Registration Directory Service (RDS-WHOIS2) Review

Draft Report including F2F#3 agreements and action items

OBJECTIVE 3 SUBGROUP REPORT - SECTION 5 ONLY
FOR CATHRIN TO PROVIDE REDLINED UPDATES

RDS-WHOIS2 Review Team
30 July 2018

5 Objective 3: Law Enforcement Needs

[SUBSECTION NUMBERS WILL BE ADJUSTED WHEN ADDED BACK TO MASTER DOC]

1.1 Topic

Subgroup 3 - Law Enforcement Needs is tasked with investigating, analyzing, and drafting recommendations (if needed) to address the following Review objective:

> *Consistent with ICANN's mission and Bylaws, Section 4.6(e)(ii), the review team will assess the extent to which the implementation of today's WHOIS (the current gTLD RDS) meets legitimate needs of law enforcement for swiftly accessible, accurate and complete data by (a) establishing a working definition of "law enforcement" used in this review, (b) identifying an approach used to determine the extent to which these law enforcement needs are met by today's WHOIS policies and procedures, (c) identifying high-priority gaps (if any) in meeting those needs, and (d) recommending specific measureable steps (if any) the team believes are important to fill gaps. Note that determining which law enforcement requests are in fact valid will not be addressed by this review.*

To accomplish this objective, the subgroup agreed to take into account current and emerging technology and to include:

1. Cybercrime investigations and enforcement;
2. Data protection laws and enforcement;
3. What's required of the Registrar to retain data under the RAA;
4. A clear direction from Law Enforcement of what is needed; and
5. A better understanding of procedures and requirements by both Law Enforcement and the Registrars.

1.2 Summary of Relevant Research

To conducts its research, all members of this subgroup reviewed the following inventoried WHOIS policy and procedure materials, posted on the subgroup's wiki page:

- WHOIS Review Team (WHOIS1) Final Report (2012), Chapter 6 and Appendix E: The WHOIS Review team's Law Enforcement Survey
- WHOIS Misuse Study Final Report, especially Section 4. Law Enforcement & Researchers survey
- ICANN61 GAC PSWG - OCTO Update
- Additional links specific to Subgroup 3 may be added here, once identified by this subgroup

To conduct its research, the subgroup agreed to:

- Establish a working definition of "law enforcement" to be used in this review
- Conduct a first informal outreach to law enforcement contacts to solicit input on needs, including for example GAC PSWG, APWG, and SSAC members
- Review prior RT Law Enforcement Survey
- Review the update given by the ICANN Office of CTO to the GAC PSWG

The subgroup reviewed the definition of law enforcement used by the previous WHOIS Review Team, which was the following:

Law enforcement is "any entity charged or otherwise mandated by governments with enforcing or ensuring observance of or obedience to the law; an organized body of people officially maintained or employed to keep order, prevent or detect crime and enforce the law."[1]

The previous WHOIS Review Team added the following considerations:

The adopted definition intentionally does not include private individuals and organizations, such as anti-spam groups or those bringing civil enforcement actions, whose efforts may be viewed as within a larger concept of law enforcement. By adopting the narrower definition, the Team does not intend to discount the value of private sector efforts to curb abusive uses of the DNS. [2]

The definition was maintained for the purposes of the present review.

The subgroup conducted a survey of law enforcement agencies worldwide, which is also posted on the team's Wiki page:

- to find out more about their use of the WHOIS,
- to determine whether WHOIS met their investigative needs, and
- to provide a first assessment of the impact of changes made to the WHOIS by the Temporary Specifications adopted by the ICANN Board on 17 May 2018.

The survey was first run between 16 and 25 July 2018 and extended once, until 6 August 2018, to allow for greater geographical diversity after review of the first round of results.

1.3 Analysis and Findings

1.3.1 Law enforcement survey

The survey received 55 responses, many of which were made on behalf of countries. For example, for the European Union Member States, a request was made earlier in the year to nominate one national expert on WHOIS for law enforcement who was asked to respond to the survey.

Responses to the survey were received from Australia, Austria, Bahrain, Belgium, Brazil, Chile, China, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, India, Iran, Ireland, Italy, Japan, Kenya, Korea (South), Kuwait, Latvia, Mexico, Morocco, Nigeria, Philippines, Singapore, Slovakia, Slovenia, Sweden, Taiwan, Trinidad and Tobago, United Kingdom, United States of America and Zambia.

At its face-to-face meeting in Brussels, the Review Team found that, in general, there was a lack of reliable data to support in-depth analysis on a number of issues, in particular when it came to the uses of the WHOIS. The Review Team therefore discussed whether it would be useful 1) to conduct surveys such as the law enforcement survey periodically, e.g. every year or every two years, and 2) to extend such surveys to other users such as cybersecurity professionals. The Review Team also came to the conclusion that there was an underrepresentation of certain geographic regions in the survey, with a large proportion of responses coming from Western Europe, some parts of East Asia and North America. While specific efforts were made to reach out to underrepresented regions, these are still not fully

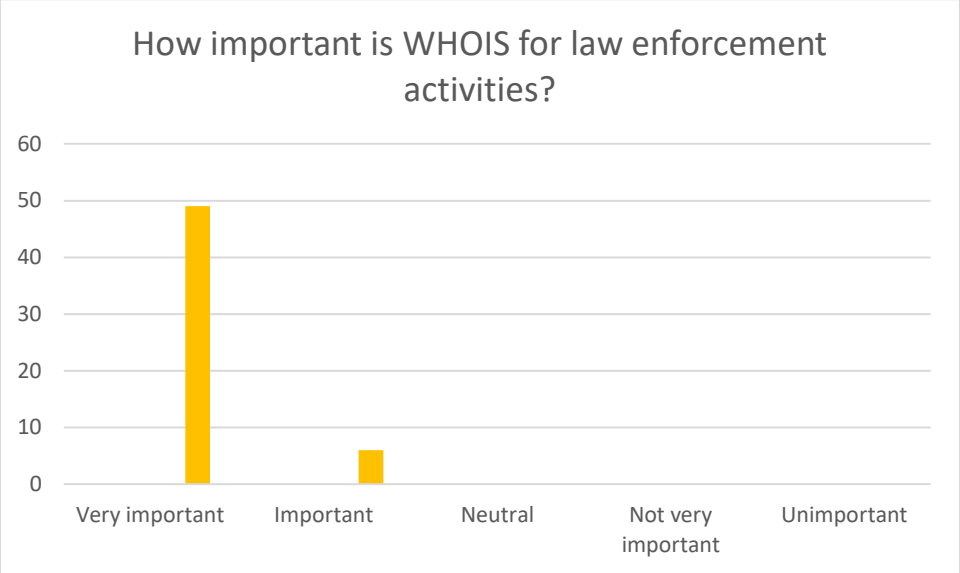
[1] WHOIS Policy Review Team, Final Report, 11 May 2012, p. 23.
[2] WHOIS Policy Review Team, Final Report, 11 May 2012, p. 23.

represented. This matches ICANN experience in other areas but efforts should nonetheless be made to ensure greater geographic representativeness in further iterations of this survey.

In the following sections, the survey results are outlined, broken down by category.

1.3.1.1 Importance of WHOIS data for law enforcement investigations

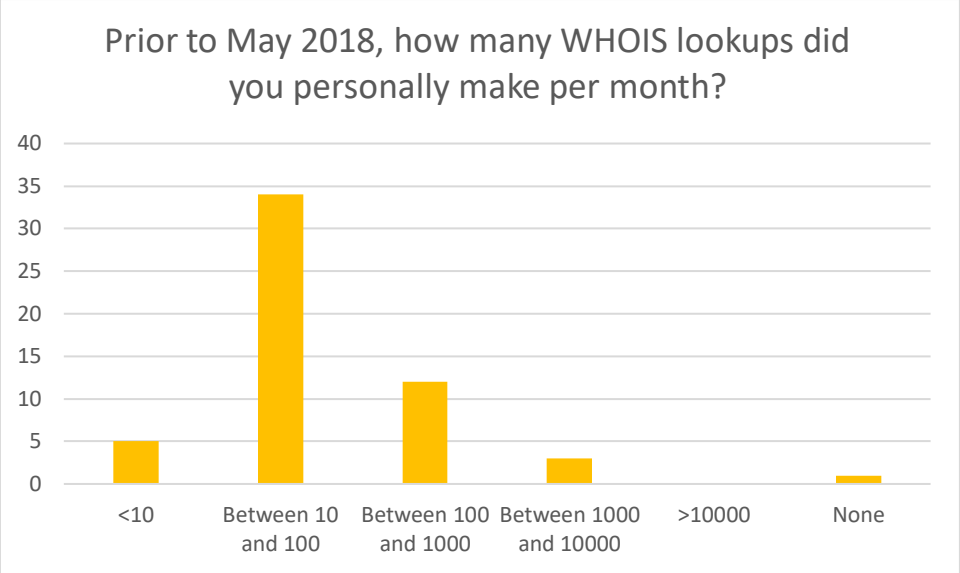
The survey requested feedback from law enforcement on the importance of WHOIS for law enforcement activities. 89% of respondents deemed WHOIS as "very important", while 11% deemed it as "important" for their activities. No respondents chose "neutral", "not very important" or "unimportant":



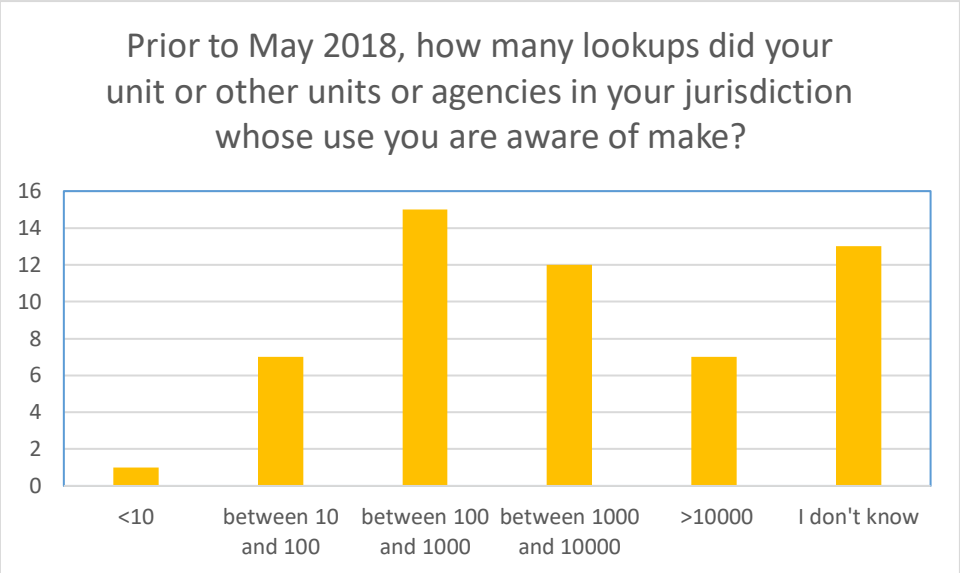
This confirms the results of the 2012 survey, where a number of respondents deemed WHOIS data as being of "great importance" or "very important". It is important to note that the survey assumes a certain familiarity with the use of WHOIS for investigations and may therefore not be representative of all law enforcement activities but rather only for those activities for which access to the WHOIS would be of relevance.

1.3.1.2 Frequency of use

Respondents were also asked how frequently they made use of the WHOIS. The largest proportion - 62% of respondents - make between 10 and 100 lookups per month themselves, 22% make between 100 and 1000 lookups, and 5% make more than 1000 lookups per month. 9% of respondents make less than 10 lookups per month, and 2% make no lookups.



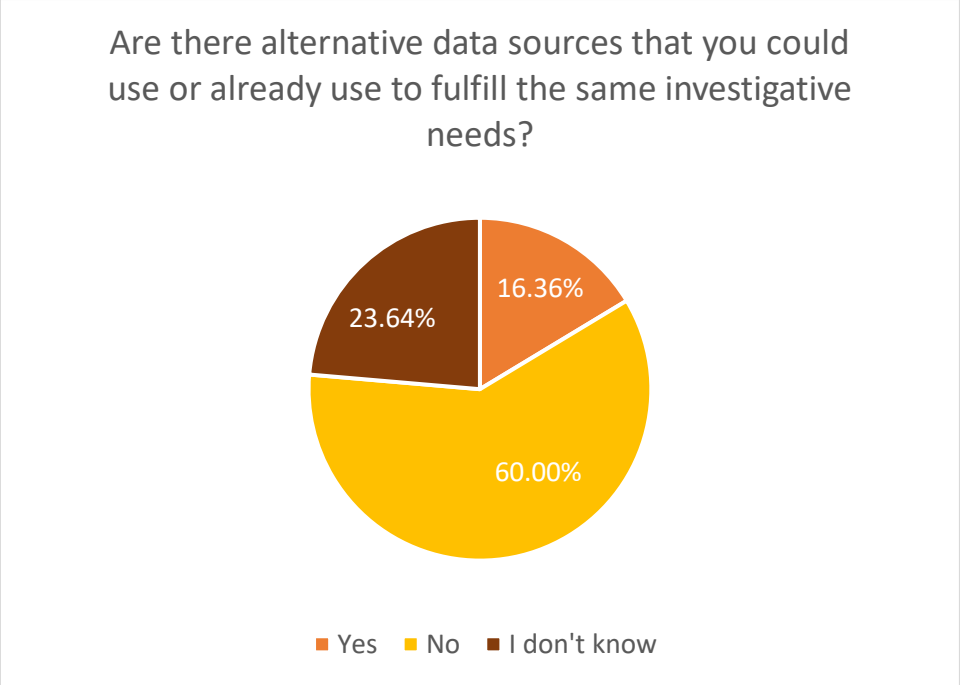
As a significant number of respondents were responding on behalf of larger entities such as their units or agencies, the survey also asked them to estimate the number of lookups these entities made:



As is to be expected, the number of lookups for entire units or agencies is significantly higher, with the highest percentage (27%) of units making between 100 and 1000 lookups per month, 22% between 1000 and 10000 lookups, and still 13% making more than 10000 lookups per month.

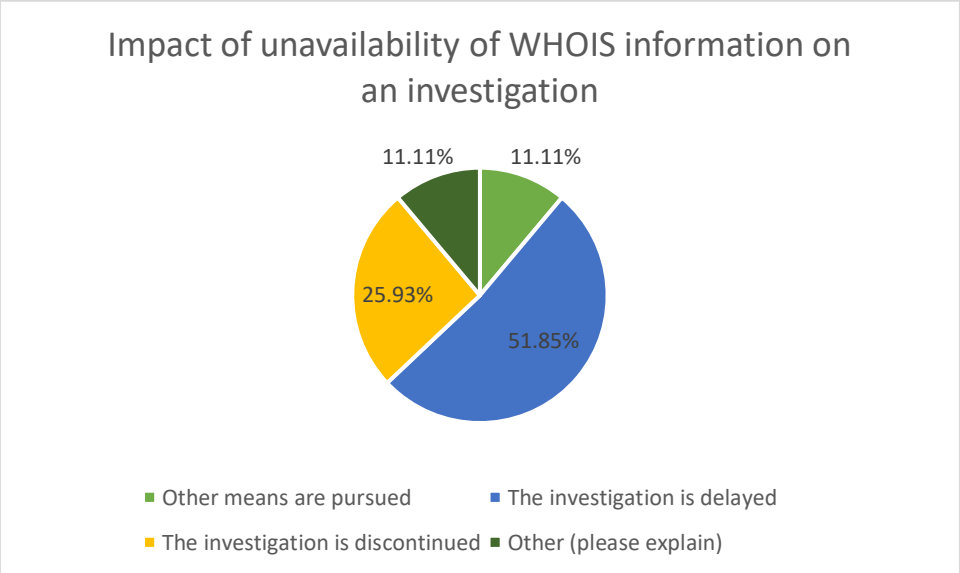
1.3.1.3 Alternative options to WHOIS lookup

Assuming that a WHOIS lookup is not available, the Review Team asked respondents to identify possible alternatives that they already use or could use. A significant number of respondents - 16% - stated that they had other tools available:



However, when respondents who said that they had alternative options were asked to identify the tools that could be used instead, a majority of them identified tools that also rely on WHOIS lookup, both open-source and freely available and those provided by companies.

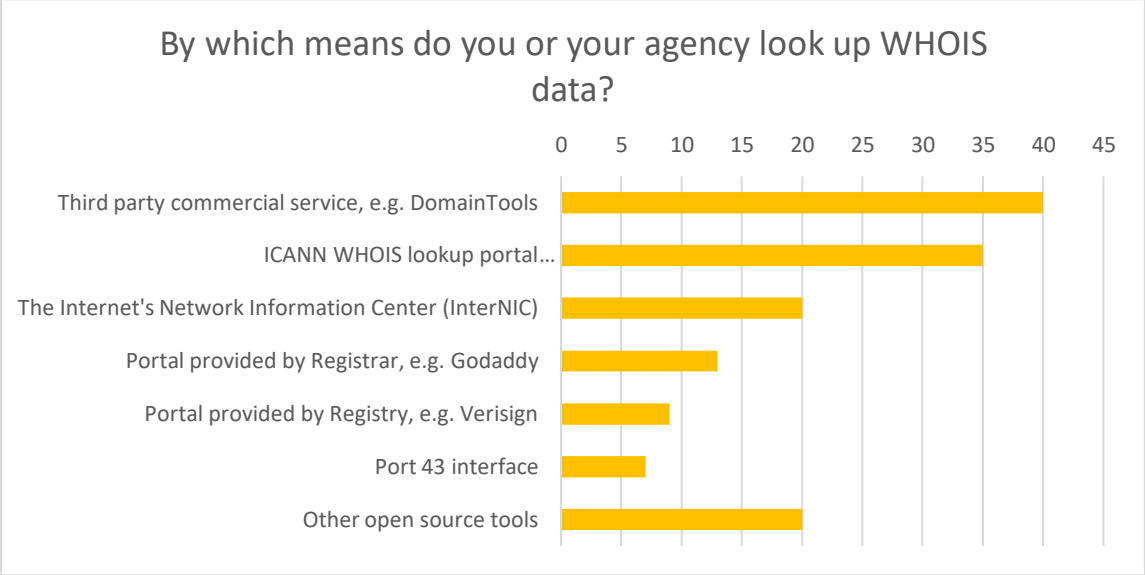
Respondents were also asked how it usually affects an investigation if WHOIS information is not available on a public query basis. According to 79% of respondents, the investigation is delayed or discontinued altogether:



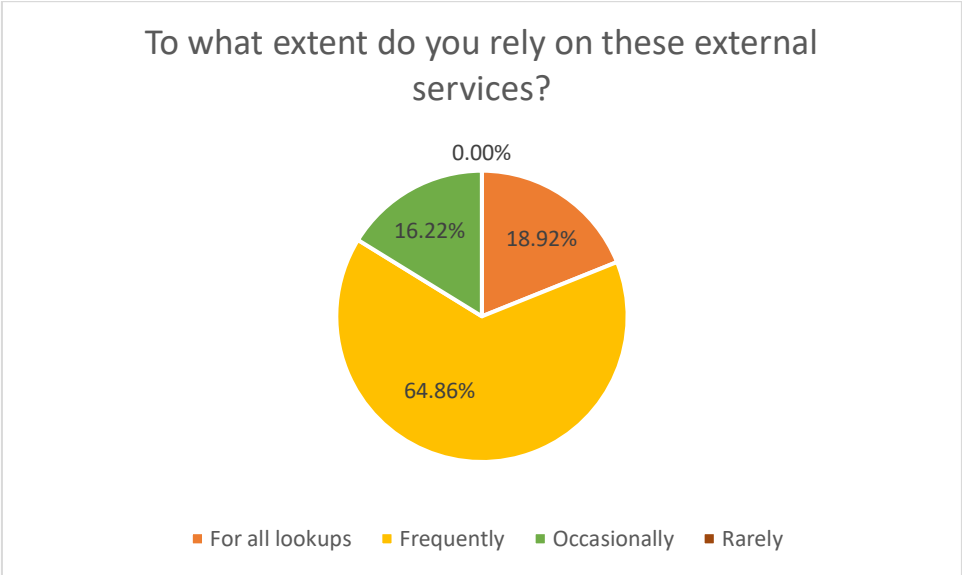
1.3.1.4 Tools used to access WHOIS data

The survey also sought information on the tools which law enforcement use to access WHOIS data. Respondents could name more than one tool. The responses show that the WHOIS lookup portal provided by ICANN following a recommendation by the first WHOIS

Review Team has become a popular tool, coming in second only to third party commercial services:

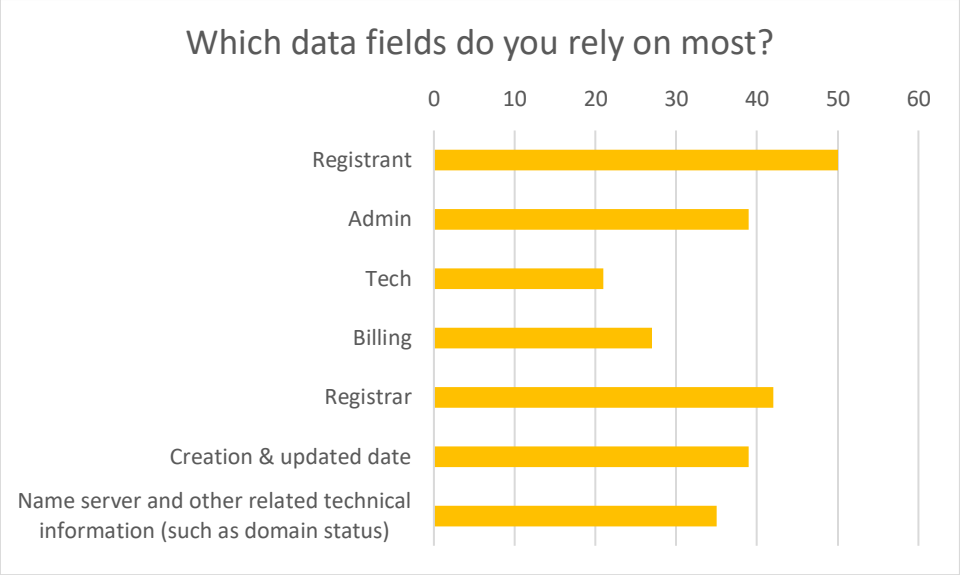


It is important to note that 73% of respondents currently use third-party commercial tools, which may be negatively affected by recent changes to the WHOIS protocol. Respondents were also asked specifically whether they rely on third-party services provided by private parties, such as DomainTools or others; 67% stated that they did, 22% did not, and 11% were not sure. Those who responded in the affirmative were then asked how frequently they made use of the tool:



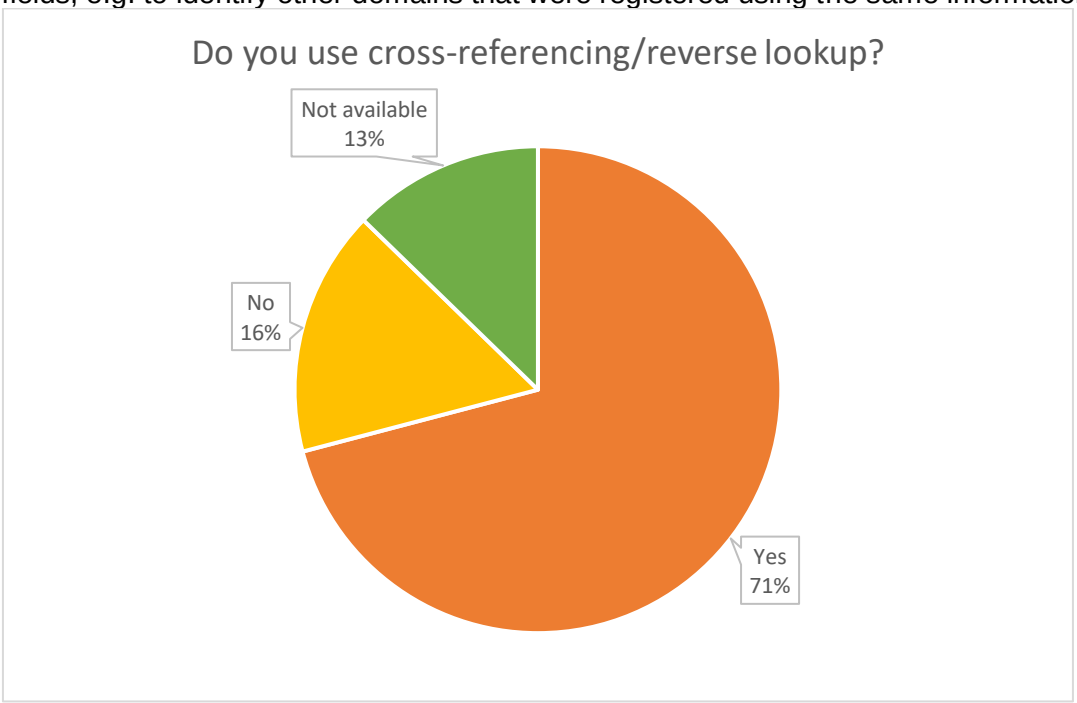
1.3.1.5 WHOIS lookup use

Respondents also answered a series of questions about the way in which they use the WHOIS lookup, starting with a question about which data fields they rely on most or which are most useful to their investigations:

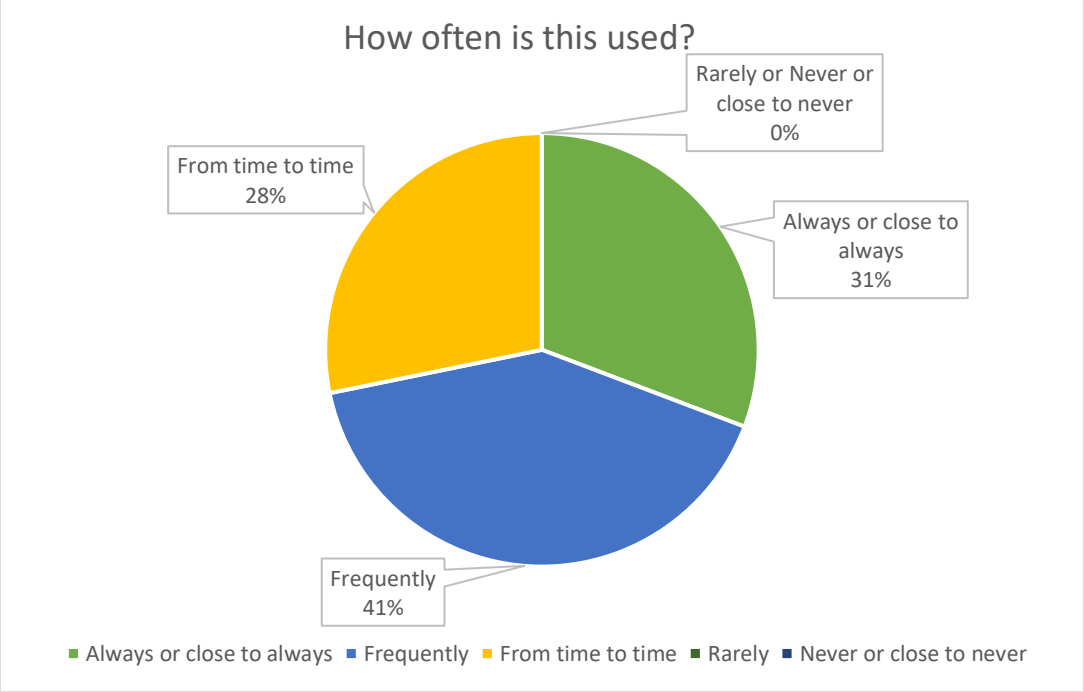


The most important set of fields is that relating to the registrant contact information. However, the gap to admin, tech and billing contact information is not very large. Responses show that the registrar fields are the second most important source of information in a WHOIS lookup for law enforcement; this can provide information both on where to go for further leads. The data also shows that there are no data field groups that are clearly unimportant to law enforcement; it could be useful to dive into this in more detail into a follow-up survey to determine whether there are individual data fields in these groups that are more or less useful to investigations. These results match the feedback received during ICANN's data mapping exercise in summer 2017, where law enforcement also provided input to show that any field can prove to be of use for investigations, depending on the leads that it can provide in an individual case.

Respondents were also asked whether they use cross-referencing/reverse lookup of WHOIS data fields, e.g. to identify other domains that were registered using the same information:



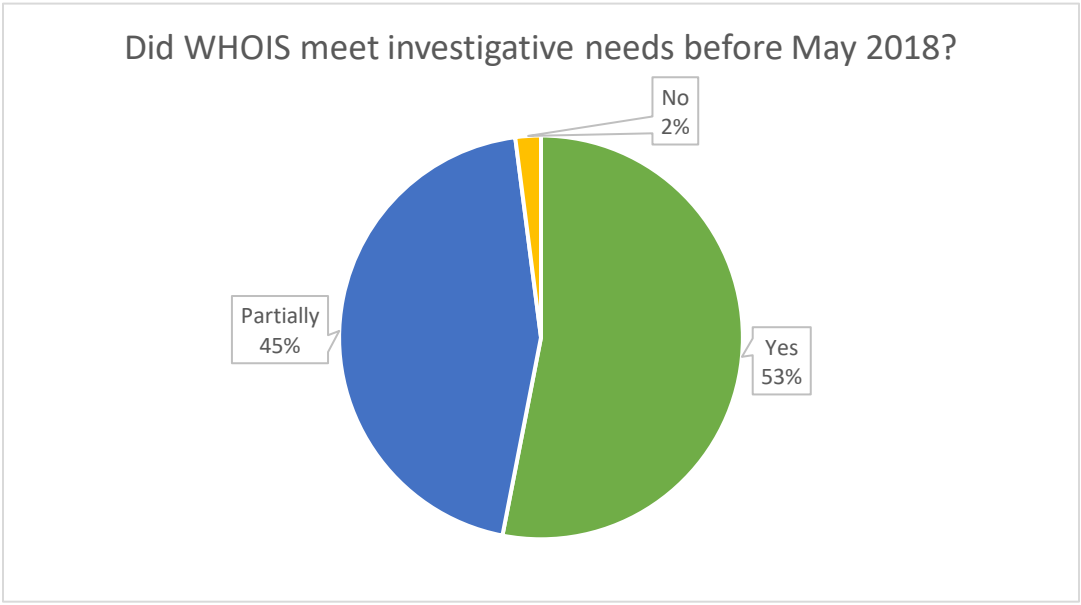
While the majority of respondents use cross-referencing, more than a quarter of respondents were of the opinion that it was not available to them or did not use it. Of those who did make use of it, a follow-up question asked them to identify how often they used it:



Respondents commented that this allowed them to identify other domains registered by the same registrant and to track abuse across multiple domains.

1.3.1.6 Issues encountered when using WHOIS data

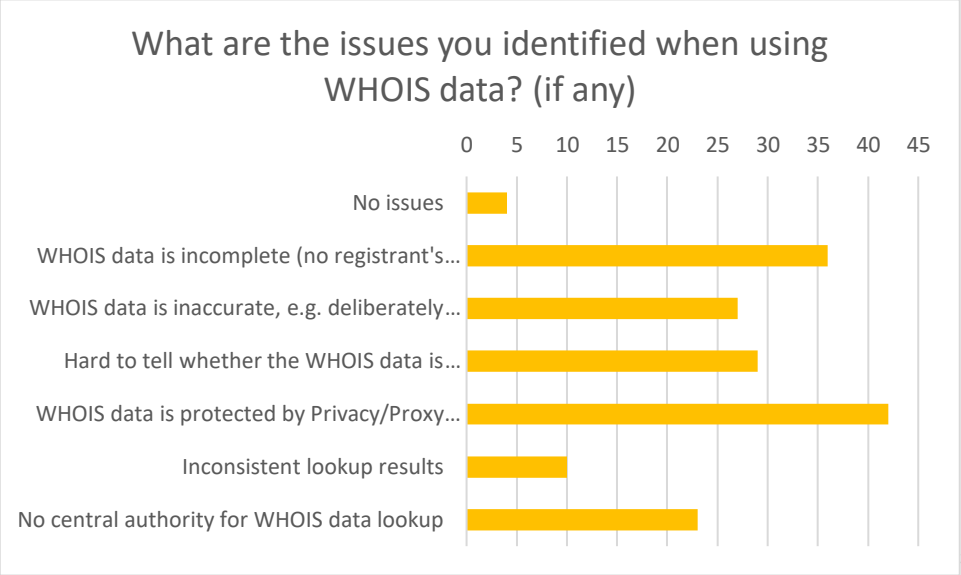
Respondents were asked whether the WHOIS lookup functionality (anonymous & public access) prior to May 2018 met their needs for the purposes of law enforcement investigations.



Those who responded "Partially" or "No" were asked to specify in which ways WHOIS did not meet their investigative needs. A large proportion of respondents (38%) cited inaccurate data, 12% referred to no data being available, and 50% named other issues, such as

incomplete information, inaccurate data (despite the separate answer category), falsified information, and the use of privacy and proxy services.

A dedicated series of questions then honed in on specific issues in WHOIS use, as far as possible. Survey respondents identified the following issues when using WHOIS data:



[3]

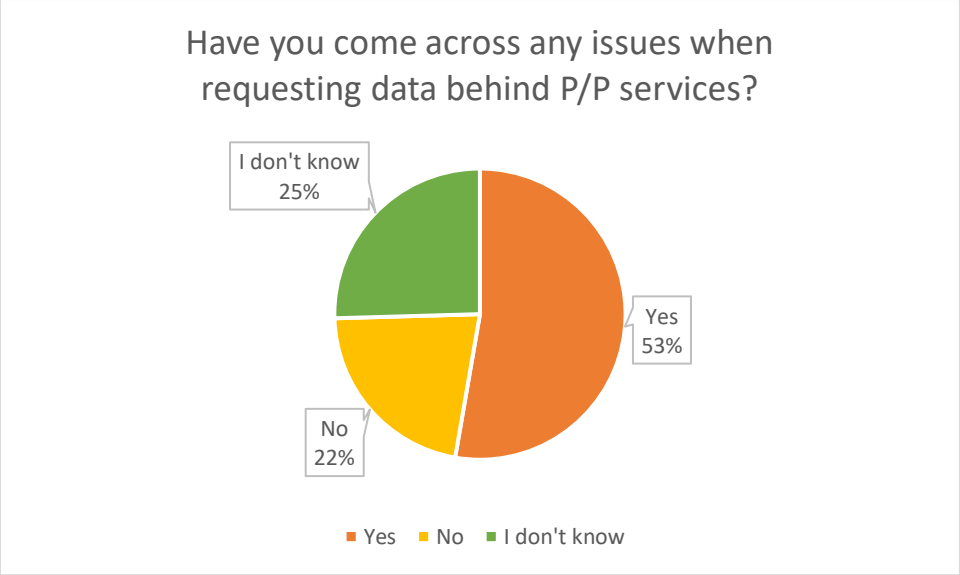
When put in order of importance, the use of privacy/proxy services scores highest among the issues (listed by 76% of respondents), followed by incomplete available WHOIS data (65%), challenges in determining whether the data is accurate (53%) and inaccurate WHOIS data (49%). It is to be noted that it is not clear from the responses how law enforcement can ascertain the use of a privacy/proxy service as opposed to fake data being provided.

These results show that, despite the recommendations made by the previous WHOIS Review Team and ICANN's efforts to implement them, one major user group still faces largely the same issues as it did in 2012. The use of Privacy/Proxy services, which was not yet prevalent in 2012, has risen to become the top challenge.

1.3.1.6.1 Issues related to Privacy and Proxy services

A number of questions targeted Privacy/Proxy services specifically, starting with whether respondents had come across any issues when requesting data behind privacy and proxy services:

[3] Respondents were able to select multiple issues.



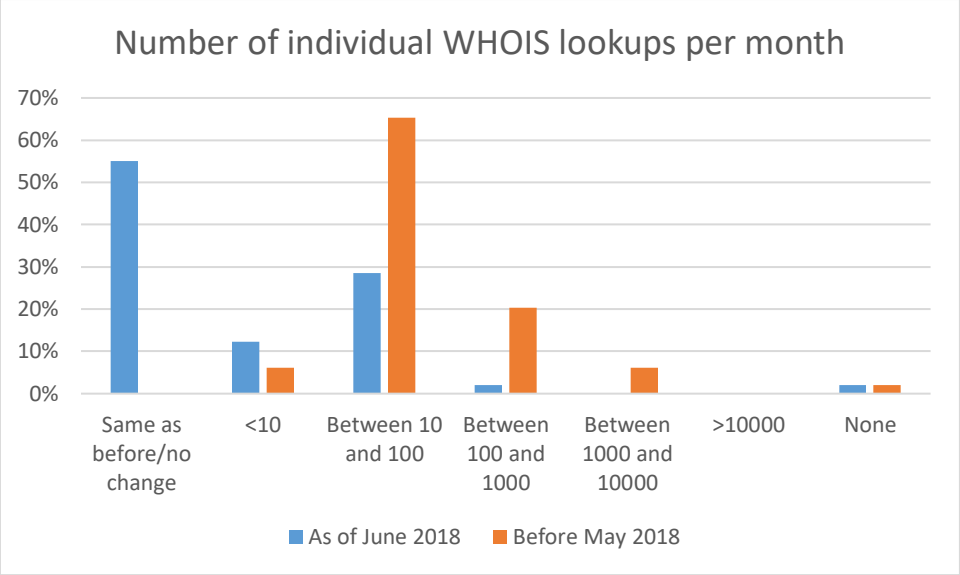
Those respondents who chose "yes" were then asked to further specify the issues they faced. A number of respondents listed jurisdictional challenges, as the privacy or proxy service provider was outside their jurisdiction and would not respond without a national order. The time it took to obtain data was named as too long by several respondents, and a number of them also stated that they received no reply or the service was uncooperative.

When asked whether they were able to obtain data on the actual registrant, 72% said no. 97% said that the cooperation with the P/P service did not function well; only in 21% of cases was the data obtained in time to allow the investigation to proceed. For 79% of investigations, the failed cooperation with the P/P service effectively ended the investigation.

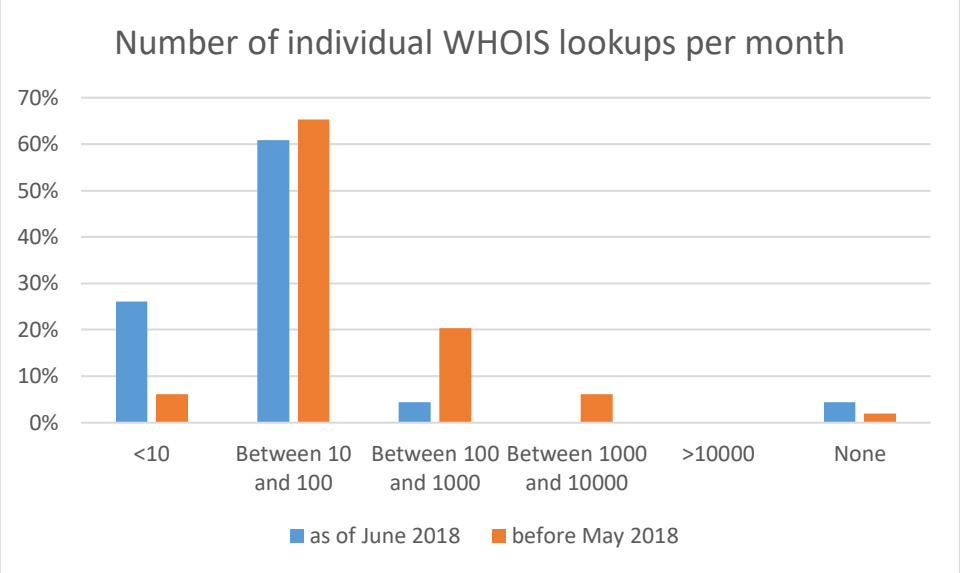
1.3.1.6.2 Impact of Temporary Specifications

The Subgroup also included a number of questions to attempt to assess the initial impact of the Temporary Specifications. According to feedback from law enforcement, many units are still busy investigating cases that concern actions taken before May 2018. As a result, the data available in particular in the private tools used for law enforcement WHOIS lookups is still pre-May 2018 data and therefore many investigations are not yet affected by the changes brought about by the Temporary Specifications. When asked whether their use of the WHOIS lookup had changed since May 2018, 44% consequently responded "no". 47% responded "yes" and 9% were not sure.

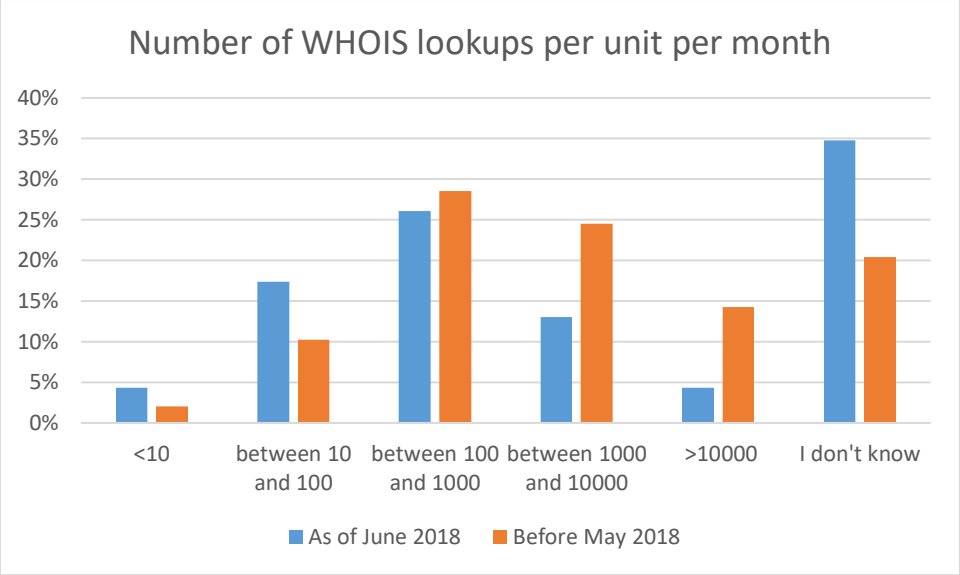
Nonetheless, an impact is already beginning to show, as evident from the following charts. Those respondents who indicated that use had changed were asked a number of follow-up questions, starting with how many lookups per month they now made:



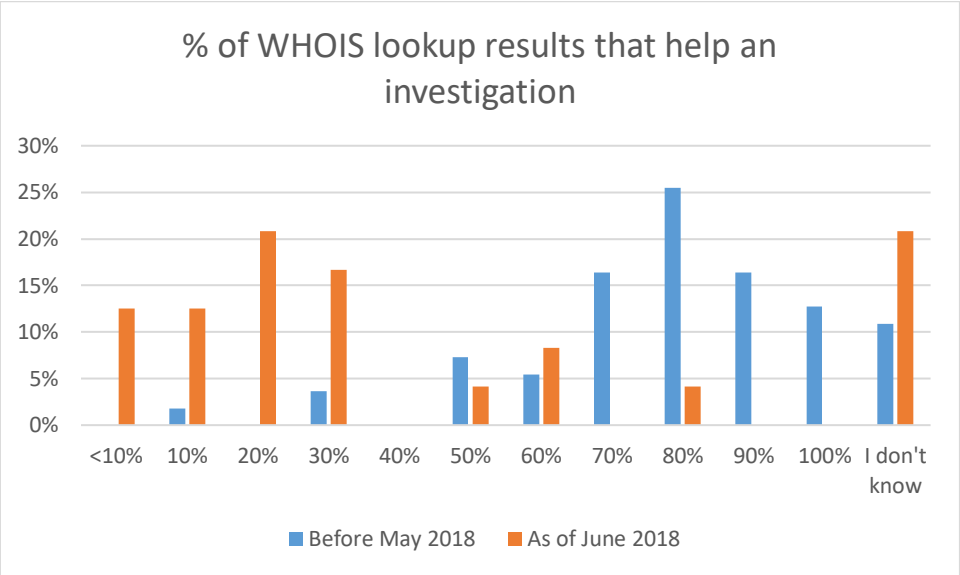
When all respondents are included, the difference is hard to tell, but when the "same as before" category is factored out, it becomes evident that the number of individual lookups has already decreased somewhat on average:



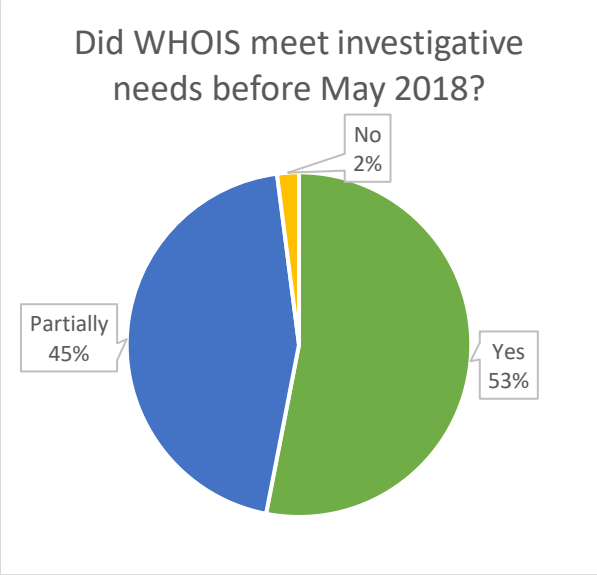
The same trend can be observed when comparing the requests per unit per month:

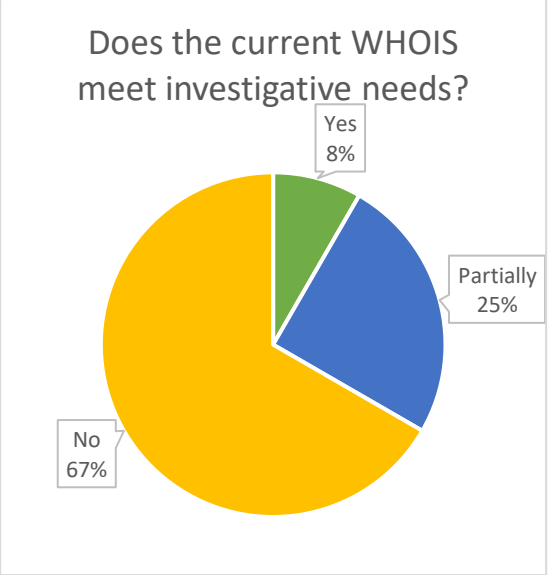


The overall rates of lookup have dropped slightly, even when factoring in the larger percentage of "I don't know" replies. Respondents were also asked about changes in usefulness of WHOIS lookups; the survey asked them to estimate the percentage of WHOIS lookup results that help their investigation. While the pre-May 2018 usefulness has its peak around 80% of lookups being useful to investigations, the June 2018 estimates show a strong decrease in that peak, which shifts to around 20% of lookups:



This change is also reflected in the responses to the question of whether WHOIS met investigative needs before the Temporary Specifications went into effect and now. As shown in the graphs below, the number of respondents who did not find that the WHOIS lookup functionality met their needs increased from 2% to 67%.





When asked to further specify the problem compared to before, respondents cite

- the lack of data availability,
- the impossibility of detecting patterns given the dearth of information,
- the different and time-consuming request processes across registries and registrars,
- the loss of confidentiality of requests, and
- the change from a quick and somewhat helpful system to one that relies on many different forms of requests which may go unanswered.

One respondent referred to a severe disruption of criminal investigations.

Respondents were able to provide final comments before ending the survey. Of those who chose to comment, many comments mainly refer to these recent changes, highlighting the need for law enforcement from all across the world to have swift access to data not just from their own jurisdiction.

1.3.2 Other input from law enforcement

Beyond the survey, law enforcement also provided evidence of its uses of the WHOIS at various points in time, including

- during the data mapping exercise conducted by ICANN in summer 2017;[4]
- at a number of High Interest Topic and Cross-Community sessions at ICANN meetings[5];
- and in reports and presentations, notably to the Governmental Advisory Committee and its Public Safety Working Group.

This input and examples provided largely confirm the findings of the survey, highlighting:

- that access to the WHOIS is an important tool for law enforcement;
- that law enforcement struggles both with inaccurate data (while highlighting that even inaccurate data may allow the detection of patterns or provide helpful leads) and with the use of Privacy and Proxy Services;
- and that law enforcement is significantly impacted by recent changes to the WHOIS by the Temporary Specifications.

[4] Available on ICANN's gTLD Registration Dataflow Matrix and Information page; see in particular input provided by the GAC Public Safety Working Group, Europol, the U.S. FBI, Canadian Criminal and Consumer Protection Law Enforcement Agencies and the U.S. IRS.

[5] Including the ICANN57 Update on WHOIS Related Initiatives, the ICANN56 Next-Generation RDS Cross-Community Session,

1.4 Problem/Issue

The problem identified on the basis of the input summarized above is two-fold:

- First, despite the efforts made in following up on the previous WHOIS Review Team's recommendation, the survey results make it clear that law enforcement still felt faced with a large number of inaccurate records. In addition to the previous issues, the prevalence of Privacy and Proxy services seems to have become a larger issue.

- Secondly, when considering the changes brought about by the Temporary Specifications in an effort to secure compliance with the GDPR, law enforcement seems particularly impacted in their investigations. This is clear in particular from the significant drop in usefulness of WHOIS lookups from around 80% to around 20% of lookups among those agencies that can already detect an impact, and from the large increase in respondents who are not satisfied with the WHOIS lookup functionality when comparing pre-May 2018 figures with June 2018 figures.

1.5 Recommendations

For the issues concerning data accuracy and the use of privacy and proxy services, reference is made to the relevant sections of the report.

For the issues that have arisen due to the implementation of the Temporary Specifications, an expedited policy development process is under way. Therefore, no specific recommendation is deemed necessary at this point in time; the survey results can be taken into due account by the policy development team. Given the limited and staggered scope of the exercise, which will deal with the problems relating to access only if and once a number of other questions are answered, the Review Team will take stock of the issue and of a possible need for further recommendations before issuing its final report.

The Review Team has come to the conclusion, as outlined above, that insufficient data is available to support in-depth analysis of the WHOIS functionality and of whether it meets requirements set out in the Bylaws for review. An ad-hoc study or survey as performed here or commissioned by other Review Teams can only partially replace a regular data gathering exercise as it does not allow tracking of trends over time. Therefore, the Review Team **recommends** that:
Recommendation LE.1:

- The ICANN Board should resolve that regular data gathering through surveys and studies are to be conducted by ICANN to inform a future assessment of the effectiveness of WHOIS in meeting the needs of law enforcement, as well as future policy development (including the current expedited Policy Development Process and related efforts).

Recommendation LE.2:

- Such surveys and/or studies should also extend to other WHOIS users, such as cybersecurity professionals and related professionals.

Findings: The Review Team found that the lack of available data on WHOIS uses, advantages and shortcomings had a negative impact on the possibility to assess the functionality of the WHOIS and whether it meets requirements set out in the Bylaws.

Rationale: The intent behind this recommendation is to ensure that future reviews, but also policy development processes, can benefit from a better and more reliable evidence base.

The issues identified could best be addressed by repeated data gathering exercises that include the running of surveys at regular intervals to create comparable data sets.

The potential impact of not addressing the recommendation would be a continued lack of data, which has already shown to add to current problems plaguing both reviews and policy development processes, where disagreement on basic facts has sometimes led to significant and enduring conflict.

This recommendation is aligned with ICANN's Strategic Plan and Mission, which already seek to reflect the strategic priority given to WHOIS and which could benefit from a better evidence base to assess whether its own projects and processes meet KPIs.

This recommendation is also within the scope of the RT's efforts.

Impact of Recommendation: This Recommendation would impact ICANN as an organisation, creating an administrative burden. It would contribute to the legitimacy, transparency and accountability of the organization and the ICANN community, by ensuring that a better evidence base is made available to assess the uses and other aspects of the WHOIS and further develop WHOIS policy.

Feasibility of Recommendation: Given that the main burden of surveys lies on the respondents, the feasibility of the recommendation will depend on their willingness to participate. However, in light of the importance attributed to the WHOIS in recent discussions, this risk seems to be manageable. Conducting surveys and possibly also studies would create an administrative and possibly also financial burden for ICANN as an organisation, which however seems manageable in light of the benefits that are to be expected.

Implementation: The implementation has to be provided by the ICANN Board and organisation. A successful implementation would consist in a Board resolution within the next six months that is then put into practice by the ICANN organisation, e.g. through annual surveys of relevant user groups as defined by policy development processes.

Priority: This recommendation creates an essential factual basis for further discussion and analysis. It is therefore considered a high priority.

Level of Consensus: TBD

1.6 Possible impact of GDPR and other applicable laws

Please see above under 1.3.1.6.2 "Impact of Temporary Specifications".