ICDPPC DATA PROTECTION METRICS WORKING GROUP

Report to the 40th Conference on Data Protection Metrics
Review of 2017 ICDPPC Census Questionnaire

Introduction

In 2017 the Conference undertook its first ever census which was designed to give a detailed 'snapshot' of privacy and data protection authorities across the globe.

The ICDPPC Census was designed to contribute to the aims of the Resolution on developing new metrics of data protection regulation which include to:

- develop internationally comparable metrics in relation to data protection and privacy; and
- support the efforts of other international partners to make progress in this area.

The ICDPPC Data Protection Metrics Working Group has concluded that the 2017 Census was a success and should periodically be repeated. Future censuses would update the international 'snapshot' and reveal trends over time.

The Working Group reviewed the content of the 2017 ICDPPC Census questionnaire. The purpose of this review was threefold:

- To assure ourselves of the usefulness of each of the questions posed in 2017.
- To identify whether any questions could be omitted from a future census.
- To suggest textual changes where necessary.

As part of its review, the working group solicited input from the OECD Secretariat, which assisted in developing the 2017 Census questions, and members of the APPA Comparative Statistics Working Group. The working group acknowledges with gratitude that input.

Annexed to this report are:

- The text of the 2017 census marked up with the working group's recommendations.
- A resolution recording the working group's recommendation that the Conference periodically repeat the census.

Blair Stewart
Convenor, ICDPPC Data Protection Metrics Working Group

Report on Review of ICDPPC Census 2017

The Working Group considers that the 2017 census was successful and contributed substantially to the aims of the Conference Resolution on developing new metrics of data protection regulation.

The group notes the following positive outcomes from the inaugural census:

- Release of a 53 page high level report on the census (*Counting on Commissioners*).
- Online resources providing links to DPAs' annual reports, online presence and incomes as well as to national constitutional provisions.
- Publication of three infographics on jurisdiction, exemptions and digital presence.
- Release of raw data to 7 approved researchers which contributed to, amongst other things, a project examining Regulation of cross-border transfer of personal data in Asia and an APPA regional analysis.

The working group recommends that the census be repeated periodically. It suggests that running the census every 3 years would be appropriate with the next one to be undertaken in 2020 with the results available for the 42nd Conference.

Usefulness of each of the questions posed in 2017

The working group reviewed every question asked in the 2017 census and was satisfied that all were useful. (The full questionnaire used in 2017 is available at ICDPPC.org in English, French and Spanish.)

However, there were some questions that were useful to ask in 2017 but the working group considered need not be asked again in a future census. This included a question about the process for appointing the head of the authority and some of the questions touching upon case reports and voluntary breach notification. This aspect is discussed further in the next part of this report.

Questions that may be omitted from a future census

The 2017 census asked all respondents 41 basic questions. Depending upon the answers given, respondents might be asked approximately a further 10 supplementary questions.

The working group is satisfied that 41-51 questions is appropriate and is not an excessive number of questions to pose in a census survey of this type. Nonetheless the group has looked for opportunities to reduce the number of questions in order to leave greater scope for adding additional new questions when the survey is repeated without increasing the respondent burden.

The working group concluded that the following 6 basic questions and 6 supplementary questions may appropriately be omitted from a future census for the following reasons:

Questions to be omitted	Reasons for omission
Part A Authority profile	
1(d) The authority was established in which decade? (1970s or earlier; 1980s; 1990s; 2000s; 2010s).	This question was redundant as respondents were asked for the year of establishment of an allowing for easy calculations by decade.
4 How is the Head of the authority appointed? (Executive appointment; Legislative committee	The question has been asked in identical form in IAPP surveys in 2010 and 2011 and, in the view

appointment; Election; Civil servant/direct hire; Other)	of the group, is not worth asking again.
Part B: Data protection law, jurisdiction and exemptions	
6 Is your data protection or privacy law currently being revised? Yes/No	The survey had two questions on the same topic. This question can be dropped so long as the other question is retained ('has your data protection or privacy law been revised in the last 3 years?').
Part C: Authority's funding and resources	
6 Please describe the geographic distribution of your staff: (One office: All staff work at the same location; Two offices: Staff are split between two offices; More than two offices: Staff work at three or more offices)	Although interesting to ask once, the group did not consider this question to be of sufficient value to ask again in a future census.
Part D: Authority's enforcement powers, case handling and reporting	
5(c) Is a formal citation assigned to each case report?	Although useful to ask once as a measure relevant to the aims of the Resolution on Case Reporting, the group did not consider this question to be of sufficient value to ask again in a future census.
6(a) Does the authority keep any of the fine or penalty?	Although useful to ask once, the group did not consider this question to be of sufficient value to ask again in a future census.
8 Does the authority ever publicly name organisations that have breached the privacy or data protection law? Yes/No 8(a) If Yes, How many organisations were publicly named in 2016 as having breached the law?	Although useful to ask once, the group did not consider this basic question and the supplementary question to be of sufficient value to ask again in a future census.
Part E: Cross-border data flows, enforcement and cooperation	
4(a) If YES [in relation to secondment question]: (i The authority hosted a staff member or members from another authority on secondment; ii The authority sent a staff member or members to another authority on secondment; iii Both, sent and hosted)	The supplementary question can be dropped as answers did not add anything useful to the answers to the primary question (which was 'In 2016, has the authority participated in a secondment with another privacy enforcement authority?').
Part F: Breach notification	
1 Are there any voluntary breach notification guidelines issued by the authority in your jurisdiction? Yes/No 1(a) Do they recommend notification to: (i the data subject; ii the authority; iii both the data subject and the authority)	With mandatory breach notification now very common, it will simplify the census to omit questions relating to voluntary notification schemes.
3 Is the authority involved in enforcing regulations on security breach notifications?	The language used was selected to repeat a question used in an earlier IAPP survey and allows comparisons with that survey. However, the question essentially duplicates other questions and should therefore not be repeated.
Part G: Other matters	

1. Has the authority published guidance relating to data protection aspects of any of the following (select all that apply): [a. Profiling? / b. App development? / c. The internet of things? / d. Transparency reporting? / e. Artificial intelligence?]	This question was looking specifically at whether there were identifiable domestic guidance outcomes from the in-depth discussion topics hosted at the Conference from 2012-16. That purpose has been served and there is no need to pose the same question (although consideration could be given to a similar question modelled upon post-2016 topics).

Suggested textual changes

Generally speaking the working group recommends keeping the text of questions the same when the census is repeated as this will ensure the answers obtained will be directly comparable.

In some cases where the group identified drafting problems it has, for more general reasons, recommended that a question be dropped. In those cases we do not record suggestions for textual changes in this part of the report.

The group recommends the following small changes for the reasons given:

Questions to be changed	Reasons for change
Part A Authority profile	
1(c) Please indicate the region in which the authority is located …	Suggest that the North America entry read 'North America and Caribbean'.
2(a) As appropriate, please provide the details of the following social media …	Suggest that 'LinkedIn' be added to the prompted list.
Part B: Data protection law, jurisdiction and exemptions	
-	-
Part C: Authority's funding and resources	
3. Does the authority's funding coming from any of these sources (select all that apply): a. Government grants …	'Government grant' was thought to be confusing by some working group members. It might be better to refer to 'Government grant/appropriation/allocation.'
Part D: Authority's enforcement powers, case handling and reporting	
-	-
Part E: Cross-border data flows, enforcement and cooperation	
Does the authority perform an enforcement role under any of these supra-national arrangements (select all that apply): a. EU-US Privacy Shield b. Swiss-EU Privacy Shield c. EU Binding Corporate Rules d. APEC Cross-border Privacy Rules system (CBPRs)	APEC's Privacy Recognition for Processors (PRP) system was not fully operational at the time of the questions for the 2017 census were developed but could now usefully be listed.
Part F: Breach notification	
-	-
Part G: Other matters	
2. Does the authority have a formal process for engagement with civil society (e.g. regular	This is a useful topic to resurvey. However, the current question generates a lot of unstructured

scheduled meetings)? 2(a) If yes, please specify:	responses that are hard to count 'census style'. It is suggested that the supplementary question begin with a couple of prompted options before offering the unstructured 'other' option. It is suggested that the prompted options cover scheduled meetings, advisory committees and public consultation opportunities.
3. Did the Authority conduct a public opinion survey in 2016? 3(a) If yes, please specify.	Rather than asking whether a domestic survey was undertaken in the year preceding the census, as was the case in the 2017 census, the working group recommends that the question ask, in effect, whether a public opinion survey was undertaken in the years since the census question was last asked (i.e. in 2017 or since).

Additional questions

With the reduction of the number of questions to be repeated the working group thinks that there will be ample scope to identify additional useful questions. An example might be, for example, a question seeking to quantify the resources that DPAs devote to processing breach notifications. This might be useful as it is a relatively new function for most DPAs and there will be a paucity of existing data on the topic.

The group does not offer recommendations in this report as it is a matter that should be considered closer to the time that the next census is run.

Amended text

A version of the survey questions with the recommended omissions and changes follows:

Recommended changes to 2017 survey questions for use in future censuses
Part A
Please provide the following details regarding your data protection or privacy authority: a) Name of Authority
b) Country/economy
c) Please indicate the region in which the authority is located: a. Africa and Middle East b. Asia c. Europe d. Oceania e. North America and Caribbean f. South or Central America g. Other
~~d) The authority was established in which decade?~~ ~~a. 1970s or earlier~~ ~~b. 1980s~~ ~~c. 1990s~~ ~~d. 2000s~~ ~~e. 2010s~~
Year of establishment
Does the authority have an official digital presence online?
If yes, As appropriate, please provide the details for the following social media: i. Website URL or user name: … ii. Twitter account: @... iii. Facebook URL or username: … iv. YouTube channel URL … v. LinkedIn: … ~~v.~~vi Any other social media account address: …
Does the authority publish an annual report?
Is the annual report available online?
If Yes, please provide the URL address
~~How is the Head of the authority appointed?~~ ~~a. Executive appointment~~ ~~b. Legislative committee appointment~~ ~~c. Election~~ ~~d. Civil servant/direct hire~~ ~~e. Other~~

Part B: Data protection law, jurisdiction and exemptions
Does the authority oversee privacy protection practices by: a. Only the public sector? b. Only the private sector? c. Both public and private sectors?
In addition to a data protection or privacy law, does your country's constitution include a reference to data protection or privacy?
Please provide the specific reference to the constitution (URL is preferable)
In addition to roles under a data protection or privacy law, does the authority perform any functions under the following types of information, rights or accountability laws?

a. Government information access or Freedom of Information law b. Unsolicited electronic communications or spam law c. Human rights or anti-discrimination law d. public key infrastructure (PKI) or cryptography law e. Cyber-security law f. Data portability law g. Government ethics law h. Competition law i. Telecommunications regulation law j. Health information law
Does your data protection or privacy law contain: a. A partial exemption for State intelligence and security agencies? b. A complete exemption for State intelligence and security agencies?
Has your data protection or privacy law been revised in the last 3 years?
~~Is your data protection or privacy law currently being revised?~~

Part C: Authority's funding and resources
What was your total income for 2016 in your national currency? (no decimals, please do not put commas or dots to differentiate thousands)
How does the authority's total budget compare to the previous year? a. The budget increased b. The budget remained the same c. The budget decreased
If the authority's budget increased from the previous year, by what percentage did it increase? i. 1-5% ii. 6-10% iii. 11-20% iv. more than 20%
Does the authority's funding coming from any of these sources (select all that apply): a. Government grants/appropriations/allocations b. Registration or licensing fees c. Chargeable services (e.g. auditing, training, publications) d. Fines and penalties e. Other (please specify)
How many staff are employed by the authority (full time equivalent employees)?
How does the authority's total number of staff compare to the previous year? a. The number of staff has increased b. The number of staff has remained the same c. The number of staff has decreased
~~Please describe the geographic distribution of your staff:~~ ~~a. One office: All staff work at the same location~~ ~~b. Two offices: Staff are split between two offices~~ ~~c. More than two offices: Staff work at three or more offices~~

Part D: Authority's enforcement powers, case handling and reporting
What are the principal roles performed by the authority under the privacy or data protection law (indicate as many as apply): a. Mediation/ arbitration

b. Policy research c. Handle complaints d. Registry activities e. Auditing/ inspections f. Public outreach/ education g. Advocate for privacy rights/ legislation h. Compliance/ investigations/ enforcement i. Other (please name)
How many cases did the authority accept for investigation in 2016?
Does the authority: a. Have the power to make binding decisions in individual cases? b. Have the power to make recommendations in individual cases? c. Have the power to refer to another authority with decision-making powers?
Are the decisions or recommendations of the authority subject to appeal to another body (agency, court or tribunal)?
How many cases were taken on appeal in 2016?
Does the authority report publicly on cases it has handled?
If yes, How many case reports were released in the last year?
In the case reports are posted on the authority's website, please provide the URL
~~Is a formal citation assigned to each case report?~~
Are the case reports uploaded to a central repository (such as an online legal information institute)?
Does the authority impose fines or penalties for a breach of the data protection or privacy law?
~~Does the authority keep any of the fine or penalty?~~
Please provide the amount of the largest fine or penalty imposed by the authority (or an appeal authority, court or tribunal) for a breach in 2016 (amount to be provided in your national currency)
What was the largest amount of compensation awarded by the authority (or an appeal authority, court or tribunal) for harm caused by a breach of the privacy or data protection law in the last year (amount to be provided in your national currency)?
~~Does the authority ever publicly name organisations that have breached the privacy or data protection law?~~
~~How many organisations were publicly named in 2016 as having breached the law?~~

Part E: Cross-border data flows, enforcement and cooperation
Does the privacy or data protection law include express provision for any of the following : a. Transfer of complaints to privacy enforcement authorities in other jurisdictions? b. Disclosure to privacy enforcement authorities in other jurisdictions of information obtained in investigations? c. Assisting other privacy enforcement authorities in cross-border investigations? d. A prohibition on providing information to other enforcement authorities?
Does the jurisdiction have legal provisions (whether in the privacy or data protection law or otherwise) that: a. Restrict the cross-border transfer of personal information? If YES, does the authority have a role to enforce this law? b. Require data processing facilities to be located within the jurisdiction? If YES, does the authority have a role to enforce this law?
Does the data protection or privacy law establish a process for formally recognising other jurisdictions that that have laws establishing comparable data protection standards?
Does the authority perform any role in that recognition process?
In 2016, has the authority participated in a secondment with another privacy enforcement

authority?
~~If YES:~~ ~~i. The authority hosted a staff member or members from another authority on secondment~~ ~~ii. The authority sent a staff member or members to another authority on secondment~~ ~~iii. Both, sent and hosted~~
Which of these enforcement cooperation networks or arrangements does the authority participate in (select all that apply): a. Global Privacy Enforcement Network (GPEN) b. GPEN Alert c. APEC Cross-border Privacy Enforcement Arrangement (CPEA) d. ICDPPC Enforcement Cooperation Arrangement e. Unsolicited Communications Enforcement Network (UCENet)
Does the authority perform an enforcement role under any of these supra-national arrangements (select all that apply): a. EU-US Privacy Shield b. Swiss-EU Privacy Shield c. EU Binding Corporate Rules d. APEC Cross-border Privacy Rules system (CBPRs) e. APEC Privacy Recognition for Processors (PRP)
Does the authority have any bilateral arrangements with the privacy enforcement authorities of other countries to co-operate in the enforcement of privacy laws?
In 2016, has your office been involved with the following coordinated efforts, involving authorities from many countries, to raise awareness of privacy and data protection: a. Data Protection Day b. Asia Pacific Privacy Awareness Week c. GPEN Sweep
In 2016, has the authority (select all that apply): a. Undertaken a joint investigation with any other enforcement authority or regulator within the same country? b. Undertaken a joint investigation with a privacy enforcement authority from another country? c. Provided assistance to an investigation being undertaken by a privacy enforcement authority from another country? d. Transferred a complaint to a privacy enforcement authority in another country? e. Received the transfer of a complaint from a privacy enforcement authority in another country?

Part F: Breach notification
~~Are there any voluntary breach notification guidelines issued by the authority in your jurisdiction?~~
~~Do they recommend notification to:~~ ~~i. the data subject~~ ~~ii. the authority~~ ~~iii. both the data subject and the authority~~
Are there any mandatory breach notification requirements in your jurisdiction?
Do the mandatory breach notification requirements apply generally or to particular sectors? i. Generally ii. all public sector iii. all private sector iv. telecommunications sector

v. health sector vi. other sector (please describe):
Do mandatory breach notification requirements recommend notification to: i. the data subject ii. the authority iii. both the data subject and the authority?
Do the requirements provide any explicit direction on notification to individuals living in other jurisdictions?
If Yes, please briefly describe
~~Is the authority involved in enforcing regulations on security breach notifications?~~
How many breach notifications (under voluntary or mandatory arrangements) did the authority receive in 2016?
Does the authority publish any information on the breach notifications it receives, for example total number of notifications received, sectoral breakdown, details of those that result in formal action?
If yes, where is this information published? Select as appropriate and/or provide other examples a. authority's annual report b. authority's website c. other

Part G: Other matters
~~Has the authority published guidance relating to data protection aspects of any of the following (select all that apply):~~ ~~a. Profiling?~~ ~~b. App development?~~ ~~c. The internet of things?~~ ~~d. Transparency reporting~~ ~~e. Artificial intelligence~~
Does the authority have a formal process for engagement with civil society (e.g. regular scheduled meetings)?
If yes, please ~~specify~~ <u>indicate any that apply</u>: a. <u>Regular scheduled meetings with representatives of civil society organisations</u> b. <u>Use of advisory committees draw from civil society</u> c. <u>Open public consultation opportunities when setting rules.</u> d. <u>other (please specify)</u>
Did the authority conduct a public opinion survey in ~~2016~~ <u>the last 3 years</u>?
Please provide URL:

Proposed resolution

The working group proposes that a resolution be adopted reflecting the recommendations of this report. It is proposed to proceed in this formal way because another census would not be held for more than a year and accordingly it is desirable to record the intentions in writing ready for later action.

The resolution has three objectives:

- To formalise a Conference intention to periodically repeat the census.
- To reference the working group's report as a resource for those working on the next census.
- To assign responsibility for getting the task done.

Resolution on the Conference Census

The 40th International Conference of Data Protection and Privacy Commissioners:

Noting that:

a) The 38th Conference adopted the Resolution on developing New Metrics of Data Protection which, amongst other things:
   - Recorded the Conference's intention to play a part in helping to build internationally comparable metrics in relation to data protection and privacy:
   - Directed the Executive Committee to identify ways in which the Conference can encourage the development of internationally comparable metrics:
   - Authorised the Executive Committee to convene working groups to assist with the task if necessary:

b) To give effect to the resolution the 6th Executive Committee:
   - Arranged for the ICDPPC Secretariat to arrange and deliver the inaugural ICDPPC Census 2017:
   - Established the ICDPPC Data Protection Metrics Working Group:

c) At the 39th Conference the ICDPPC Secretariat presented a report on high level results of the inaugural ICDPPC Census:

d) Following a review of the inaugural census, the ICDPPC Data Protection Metrics Working Group:
   - Concluded that the census made a substantial contribution to achieving the objectives of the Resolution on developing New Metrics of Data Protection:
   - Recommended that the Conference should periodically repeat the census with the next census in 2020:
   - That many of the census questions used in 2017 would usefully be repeated in future but that some identified questions could be omitted to facilitate inclusion of additional new questions:

Therefore resolves to:

1. Record its intention to periodically repeat an ICDPPC Census every three years.

2. Direct the Executive Committee to arrange for the next census to be held in 2020.