 1,061 requests and received 1,061 positive responses so the success rate is 100%.
- The MOEA’s 1,061 requests affected a total of 1,061 users. It means that 1 user was affected per request.

---

11. For the above statistics, please see the MOEA’s letter Jing-Fa-Zi No. 10404644530 dated March 06, 2015.
**Box 6**

2012-2014 internet personal data requests from Ministry of Health and Welfare

For the above statistics, please see the MOHW's letter Wei-Bu-Fa No. 1043160037 dated March 31, 2015.

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of requests</th>
<th>No. of successful requests</th>
<th>No. of affected users</th>
</tr>
</thead>
<tbody>
<tr>
<td>1H12</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2H12</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>1H13</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2H13</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>1H14</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2H14</td>
<td>6</td>
<td>6</td>
<td>8</td>
</tr>
</tbody>
</table>

- The Ministry of Health and Welfare (MOHW) only provided us the data in 2H14, which only relates to the statistics prescribed in Subparagraph 2 of Paragraph 1 of Article 3 of the “Rules Governing Operational Procedures for Telecommunications Enterprises to Handle Inquiries for Users’ Data” and Article 5 of the Telecommunications Act.

- In 2H14, the MOHW had 6 requests and received 6 positive responses so the success rate is 100%.

- The MOHW’s 6 requests affected a total of 8 users. It means that 1.33 users were affected per request.

12. For the above statistics, please see the MOHW’s letter Wei-Bu-Fa No. 1043160037 dated March 31, 2015.
2012-2014 internet personal data requests from 2\textsuperscript{nd} Special Police Corps\textsuperscript{13}

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of requests</th>
<th>No. of successful requests</th>
<th>No. of affected users</th>
</tr>
</thead>
<tbody>
<tr>
<td>1H12</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2H12</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>1H13</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2H13</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>1H14</td>
<td>651</td>
<td>651</td>
<td>651</td>
</tr>
<tr>
<td>2H14</td>
<td>867</td>
<td>867</td>
<td>867</td>
</tr>
</tbody>
</table>

- The 2\textsuperscript{nd} Special Police Corps only provided us the data in 2014.
- In 2014, the 2\textsuperscript{nd} Special Police Corps had 1,581 requests and received 1,581 positive responses so the success rate is 100%.

\textsuperscript{13} For the above statistics, please see the 2\textsuperscript{nd} Special Police Corps’ letter Bao-Er-Xing-Zi No. 1040063651 dated May 19, 2015.
Overview on statistics data about personal data requests from various units in 2012-2014

Box 8

Overview on numbers of internet personal data requests from various units in 2012-2014

<table>
<thead>
<tr>
<th>Unit</th>
<th>No. of requests</th>
<th>% of total requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIB</td>
<td>2237</td>
<td>45.6%</td>
</tr>
<tr>
<td>2nd Special Police Corps</td>
<td>1518</td>
<td>30.9%</td>
</tr>
<tr>
<td>MOEA</td>
<td>1061</td>
<td>21.6%</td>
</tr>
<tr>
<td>MOF</td>
<td>60</td>
<td>1.2%</td>
</tr>
<tr>
<td>NIA</td>
<td>22</td>
<td>0.4%</td>
</tr>
<tr>
<td>MOHW</td>
<td>6</td>
<td>0.1%</td>
</tr>
<tr>
<td>MOTC</td>
<td>4</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

- The aforesaid data was unable to fully reflect the situation in 2012-2014. In addition to the units which did not provide us any data, MOHW and the 2nd Special Police Corps only provided us the (partial) data in 2014.

- In 2012-2014, there were at least 4,908 requests for personal data. Most of the requests were from the police, which totaled 3777, accounting for 77% of all requests. The MOEA came in the second with 1,061 requests, accounting for 21.6% of the total requests.

14. The above statistics is based on the data provided by various units prescribed in the previous section.
### Overview on numbers of affected users in 2012-2014

The aforesaid data was unable to fully reflect the situation in 2012-2014. Despite the units which did not provide us any data, CIB and the National Immigration Agency did not provide us such data, either.

In 2012-2014, our government had at least requests for personal data of 4,129 users. The MOF and the 2nd Special Police Corps had the most requests, which were 1,541 and 1,518 requests, respectively. The requests from these two units accounted for 74% of the total requests. The MOEA came in the third on the list with 1,061 requests, accounting for 26% of all requests.

<table>
<thead>
<tr>
<th>Unit</th>
<th>No. of users</th>
<th>% of total users</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIB</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>2nd Special Police Corps</td>
<td>1518</td>
<td>36.8%</td>
</tr>
<tr>
<td>MOEA</td>
<td>1061</td>
<td>25.7%</td>
</tr>
<tr>
<td>MOF</td>
<td>1541</td>
<td>37.3%</td>
</tr>
<tr>
<td>NIA</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>MOHW</td>
<td>8</td>
<td>0.2%</td>
</tr>
<tr>
<td>MOTC</td>
<td>1</td>
<td>0%</td>
</tr>
</tbody>
</table>

*Figure: No. of users for each unit from 2012-2014*
Overview on reasons for internet personal data requests in 2012-2014

For crime investigation, 76.71%

<table>
<thead>
<tr>
<th>Item</th>
<th>Unit</th>
<th>No. of requests</th>
<th>% of total reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>For crime investigation</td>
<td>CIB</td>
<td>2237</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2nd Special Police Corps</td>
<td>1518</td>
<td>76.71%</td>
</tr>
<tr>
<td></td>
<td>MOHW</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MOTC</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>For investigating acts on illegal display and sale of products or legal measuring instruments</td>
<td>MOEA</td>
<td>1061</td>
<td>21.62%</td>
</tr>
<tr>
<td>For investigating taxation data or reporting from citizen</td>
<td>MOF</td>
<td>60</td>
<td>1.22%</td>
</tr>
<tr>
<td>For investigating illegal advertisements for international marriage matching services</td>
<td>NIA</td>
<td>22</td>
<td>0.45%</td>
</tr>
</tbody>
</table>
Reasons for unwilling (or unable) to disclose data

Regarding the requests for internet personal data, 14 units have the authorities to do so while only 7 of them provided us the statistics. However, among those which provided partial statistics or no statistics at all, some gave us clear reasons while some only gave simple replies for not being able to provide us full statistics. As not all the reasons that we received were very specific, so we called the units one by one after receiving their replies to look into the reasons for lack/short of the statistics. After our enquiries, the reasons could be categorized as the following three:

No statistics was compiled

- No regular operations for compiling the statistics
  Only the Criminal Investigation Bureau said that they have had related statistics but other units have never established any statistical systems before we enquired them.

- Official documents transferred to other units
  The Ministry of Interior and National Police Agency would normally transfer the official documents to the CIB after receiving them. They didn’t tell us the reasons for the document transfer and we didn’t know who made the decisions to transfer the documents to the CIB.

- Short of staff
  The Agency Against Corruption, Taichung City Police Department, Tainan City Police Department, Kaohsiung City Police Department all told us that they were unable to compile the statistics due to short of staff.

- Few cases
  The Fair Trade Commission indicated in its reply that there were only a few cases so it had yet compiled the statistics.

- No statistics
  The Ministry of Health and Welfare indicated in its second reply to us that it had no statistics other than that relating to the Telecommunications Act.

- The statistics was not precise enough so it would not mean much if it was provided to us.
  Taipei City Police Department told us over the phone that it has yet established any standard regular statistical system. Hence, even if it provided us the existing statistics, it wouldn’t be comprehensive. Therefore, it decided not to provide us any as it wouldn’t mean much.

NOTE: After the Office of Legislator You Mei-nu sent a mail to request for the statistics, the MOHW provided us related statistics of the Food and Drug Administration, the Department of Mental and Oral Health, the Department of Medical Affairs. However, we decided not to include the statistics in this report because 1) the statistics was for 2013-2015, not for 2012-2014 which we needed; and 2) the statistics from the aforementioned three units is not divided by year. Overall, the Food and Drug Administration said that it successfully obtained from the ISPs 1,571 pieces of information ranging from January 1, 2014 to end July, 2015 and asked them to remove 1,571 web pages. In addition, the Department of Mental and Oral Health said that it removed 144 personal web pages from 2013 to 2015. However, the Department of Medical Affairs indicated it had no relevant cases.

15. Please see the FTC’s letter Gong-Fa-Zi No. 1040004494 dated April 7, 2015.
No statistics was provided

- Concerns over the Personal Information Protection Act and the Freedom of Government Information Law
  - Ministry of Health and Welfare (MOHW): In the first response from the MOHW, it quoted Paragraph 1 of Article 19 of the “Personal Information Protection Act” and Paragraph 1 of Article 18 of the “Freedom of Government Information Law” but gave no further explanation. The MOHW seems to imply that the data that we requested for the TITR project was considered as the “personal information”, so it couldn’t provide any of them unless there is a specific purpose. So we replied that the statistics we requested for this project is simply the statistical data, which is not relevant to “personal data” of any natural persons at specific time and places. Therefore, it is not under the jurisdiction of the “Personal Information Protection Act”. Afterwards, the MOHW provided us some statistics in its 2nd response.
  - Ministry of Finance (MOF): In the first response from the MOF, it rejected our request for concerns over leaking personal information. It pointed out that if it provides us the number of affected users, it would cause difficulties in future tax collection. Therefore, we tried to communicate with the MOF again, explaining that the data is not relevant to any specific time, places, and units but just some figures so there is no need to be concerned and it wouldn’t cause any problems. After that, the MOF provided us related data in its second reply.

- Relating to non-disclosure during investigations
  - The Agency Against Corruption of the Ministry of Justice replied to us that it has no related statistics for us due to difficulties listed below: 1) there are too many statistics for evidence investigation and collection; 2) the data may not be all available as prosecutors may ask investigators to provide them related documents for investigations; and 3) there are provisions on non-disclosure during investigations. Taipei City Police Department said that it couldn’t provide us the statistics because the statistics is categorized for “internet crime investigations”, which is not allowed for disclosure based on the “Freedom of Government Information Law”. Although we tried to communicate with these units again, we still couldn’t obtain related statistics.

- Provisions prescribed in the Communication Security and Surveillance Act
  - The National Security Bureau told us in phone that it was unable to disclose related information based on Paragraph 2 of Article 16-1 of the Communication Security and Surveillance Act.

16. Please see the MOHW’s letter Wei-Bu-Fa-Zi No. 1040001762 dated February 15, 2015.
17. Please see the MOHW’s letter Wei-Bu-Fa-Zi No. 1043160037 dated March 31, 2015.
18. Please see the MOF’s letter Tai-Cai-Fa-Zi No. 1041390763 dated February 11, 2015.
20. Please see the AAC’s letter Lian-Su-Zi No. 10406000690 dated February 6, 2015.
21. Please see the Taipei City Police Department’s letter Jing-Xing-Zi-Zi No. 10431011600 dated March 30, 2015.
Others

- Never exercising the authorities:
  - Coast Guard Administration: According to Article 10 of “The Coast Guard Act”, some of the Coast Guard Administration personnel are judicial police or judicial police officers and have the authority to conduct criminal investigations based on the “Communication Security and Surveillance Act”. However, per the response from the Coast Guard Administration, the communication statistics requested or retrieved by the Administration in the past is traditional telecommunication statistics due to its duties so it never had any requests for internet personal data or content removal.
  - National Communications Commission (NCC): Previously, the NCC replied to the TITR project team that the legal bases for its related requests to telecommunication enterprises, users of dedicated telecommunications, or installers and users of radio stations were based on Paragraph 2 of Article 55 and Paragraph 2 of Article 7 of the Telecommunication Act. However, when our project team and the office of legislator Yu Mei-nu further enquired for relevant statistics, the NCC said that it has never had related requests for three years.

- Seeking assistance from other organizations
  - The Central Election Commission (NEC) pointed out that if any one violates the government’s election and recall acts on the internet, it would seek other organizations’ assistance to investigate the identities of the offenders based on Article 19 of the Administrative Procedure Act. However, the Central Election Commission itself has no related authority.

- No replies
  - The Military Police Command didn’t reply any mail.

- Refusing to cooperate
  - The Investigation Bureau of the Ministry of Justice is the least cooperative unit. On May 8, 2015, a responsible person from the Investigation Bureau repeatedly told us over the phone that the Bureau has never engaged in illegal wiretapping activities and even advised the TAHR to discontinue the TITR project.

22. Please see the CGA’s letter Shu-Qing-San-Zi No. 1040001068 dated February 3, 2015.
23. Please see the NCC’s letter Tong-Chuan-Tong-Xun-Zi No. 10341044200 dated November 17, 2014.
24. Please see the NCC’s letter Tong-Chuan-Ping-Tai-Zi No. 10441005600 dated February 17, 2015.
25. Please see the NEC’s letter Chong-Xuan-Fa-Zi No. 1040000567 dated March 20, 2015. The NEC told us that its requests were based on the “Administrative Penalty Act and Administrative Procedure Act”. However, in reply to our further enquiry, the NEC confirmed that its requests were based on Article 19 of the Administrative Procedure Act.
Comprehensive statistics review

Based on the legal bases provided by the 14 units and the statistics provided by the 7 units, we have the following findings:

Legal Bases and SOPs

- Most units don’t have SOPs.
  Among all the units, only the Ministry of Transportation and Communications has the SOP for their administrative staff and related enterprises to follow and cooperate. As to other units, they were either not very clear about the statistics or have yet consolidated it.

- Few units refused to provide specific legal bases.
  Few units, such as the National Security Bureau, the Agency Against Corruption, the National Police Agency, the Criminal Investigation Bureau, and the 2nd Special Police Corps provided us ambiguous legal information.

- No units provided us their internal audit SOPs
  Apart from the Council of Agriculture, which mentioned about its internal audit SOPs, all the other units didn’t mention their internal audit mechanisms on personal data collection, use, storage, and destruction.

Statistics

- The statistics from some units was incomplete in terms of year and scope.
  Some units were unwilling and unable to provide us statistics, such as National Security Agency, Investigation Bureau, Agency Against Corruption, National Police Agency, Fair Trade Commission. However, some replied and provided us related statistics. The followings are the units which provided very little information:
    - Criminal Investigation Bureau: It didn’t provide us statistics about the number of affected users, reasons and number of rejections, legal bases and number of requests.
    - 2nd Special Police Corps: It only provided the statistics in 2014.
    - Ministry of Health and Welfare (MOHW): It provided us the statistics only from July to December of 2014 and only relating to the Telecommunications Act. The MOHW previously told us that it has five legal bases.

- Big gap between the statistics provided by the government and enterprises
  Among all enterprises that would regularly release transparency reports according to a list from the Access, five of them (Google, Apple, Facebook, Microsoft, and Yahoo) have disclosed the statistics of Taiwan government's requests for personal data. The chart below shows that in the first half of 2014, these five enterprises received 4,181 data requests from our government. However, according to the statistics provided by some of the Taiwan government organizations as mentioned above, the number of the government’s data requests totaled only 4,908 in 2012-2014. As a result, we assumed that if we could obtain more statistics from local enterprises, the gap between the figures provided by the government organizations and those provided by the enterprises is expected to significantly increase.

26. In response to our first official letter, the National Police Agency answered the questions for itself and its subsidiary, the Criminal Investigation Bureau.

27. There are currently over 50 enterprises that would periodically release their transparency reports to actively disclose the requests that they received from the government organizations as well as their responses and polices. For the data below, please see the following link for the transparency reporting statistics consolidated by the Access: https://www.accessnow.org/pages/transparency-reporting-index.
The TTTR project team believes that the big gap could be due to the following reasons:

- A significant amount of statistics has not been disclosed;
- The content of the personal data is different in terms of the perspectives from the government and enterprises.

- Lacking statistics on communication surveillance

All the statistics obtained from the government units shows that no requests from the units were made pursuant to the "Communication Security and Surveillance Act".

Article 16-1 of the “Communication Security and Surveillance Act”, amended in 2014, specifies what an annual report on communication surveillance shall cover. As such, the TTTR project team asked the Department of Statistics of the Judicial Yuan about relevant statistics and then obtained the statistics of various “lines” of communications in the second half of 2014.

According to the statistics provided by the Judicial Yuan, there are eight types of “lines” for communication surveillance: 1) local telephone and mobile phone accounts, 2) IMEI, 3) IMSI, 4) HiNet ADSL accounts, 5) internet phone accounts (e.g. Skype), 6) email accounts, 7) IP addresses; and 8) others.

In the second half of 2014, the prosecutors filed 14,292 requests for communication surveillance on 21,125 lines. The portfolio is shown as follow:

![Pie chart showing the percentage of requests for communication surveillance](chart.png)

**% of lines relating to requests for communication surveillance**

- **local telephone and mobile phone accounts, 89.31%**
- **IMEI, 8.01%**
- **Internet phone accounts, (e.g. Skype), 0.28%**
- **Hinet ADSL accounts, 0.05%**
- **Email accounts, 0.07%**
- **IP address, 0.00%**
- **IMSI, 0.09%**
- **Others, 2.18%**

---

28. For related data, please see the Statistics Department’s letter Chu-Tong-Yi-Zi No. 1040013189 dated May 21, 2015, or the 2014 judicial statistics of the Judicial Yuan in the following link: http://www.judicial.gov.tw/juds/suryear103/10/08.pdf.
Among the lines relating to the requests for communication surveillance, the courts approved requests for 14,532 lines and rejected requests for 6,593 lines (31% of total requests). The details are listed below:

<table>
<thead>
<tr>
<th>No</th>
<th>Type of line</th>
<th>No. of requests filed by prosecutors</th>
<th>No. of lines requested for surveillance by prosecutors</th>
<th>No. of lines for surveillance approved by district courts</th>
<th>No. of lines for surveillance rejected by district court</th>
<th>Rejection ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Local telephone and mobile phone accounts</td>
<td>12841</td>
<td>18866</td>
<td>12923</td>
<td>5943</td>
<td>31.5%</td>
</tr>
<tr>
<td>2</td>
<td>IMEI</td>
<td>1093</td>
<td>1693</td>
<td>1193</td>
<td>500</td>
<td>29.5%</td>
</tr>
<tr>
<td>3</td>
<td>IMSI</td>
<td>7</td>
<td>19</td>
<td>16</td>
<td>3</td>
<td>15.8%</td>
</tr>
<tr>
<td>4</td>
<td>HiNet ADSL accounts</td>
<td>8</td>
<td>11</td>
<td>10</td>
<td>1</td>
<td>9.1%</td>
</tr>
<tr>
<td>5</td>
<td>Internet phone accounts (e.g. Skype)</td>
<td>47</td>
<td>60</td>
<td>50</td>
<td>10</td>
<td>16.6%</td>
</tr>
<tr>
<td>6</td>
<td>Email accounts</td>
<td>12</td>
<td>14</td>
<td>10</td>
<td>4</td>
<td>28.6%</td>
</tr>
<tr>
<td>7</td>
<td>IP addresses</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>8</td>
<td>Others</td>
<td>283</td>
<td>461</td>
<td>329</td>
<td>132</td>
<td>28.6%</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>14292</td>
<td>21125</td>
<td>14532</td>
<td>6593</td>
<td>31.2%</td>
</tr>
</tbody>
</table>

Based on the statistics received from the Judicial Yuan, the most conservative interpretation would be categorizing Items 4, 5, 6, 7 as the items “directly” related to internet. Accordingly, in the second half of 2014, a total of 68 lines were directly related to internet.

None of the government units, including the Ministry of Justice and various police organizations, told us that they had engaged in any information collecting or monitoring activities based on the Communication Security and Surveillance Act.

As to why the statistics from the Judicial Yuan is inconsistent with the statistics provided by other organizations, we assume there could be three reasons:

- The organizations didn't have complete statistics.
- The statistics relating to communication surveillance was held by the units which did not provide us anything.
- As communication surveillance is not allowed without the prosecutor’s permission, the responsible units therefore didn’t include the communication surveillance requests in the statistics.
Other cases and review

- Statistics from local enterprises

With the help from the Office of Legislator You Mei-nu, we also obtained some statistics from several local enterprises which refused to reveal their identities. The statistics includes the number of the government’s data requests, the number of the enterprises’ responses with statistics, the number of affected users, the numbers of various government units’ data requests, legal bases provided by the units, etc. The details are as below:

1) Related statistics of the government’s data requests

According to the statistics provided by the enterprises, during 2013-2015, the government had a total of 5,292 requests for internet personal data from the enterprises and received 5,292 positive responses. Hence, the success rate is 100%. The 5,292 responses involved a total of 9,932 users, representing 1.88 users per request.

2) Numbers of various government units’ request

In addition, these enterprises also provided us the 2013-2015 statistics in terms of the breakdowns of the % of total requests or affected users:

29. The statistics from the two enterprises was for 2013-2015. Although the statistics period (2013-2015) is not what we previously asked for (2012-2014), it wouldn’t affect the analysis and opinions of this project.

30. We previously asked the enterprises to provide the “numbers of requests” that they received from the government units. However, some enterprises provided us the “numbers of requests”, yet some others provided us the “numbers of affected users”. As it was difficult to consolidate the inconsistent statistics, we categorized the data into two types: Type I and Type II. We assume that the numbers of requests are highly related to the numbers of affected users, which is the more requests, the more affected users. However, it could also be another situation, which is multiple requests all targeted the same user. Hence, the “number of requests” not necessarily means the “number of affected users”. Accordingly, the two types of data were unable to be combined and had to be listed concurrently at the same time.
Below are the government organizations' legal bases according to the statistics provided by local enterprises:

3) Regarding the legal bases claimed by the government organizations

Below are the government organizations’ legal bases according to the statistics provided by local enterprises:

<table>
<thead>
<tr>
<th>Unit</th>
<th>Response from government unit</th>
<th>Response from local enterprises</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation Bureau</td>
<td>no requests for communication surveillance</td>
<td>% of total requests: 3.83%</td>
</tr>
<tr>
<td>NCC</td>
<td>no requests for communication surveillance</td>
<td>% of total affected users: 0.11%</td>
</tr>
<tr>
<td>Coast Guard Administration</td>
<td>No requests for internet communications and other communication surveillance activities targeted at conventional communications.</td>
<td>% of total affected users: 0.13%</td>
</tr>
<tr>
<td>Military Police Command</td>
<td>no response</td>
<td>% of total affected users: 0.11%</td>
</tr>
</tbody>
</table>

With respect to the inconsistent responses, the TITR project team suggests that the government organizations should have more specific or precise methods for compiling the statistics as well as better internal communication to avoid missing any statistics of relevant cases.

3) Regarding the legal bases claimed by the government organizations

Below are the government organizations’ legal bases according to the statistics provided by local enterprises:
Legal bases claimed by the government organizations

- Articles 229-231 of the Code of Criminal Procedure
- Article 3 of the “Rules Governing Operational Procedures for Telecommunications Enterprises to Handle Inquiries for Users’ Data”
- Articles 15, 16, 20 of the Personal Information Protection Act
- Article 27 of the Fair Trade Act
- Paragraph 2 of Article 7 of the Telecommunications Act
- Article 33 of the Enforcement Rules of the Immigration Act
- Article 70 of the Protection of Children and Youths Welfare and Rights Act

Regarding the above legal bases provided by the enterprises, Articles 15, 16, 20 of the “Personal Information Protection Act” and Article 70 of the “Protection of Children and Youths Welfare and Rights Act” were not mentioned in the government organizations’ previous responses (see P7-8). Also, the Fair Trade Commission (competent authority for the Fair Trade Act) was not on the list of the government units previously provided by the enterprises (see P29).

- Standard form and wrong legal bases

During our survey conducted this year, a company that refused to identify itself provided us a document issued by the police when requesting for its users data.

The above screenshot shows the following messages:
1. The police has already had a standard form for requesting enterprises to provide users’ data.
2. The prosecutors’ offices, police units, and the MOJ’s Investigation Bureau probably share the same standard form.
3. The legal basis, the “Organic Act for Investigation Bureau, Ministry of Justice”, that the MOJ’s investigation Bureau uses was under the “administrative organization law” rather than the “administrative action law”. Therefore, the Investigation Bureau is unable to use either Article 2 or Article 14 as legal bases to request for users’ data.
Inappropriate to apply the Communication Security and Surveillance Act to retrieve information on IP addresses, users’ data, and email content

On June 24, 2014, Yahoo sent a letter to the Ministry of Justice (MOJ) to enquire if it is appropriate to apply to the newly-amended Communication Security and Surveillance Act to request for users’ IP addresses, email content, and account data. On October 17, 2014, the MOJ replied in its letter, Fa-Jian-Zi No. 10300162120, that if an organization intends to retrieve information on an IP address generated by an Internet Access Service Provider (IASP) and related data, it needs to comply with the Communication Security and Surveillance Act; however, if it intends to retrieve information on an IP address generated by a non-IASP, it does not need to abide by the Communication Security and Surveillance Act because its services are not telecommunication businesses related. Accordingly, the users’ data of a non-telecommunication enterprise is not subject to the protection prescribed in the Communication Security and Surveillance Act. As to the email content, if it has already been stored, then the email content is not subject to the protection prescribed in the said Act, either. In view of the above-mentioned, it seems that there are two shortcomings in the said Act:

- **Limited protection**: Most of the websites commonly used by the public are not owned by the telecommunications enterprises. Therefore, there is no need for the government units to abide by the said Act if they want to retrieve

- **Logically contradictory in legislation**: In the data protection policies of most enterprises (e.g. Google, Microsoft, etc.), the stored email content and stored communication records, which relate to the actual substance of data, are subject to even higher-level protection as they are even more sensitive compared to IP. Hence, a government organization cannot obtain such data without very powerful legal documents. In Taiwan, the Communication Security and Surveillance Act can protect the data relating to some IP addresses but cannot protect all the stored email content for the time being. Therefore, this is obviously not in line with the current global trends and international policies.
### 2012-2014 removal requests

#### Legal bases and procedures

Regarding the requests for removals of “online expressions”, six units claimed that they have the authority or related operations. The legal bases provided by them are as follows:

<table>
<thead>
<tr>
<th>No.</th>
<th>Unit</th>
<th>Legal bases for content removal requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MOTC</td>
<td>• Paragraph 1 of Article 17, Paragraph 1 of Article 18, and Paragraph 2 of Article 24 of the Meteorological Act</td>
</tr>
<tr>
<td>2</td>
<td>MOEA</td>
<td>• Paragraph 4 of Article 6 and Paragraph 2 of Article 60 of the Commodity Inspection Act</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Articles 20 and 55 of the Weights and Measures Act</td>
</tr>
<tr>
<td>3</td>
<td>CIB</td>
<td>none</td>
</tr>
<tr>
<td>4</td>
<td>NIA</td>
<td>• Article 34 of the Act Governing Relations between the People of the Taiwan Area and the Mainland Area</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Article 6 of Regulations for Advertising Goods, Labor and General Services of the Mainland Area in the Taiwan Area</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Paragraph 3 of Article 58 of the Immigration Act</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The Telecommunications Act</td>
</tr>
<tr>
<td>5</td>
<td>NCC</td>
<td>• Based on the “Essential Norm and Division of Work Principle for Internet Content Management”, the way for managing the internet content is the same as that for managing the social entity. Organizations may request internet services providers to remove specific content according to their duties and responsibilities.</td>
</tr>
<tr>
<td>6</td>
<td>MOHW</td>
<td>• Based on Articles 46 and 49 of the Protection of Children and Youths Welfare and Rights Act, iWIN is in charge of handling complaints on inappropriate internet content. iWIN may either forward the complaints to other responsible units or directly demand internet services providers or website administrators to remove the inappropriate content.</td>
</tr>
</tbody>
</table>

31. For more details of the aforesaid provided by various units, please see the sources listed below.
In 2012-2014, the MOEA had 1,206 removal requests and received 1,101 positive responses so the success rate of 91.3%.

The MOEA’s 1,206 requests involved a total of 1,207 items, meaning an average of 1 item involved per request.

32. For the above statistics, please see the MOEA’s letter Jing-Fa-Zi No. 10404644530 dated March 6, 2015.
**Box 12** 2012-2014 content removal requests from Criminal Investigation Bureau

For the above statistics, please see the CIB’s letter Xing-Zi-Zi No. 1041400360 dated March 25, 2015.

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of removal requests</th>
<th>No. of successful removals</th>
<th>No. of affected items</th>
</tr>
</thead>
<tbody>
<tr>
<td>1H12</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2H12</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1H13</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2H13</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1H14</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2H14</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

- In 2012-2014, the CIB had 4 removal requests and received 4 positive responses so the success rate is 100%.
- The CIB’s 4 requests involved a total of 5 items, meaning an average of 1.25 items involved per request.

33. For the above statistics, please see the CIB’s letter Xing-Zi-Zi No. 1041400360 dated March 25, 2015.
For the above statistics, please see the NIA’s letter Yi-Shu-Yan-Zi No. 1040038924 dated March 27, 2015.

In 2012-2014, the NIA had 22 removal requests and received 22 positive responses so the success rate is 100%.

The NIA's 22 requests involved a total of 22 items, meaning an average of 1 item involved per request.

---

34. For the above statistics, please see the NIA’s letter Yi-Shu-Yan-Zi No. 1040038924 dated March 27, 2015.
In 2012-2014, the MOTC had 2 removal requests and received 2 positive responses so the success rate is 100%.

The MOTC’s 2 requests involved a total of 2 items, meaning an average of 1 item involved per request.

35. For the above statistics, please see the MOTC’s letter Jiao-You-Zi No. 1040004037 dated March 25, 2015.
Box15 Overview on content removal requests from various units in 2012-2014

<table>
<thead>
<tr>
<th>Unit</th>
<th>No. of requests</th>
<th>% of total requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOEA</td>
<td>1206</td>
<td>97.7%</td>
</tr>
<tr>
<td>NAB</td>
<td>22</td>
<td>1.8%</td>
</tr>
<tr>
<td>CIB</td>
<td>4</td>
<td>0.4%</td>
</tr>
<tr>
<td>MOTC</td>
<td>2</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

- The above data may not fully reflect the situation in 2012-2014 because the MOHW did not provide related statistics.
- In 2012-2014, there were at least 1,234 requests for information. These requests were mostly from the MOEA (1,206) and NIA (22), which respectively accounted for 97.8% and 1.8% of total requests.

36. For the statistics of this section, please see the statistics provided by various units in the previous section.
### Overview on items affected by content removal requests in 2012-2014

<table>
<thead>
<tr>
<th>Unit</th>
<th>No. of Items</th>
<th>% of total items</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOEA</td>
<td>1207</td>
<td>97.7%</td>
</tr>
<tr>
<td>NAB</td>
<td>22</td>
<td>1.8%</td>
</tr>
<tr>
<td>CIB</td>
<td>5</td>
<td>0.4%</td>
</tr>
<tr>
<td>MOTC</td>
<td>2</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

- In 2012-2014, our government organizations had at least tried to remove 1,236 internet content items. Most of them were from the MOEA, requesting to remove 1,207 items (97.7% of total requests). The NIA came in second, requesting to remove 22 items (1.8% of total requests).
### Overview on reasons of content removal requests in 2012-2014

#### Violating Paragraph 4 of Article 6 of Commodity Inspection Act, 61.36%

<table>
<thead>
<tr>
<th>Item</th>
<th>Unit</th>
<th>No. of total reasons</th>
<th>% of total reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violating Paragraph 4 of Article 6 of Commodity Inspection Act</td>
<td>MOEA</td>
<td>751</td>
<td>62%</td>
</tr>
<tr>
<td>Violating Article 20 of Weights and Measures Act</td>
<td>MOEA</td>
<td>444</td>
<td>36%</td>
</tr>
<tr>
<td>Illegally posting advertisements for international marriage matching</td>
<td>NIA</td>
<td>22</td>
<td>2%</td>
</tr>
<tr>
<td>disseminating false information on earthquakes, which may possibly cause public panic</td>
<td>MOTC</td>
<td>2</td>
<td>0.1%</td>
</tr>
<tr>
<td>defamation</td>
<td>CIB</td>
<td>2</td>
<td>0.1%</td>
</tr>
<tr>
<td>obscenity and nudity</td>
<td>CIB</td>
<td>2</td>
<td>0.1%</td>
</tr>
<tr>
<td>Stealing another user’s account</td>
<td>MOEA</td>
<td>1</td>
<td>0.08%</td>
</tr>
</tbody>
</table>
Reasons for unwilling (or unable) to disclose statistics

Compared to the statistics on internet personal data requests, the statistics on content removal requests shows that only six units claimed to have the authority for removal requests or provided us related statistics. Among them, four units provided more comprehensive statistics. The remaining two units, NCC and MOHW, didn't provide us the statistics but shared some information relating iWIN with us. For this part, we received less reasons for unwilling (or unable) to disclose statistics from the units because only a few units were involved. The related reasons are compiled as below:

- No statistics
  The MOHW said in its response that it was unable to provide us the data because it has no related statistics.

- Unable to provide the statistics without the competent authorities’ permissions
  iWIN told us over a phone conversation in June 2015 that it requires the NGC’s permission to disclose the figures on the cases relating to the public’s removal complaints and the government's removal requests.

Comprehensive statistics review

Based on the statistics provided by the aforesaid 6 units, we had the following findings:

Legal bases and SOPs

- Most units don’t have SOPs.
  Among all the units, only the Ministry of Transportation and Communications has the SOP for their administrative staff and enterprises to follow and cooperate. As to other units, their administrative staff members need to learn on their own.

- Only a few units didn’t provide us the legal bases.
  The CIB only provided us the statistics on removal requests but didn’t give us any information on related legal bases.

- No units provided us their internal audit SOPs.
  No units mentioned their internal audit mechanisms relating to personal information collection, use, storage, and destruction.

Statistics

- The success rate claimed by the government organization is very different from that provided by related enterprises.
  Based on the statistics provided by the government organizations, they had 1,234 requests and received 1,129 positive responses in 2012-2014. The success rate is around 91.5%. However, compared to the statistics provided by related enterprises in the same period of time, the average success rate is way lower than that claimed by the government organizations. Let’s take Google as an example, the success rates in terms of the actual content removals from Google versus the government removal requests were between 0% and 30% in various timeframes. It is way lower than the success rate of 91.5% based on the government’s statistics.
With respect to such a big gap, we assume that there could be two reasons:

a. The requests from the government organizations, which provided us the statistics, were mostly not for Google.

b. The requests from the government units, which didn’t provide us any statistics, were mostly unsuccessful.

- Only a few units didn’t provide us the statistics.
  
  In the response from the MOHW, it said it has no statistics about the requests for content removal.

- The prosecutors and police units only had few requests.
  
  Among the 1,234 removal requests in 2012-2014, only 4 requests were from the prosecutors’ offices and police units, accounted for only 0.3% of the total requests.

- Below are the key points of the information relating to iWIN in the NCC and MOHW’s replies:
  
  - The “Essential Norm and Division of Work Principle for Internet Content Management” 37(hereinafter called the “Principle”) versus the current status:

    In the NCC’s reply, it pointed out that according to the “Principle”, the way for managing the internet content is the same as that for managing the social entity. They are both based on the competent authorities’ duties and responsibilities prescribed in the laws and regulations.

    According to the survey results of this project, the “Principle” was co-stipulated by various units assembled by the NCC. The resolution of the “Principle” was adopted at the 23rd committee meeting of the National Information & Communication Security Taskforce (NICST) of the Executive Yuan on November 22, 2012. As of now, the Principle has been amended twice. The recent revised version was passed at the NICST’s 14th internet content security group meeting on October 6, 2014. The introduction to the Principle (the same as the NCC’s reply to us) points out that “In Taiwan, the way for managing Internet content is the same as that for managing the social entity. They are both based on the competent authorities’ duties and responsibilities prescribed in the laws and regulations”.

    What we need to pay special attention to is Part II of the “Principle”, “the division of responsibilities for internet content management”. This part lists all the internet contents that cause concerns and also list all the corresponding responsible competent authorities. The “Principle” points out that the list just provides some examples and has yet covered all duties and responsibilities of all competent authorities. Despite that, the “Principle” lists over 16 central organizations and the responsibilities. Compared to the list of over 16 organizations, only 6 government organization responded to us. For such a difference, the project team assumes that it could be due to one of the following reasons:

    a. The authorities don’t have legal authority to remove content.

      The “Principle” was drawn up to specify the division of responsibilities for government units to manage internet content. It just preliminarily specifies each organization’s responsibilities and not necessarily means that all related organizations have the legal authority.

37. For brevity, so hereinafter referred to as the “Principles”. 
b. The authorities don’t know what their responsibilities are.

If all the competent authorities listed on the “Principle” have the legal authority and only six of them responded to this project, it means these authorities are not clear about their own responsibilities.

In conclusion, no matter the reason is a or b, our government’s internet content management still requires further improvements. Since 2012, the “Principle” has been stipulated for nearly three years. All relevant units have more or less participated in the initial stipulation and the two amendments. Nevertheless, given such time and process, the aforementioned situation still happened. This implies that most of our government’s internet content management is still in a chaotic situation, lacking responsible authorities, lacking solutions, and even worse, lacking specific operating procedures.

We hope our government can draw up a specific management mechanism as soon as possible to clarify the duties and responsibilities so that users and enterprises could comply with.

« Regarding iWIN

• History, funding, duty and responsibility

The MOHW indicated in its reply to us that the establishment of the Institute of Watch Internet Network (iWIN) is to receive the public’s complaints on questionable internet content pursuant to Articles 46 and 49 of the “Protection of Children and Youths Welfare and Rights Act”.

Based on Article 46 of the said Act, iWIN was founded after the NCC called each competent authority to encourage private groups to establish content protection mechanisms. Since 2015, the government has adopted the open tender method to select a private group to take charge of the iWIN operations. The winning bidder will be awarded a 2-year contract. At present, there are 21 members to run the iWIN’s operations, including 11 employees and 10 volunteer workers. According to the iWIN’s contract award notice published at the Government e-Procurement System, the 2-year budget for iWIN is around 27 million, which is be jointly covered by eight government units. The eight units are Ministry of Education, Ministry of Culture, Ministry of Health and Welfare, Food and Drug Administration, National Police Agency, Department of Commerce, Department of Industrial Technology, and the NCC.

According to the NCC, the iWIN’s outsourcing operations include administrative and technical operations, such as monitoring internet activities, implementing the mechanism for online complaints, education and propaganda, but not relate to the exercise of public power. The iWIN’s duty and responsibility is to “forward” the public’s opinions to the competent authorities or platform providers for them to handle. Such “forward” requires no regulatory power. The real regulatory power is actually held by the competent authorities.

• Connection with the “Principle”

In response to our enquiry, the NCC told us that iWIN forwards complaints to relevant authorities based on the “Principle”.

• Past performance

Based on the periodic reports posted on the iWIN’s website from 2010 to date, the project team consolidated the statistics of the complaints received by iWIN every year as below:

38. For the meeting minutes, please see https://www.dropbox.com/s/sjde2lh0xxffkd5/%E9%99%84%E4%B-B%B61_%E6%9C%83%E8%AD%B0%E7%B4%80%E9%8C%84.pdf?dl=0. For the meeting sign-in sheet, please see https://www.dropbox.com/s/6idindzt2ifyhn6/%E9%99%84%E4%B-B%B62_%E7%B0%BD%E5%88%B0%E8%A1%A8.pdf?dl=0

39. Please refer to the following link for the open tender information in 2015 and 2016: http://web.pcc.gov.tw/tps/tpam/-main/tps/tpam_tender_detail.do?searchMode=common&scope=F&primaryKey=51421091

40. Please refer to P115 of Issue 4, Vol. 104 of the Legislative Yuan Gazette

41. Please refer to the following link for iWIN’s complaint statistics as of 2Q 2015: http://www.win.org.tw/iwin/study/paper.html
• Problem 1: Some organizations are unclear about iWIN’s duty and responsibility or iWIN has never introduced its own duty and responsibility.

The Taichung City Police Department suggested in its response to us that the project team may directly contact iWIN to ask for the statistics regarding requests for content removals. It seems that some of our government’s police and prosecutors’ units are not very clear about iWIN’s limited power. They might think that the complaints forwarded by iWIN are no longer in need of any review and handling. Accordingly, the wrong interpretation might affect the public’s right to freedom of expression.

• Problem 2: iWIN has ambiguous definitions for the statistics items.

iWIN releases the complaint statistics every month and every quarter. There are three major categories of the complaint statistics: 1) child and youth-related complaints versus non-child and youth complaints; 2) complaints sent from local IP addresses versus complaints sent from foreign IP addresses, and 3) case status. With respect to the “case status” based on the latest statistics (released in July, 2015), the status includes: closed cases that have been processed, closed cases that have been found no violations, closed cases that have been forwarded to foreign services providers or put on the blacklist of telecom companies, closed cases that have been transferred to responsible units, cases without valid links, cases pending, total number of cases that have been processed, closed cases with content taken down/removed.

The above chart shows that the complaints received by iWIN have increased over the years, from the founding of iWIN’s predecessor, “e-Window of Watch Internet Network”, in August 2010; the establishment of iWIN in August 2013; to present. Particularly in 2014, iWIN received 15,051 complaints, which is a record high in years. Among these complaints, there were at least 1,990 complaints not related to children and youths, accounting for around 13.2%. In view that more and more people and government organizations have gradually attached importance to the iWIN’ work, it would be necessary for iWIN to disclose or clarify its complaint processing procedures, review standards, and related duties and responsibilities. In our survey, we also found some of the following problems about iWIN’s operations.

42. iWIN has been constantly changing the complaint items. For example, before July 2014, iWIN did not divide children and youths-related cases and non-children and youths related cases. Also, before July, 2015, iWIN never listed items that were removed after being complained. However, in its statistics after July 2015, iWIN added the list of items that were taken down in the statistics. Due to the constantly changing case classification, we found that even the items listed in the monthly reports may share the same names, they may not have the same content any more. Therefore, the 2014 statistics mentioned here is just the total number of complaints added with the figures of children and youths-related cases after July 2014.

43. In 2015, iWIN added a new contact to process internet bully complaints. Just like non-child and youth complaints, the bully complaints were not previously planned to be included in iWIN’s operations when it was founded. (Even though some internet bully cases may be child and youth-related, yet most of them may not).

44. Please see Zhong-Shi-Jing-Xing-Zi letter No. 1040022399 dated April 7, 2015
iWIN has never explained the definitions of these items in its issued reports. Therefore, people may find it difficult to directly comprehend the real meaning of these items when reading the reports. For example, the item titled “closed cases with no violations” seems to imply that iWIN has already reviewed the cases to discern if there are any violations. However, we learned that it actually means something else after we asked the NCC to explain it. According to the NCC, the item actually means the followings: 1) the websites of the content in question have taken specific measures to protect children and youths; 2) the reasons and targets of complaints were irrelevant; and 3) there were no specific competent authorities. In addition to the aforesaid item, there are also other items that have very ambiguous definitions. For instance, iWIN has no explanations about closed cases that have been processed and closed cases with content taken down/removed on its website. Even though the NCC has explained the definition for the item “closed cases with no violations”, the project team still thinks that either iWIN or NCC should provide clearer explanations on other items for other government units and the private sector to know.

- **Problem 3: It is unclear if the takedowns/removals correlate to the complaints.**

Since this June, iWIN has included the total number of takedowns/removals in its monthly complaint statistics to let people know more about the processing results of their complaints. Later, iWIN added an item of “removals versus closed cases that have been processed” in its July statistics report. However, there is a possibility that an item was removed due to the website’s initiative choice before the notice was even received. Hence, it would be difficult for the public to discern if there is a direct link between the removals of items and iWIN’s processing of complaints.

- **Problem 4: iWIN’s standards for case classification are unclear.**

Lastly, iWIN’s standards or procedures to classify the types of cases for corresponding authorities remain unclear. iWIN is not entrusted to exercise the public power. However, it is in charge of the case classification, which relate to whether the cases can be properly and timely processed. As a result, iWIN or iWIN’s competent authority should specify and disclose specific classification standards so that the public may know if their complaints are fairly processed.

45. According to the NCC’s explanation, if a case is processed and closed, it means that there is no responsible unit to handle the case so iWIN only forwarded the case to the ISP. However, there is no direct link because it is possible that an ISP removed the item before it received iWIN’s notice.
Future directions

Although we have applied quite a number of evaluation indicators in the first year for the TTTR project, there are still many aspects that we need to attend to and look further into in the future.

- **To include the blocking mechanism into the survey**
  
  Aside from requesting certain content to be taken down, another key method that governments adopt for managing online expressions is through “blocking.” The so-called “blocking” is to make certain web links inaccessible to users. As a result, their content cannot be viewed by users. According to South Korea’s transparency report, “blocking” has been viewed as a priority task.
  
  Over the past few years, Taiwan also attempted to block certain websites or web content through legislation several times. For instance, in May 2013, our Intellectual Property Office tried to amend laws to block foreign rogue websites. In June 2013, the NCC tried to amend Article 9 of the Telecommunications Act to control internet content. These attempts show the necessity to incorporate “blocking” in our survey.

- **To analyze the usage for data requests**
  
  The scope of data requests in our current survey only focuses on the times and reasons of requests. In the future, we plan to further look into the connection between data requests and their purposes. For example, we plan to analyze if there is a gap between the number of the government’s data requests and the number of pieces of data that were actually used. Meanwhile, we also intend to analyze the reasons for causing such a gap. We believe the analysis would help the public see whether the government has had a careful evaluation before it request for personal data.

- **To notify the parties concerns about the number of requests and types of cases**
  
  The timing and types of cases specified in the notices to the parties concerned from the government units highly correlate with the chance of the parties concerned to get remedies. The project team plans to include this part in the future research to look into the timing of the notices as well as the types of cases.

- **To divide metadata and content data**
  
  In our current survey, the metadata on the government’s requests to review the users’ data (e.g. the email sending time, email receiver(s), and email sending device(s), etc.) and content data (e.g. email text) are not divided. Previously, the metadata was not generally viewed as personal data because it does not involve in the content of actual activities even though it has been widely used. Nevertheless, from the surveillance programs disclosed by Edward Snowden, we learn that a government could effectively monitor its people if it can widely use the metadata.

  Meanwhile, based on the transparent reports released by some enterprises, the content data seems to have higher protection compared to the metadata. In other words, it would less difficult for government units to acquire metadata from enterprises rather than content data. Therefore, for our future surveys, we will try to divide the metadata and content data to let people know how the government uses their personal data.
To disclose data sharing among government units

Government units may try to share data among one another to reduce costs for personal data collection. Therefore, a government unit with no data may obtain the data it requires from another government unit through data sharing. Since people have the right to know how their personal data is collected, processed, and used by government units, they may also need the government to disclose the data sharing activities to safeguard the rights prescribed in the Personal Information Protection Act.

To disclose data storage

Article 11 of our "Personal Information Protection Act" prescribes that "The information collected should be deleted, discontinued to process or use, ex officio or upon the request of the Party when the specific purpose no longer exists or time period expires." In other words, people have the rights to know which data of theirs is kept by the government and also the rights to know if the purpose and time period of data storage are in compliance with the Act. Accordingly, the abuse of personal data could be prevented if the TITR project can disclose any situations where the government keeps the data without legitimate purpose or time period.

Suppliers’ data

The government data sources are mostly from the internet service providers (ISPs). As the result, we think if we could obtain the list of the ISPs from the government and also the related statistics from the ISPs, we could monitor both the government and suppliers’ situations to let people know more about the ones that they trust.
Improvement suggestions for the government

* **To establish and disclose the request statistics compiling formats and figures**

The project team found in the survey that almost no government units (except Criminal Investigation Bureau) have ever disclosed their request statistics compiling formats. In addition, aside from the Judicial Yuan that releases annual statistical report, no other government units have ever regularly released such statistics. The government units started compiling and providing the data only after the TITR project team enquired them. We think the items that the government was willing to disclose and compile statistics for must be the ones that the government considers important to the people in terms of their content. That also means the government would be more cautious when taking any actions. Hence, the best way for a government to show the respect to its people's privacy is to establish statistics compiling formats and regularly disclose the statistics every six months or every year.

* **To specify and disclose legal bases, implementation mechanism, operating procedures, audit and remedy procedures for data and removal requests**

The ISPs, especially the local ones, would normally comply with the government's requests to provide data even though they might have some doubts about the (legal) documents issued by the government. It is because they need to take care of their business operations and the government powers. The project team reckons that the government should announce the legal bases, implementation mechanism, operation workflow, audit and operating procedures in advance for its requests. As such, it may effectively reduce the ISPs' legal risks, increase ISPs' willingness to cooperate with the government, better facilitate compliance of government administrative staff, and improve the efficiency and channels for the public to get remedies for their rights and interests.

* **To set up a unified contact for government units**

Each unit should designate a specific person as a contact with enterprises. A unified contact is expected to help reduce mistakes in government administrative procedures so as to strengthen the trust relations between enterprises and the government.

* **To establish an independent supervisory mechanism**

Based on our previously consolidated data, there were a total of 4,908 requests for internet personal data and 1,234 removals of online expressions in 2012-2014 (see P17 and 38 of this report). According to our current laws, most of these requests and removals required no court authorization. In addition, there were no supervisory mechanisms to review whether the government organizations' decisions were necessary or whether the ways of their implementation (e.g. the sensitivity level of the information they requested and the scope of the content removals and takedowns) were in accordance with proportionality.

An independent supervisory organization is expected to benefit the government's operations in this regard. For instance, the government should have different legal bases when requesting enterprises to provide personal data at different sensitivity levels. An independent organization would be able to verify whether the relevant mechanisms built by the government can protect personal information at different levels in terms of procedures.
• To clarify the duties and responsibilities of various units

With respect to the removals of online expressions, we found in the survey that some government units were not very aware of its own or others’ duties and responsibilities. For example, the Taichung City Government Police Department\(^{46}\) was confused about its own and iWIN’s authorities. Therefore, the project team suggested it is necessary to clarify the duties and responsibilities of all related units as soon as possible to be in accordance with the principle of administration by law.

• To notify the parties concerned of the statistics

The key to seeking remedies for the rights and interests is whether the parties concerned are aware of the government’s activities to collect information. Articles 7 and 8 of the “Personal Information Protection Act” specify the principles for information collection units to notify or not to notify the parties concerned. In other words, the parties concerned have the right to know which unit(s) collected their personal data. The project team thinks that the enterprises or government units should actively explain the aforementioned provisions prescribed in the Personal Information Protection Act and should also disclose related statistics of notifying or not notifying the parties concerned. Therefore, the parties concerned may be aware of whether their rights are infringed and have the possibility to seek remedies.

• To request enterprises to disclose related data

According to the statistics of Access Now, there are nearly 50 global enterprises that would periodically release transparency reports on governments’ requests for personal data and content removals. Additionally, Industry Canada also published the “Transparency Reporting Guidelines” in June this year. The Guidelines points out that Canadian law enforcement, national security agencies, and regulatory authorities rely on the collection of information from private enterprises or private sectors to enforce the law and protect public safety (e.g. criminal investigation, a regulatory audit or inspection, to find a lost or injured child, or to protect an individual from an imminent threat to their well-being). Therefore, people in Canada may also have the right to know how their personal data stored in the database of these private enterprises or private sector was transmitted, shared, and used. The project team believes that our government may enhance people’s trust in enterprises and also increase its own credibility if it could follow the Canadian government’s step and join hands with suppliers to make a list of statistics items to be open to the public.

\(^{46}\) Please see Zhong-Shi-Jing-Xing-Zi letter No. 1040022399 dated April 7, 2015.
## Vocabulary

<table>
<thead>
<tr>
<th>Vocabulary</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>internet personal data</td>
<td>The data is what a person provides, posts, transmits, stores, or generates when using the service of an internet service provider. The data content may contain: 1) ideographic symbols, characters, pictures, images, or other messages; 2) registration information, application information, transaction records, or other identifiable information; and 3) information recorded or generated by an ISP when its user uses its services.</td>
</tr>
<tr>
<td>online expressions</td>
<td>A person uses an internet service provider's services to provide, post, transmit, or store ideographic symbols, characters, pictures, images, or other messages.</td>
</tr>
<tr>
<td>metadata</td>
<td>There are several Chinese terms for this English word. Metadata is data that describes other data, which can be used to define or identify electronic resources. There are many forms of metadata on the internet. For example, the content of an email is not metadata but sender, receiver, time of sending and receiving, IP addresses of sender and receiver are metadata.</td>
</tr>
<tr>
<td>Access Now</td>
<td>Access is an international organization that has advocated internet human right and internet freedom for a long period of time. It was founded in 2009 when the Iranian Green Movement took place. Since its establishment, Access has participated in various countries' supports for internet human right and internet freedom and has also hosted large-scale international forums on internet governance. Moreover, it has made a lot of efforts on the transparent reports released by enterprises and governments. In addition, it has a web page, which posts consolidated and updated information in this regard. Access is by far a leading organization in the field of transparent reports studies.</td>
</tr>
<tr>
<td>IP</td>
<td>It is the abbreviation for “Internet Protocol”, which is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6).</td>
</tr>
<tr>
<td>ISP</td>
<td>It is the abbreviation for “Internet Service Provider”. An ISP is a company that provides you with access to the Internet. The most common ways to connect to an ISP are by using a phone line (dial-up) or broadband connection (cable or DSL).</td>
</tr>
</tbody>
</table>
台灣人權促進會
Taiwan Association for Human Rights

台灣網路透明報告

地址：104 台北市中山區天祥路 61 巷 22 號
電話：02-25969525
網站：http://transparency.tahr.org.tw
FB：https://www.facebook.com/tahrtransparency
Email：info@tahr.org.tw