Agenda Item 11: PSWG Activities Update

Issue

This session in an opportunity for the GAC's Public Safety Working Group (PSWG) to present a summary of its recent activities that pertain to public policy issues in the area of public safety and consumer protection.

Highlights of recent activities:

- Development of contributions for the GAC regarding ICANN's intiiatives in relation to Whois compliance with GDPR (see Agenda Item 21 for full development of Whois and GDPR related matters)
- Development of GAC comments on the DNS Abuse recommendations contained in the New Sections of the CCT Review's Draft Report (16 January 2018)
- PSWG Intersessional meeting in Brussels on 12-13 February 2018
- Engagement with ICANN's Consumer Safeguards function (28 February 2018)

During ICANN61, the PSWG will also:

- Nominate a new Co-Chair, Laureen Kapin (US FTC) to work with current Co-Chair Cathrin Bauer-Bulst , consistent with criteria presented to the GAC in Abu Dhabi (see attachment 1)
- Seek GAC endorsement of an updated work plan, based on a strategy it has developed since ICANN60 in alignment with its Terms of Reference and relevant challenges and opportunities (see attachement 2)

GAC Action Required

Regarding the PSWG's Work Plan 2018-2019

1. Members to review, seek clarification or comment as needed, via email before Tuesday 13 March COB or face to face at ICANN61 during the PSWG Update to the GAC Plenary (Agenda Item 11) or the PSWG Meeting (Agenda Item 20).
2. Approve of language to be proposed in the ICANN61 GAC Communiqué for formal adoption of the PSWG work plan

Regarding the nomination of a new PSWG co-chair

1. GAC Members to take note of the nomination of Laureen Kapin (US FTC) to join Cathrin Bauer-Bulst (European Commission) as PSWG co-chair, and support language to be proposed in the ICANN61 GAC Communiqué to that effect.

Current Position & Recent Developments

DNS Abuse Mitigation

- In its Hyderabad Communiqué of 8 November 2016, the GAC requested written answers from ICANN on a set of targeted questions relating to DNS Abuse and ICANN's efforts at prevention, mitigation and response. The questions covered implementation of the 2013 RAA, Registrars accreditation, implementation of New gTLD Applicant Guidebook, Registry Agreement, and DNS Abuse mitigation through the ICANN Contractual Compliance department.

- On 8 February 2017, the ICANN CEO provided its answers in a letter to the GAC Chair. However, the information provided by ICANN was not sufficiently detailed to conduct the necessary assessments.

- On 15 March 2017, the GAC followed up and advised the ICANN Board in the Copenhagen Communiqué to "provide written responses to the questions listed in the Follow-up Scorecard […] no later than 5 May 2017".

- On 30 May 2017, the ICANN CEO provided draft answers to the Scorecard before engaging with the GAC in a dialogue concerning DNS Abuse and ICANN's processes, as proposed by the ICANN Board in its 26 April 2017 Scorecard on GAC Advice.

- A first Abuse Mitigation Dialogue with the ICANN CEO was held on 14 June 2017. The GAC set the goal to: 1) initiate a regular conversation to continue to address concerns, 2) establish metrics and standards for proactive monitoring of DNS Abuse and 3) seek regular reporting of Abuse and relevant actions/inactions by ICANN.

- The dialogue led to the identification of new initiatives that may address some of the remaining concerns and reporting needs in future. In particular, the PSWG has identified, engaged and is monitoring several ongoing initiatives that are expected to contribute to the establishment of regular public reporting of DNS Abuse by ICANN, both from a substantive and procedural perspective:
    - Domain Abuse Activty Reporting Tool
    - Identifiers Techonology Heath Index
    - gTLD Marketplace Health Index
    - Abuse Study Commissioned by the CCT Review

- On 22 September 2017, a GAC Public Comment was submitted on the above Abuse Study, highlighting the importance of regular, detailed and public reporting.

- During ICANN60 in Abu Dhabi, the GAC sponsored a Cross-Community Session on Reporting of DNS Abuse for Fact-Based Policy Making & Effective Mitigation at ICANN60 in Abu Dhabi, which set out to discuss the establishment of reliable, public and actionable DNS Abuse reporting mechanisms for the prevention and mitigation of abuse, and to enable evidence-based policy making.

- The session confirmed the need for publication of reliable and detailed data on DNS Abuse, as contained in the Domain Abuse Activity Reporting (DAAR) tool. The PSWG plans on futher developing a set of draft GAC principles in this regard while monitoring progress on the development of DAAR's as well as how ICANN's Consumer Safeguards Initiatives may facilitate bridging policy gap identified through abuse reporting, among other means.

- On 16 January 2018, with input from the PSWG, the GAC submitted comments endorsing DNS Abuse recommendations contained in the New Sections of the CCT Review's Draft Report. These included the use of incentives to encourage proactive DNS abuse mitigation measures and the need to fill policy gaps related to actors that are consistently seen to have abnormally high rates of abuse, as well as the collectoin by ICANN of chain of custody information of all parties responsible for gTLD domain names registrations, including resellers.

PSWG Intersessional meeting in Brussels on 12-13 February 2018

- The European Commission hosted a face-to-face intersessional meeting of the PSWG with more than 60 attendees, including cybercrime experts form 25 EU Member States and 3 associated States participating in the EMPACT Programme (European Multidisciplinary Platform against Criminal Threats).

- While the focus of this meeting was to address the impact of Whois compliance with GDPR on Law Enforcement access to domain registration data, the meeting was also an opportunity for law enforcement representatives to familiarize themselves with the activities of ICANN and to discuss the work plan of the PSWG.

- Participants in the meeting have identified specific needs and challenges that need to be addressed in the implementation of any GDPR-compliant Whois system so that Law Enforcement retains full access to Whois data while providing appropriate data protection safeguards (see Agenda Item 21 for full development of Whois and GDPR related matters).

- Law enforcement participants also discussed the workplan of the PSWG which lays out the future work for the period 2018-2019 and identified a number of opportunities for improving the outreach of the PSWG to law enforcement practitioners.

- For more information, please refer to the attached Chair's Conclusions of the meeting (Attachment 3).

Document Administration

Title	PSWG Activities Update
GAC Brief No.	ICANN61 Agenda Item 11
Distribution	GAC Members
Distribution Date	7 March 2018
Prepared by	GAC PSWG

ATTACHMENT 1: PSWG Co-Chair Selection Criteria

Considering that 2 of the 3 co-Chairs initially nominated for the PSWG have stepped down over the past year, the PSWG has been seeking to nominate at least one replacement.

To that effect, it introduced proposed selection criteria during the ICANN60 meeting in Abu Dhabi.

Considering input received from GAC Members, the criteria guiding the selection fo PSWG co-chairs are as follows:

- Geographic and gender diversity
- Active and sustained contribution to the GAC, the PSWG and/or ICANN (possibly over a period of 2 years)
- Expertise in public safety and Internet Governance issues
- Experience of ICANN's multi-stakeholder community
- Ability to devote substantial time and effort to the PSWG's work

ATTACHMENT 2: PSWG Work Plan 2018-2019

Please see document starting next page

PUBLIC SAFETY WORKING GROUP (PSWG)

Work Plan – 2018-2019 – Final Draft for GAC Endorsement

STRATEGIC GOAL 1 - DEVELOP CYBERCRIME AND DNS ABUSE MITIGATION CAPABILITIES

Develop capabilities of the ICANN and Law Enforcement communities to prevent and mitigate abuse involving the DNS as a key resource

No.	Work Topic	Description/Expected Outcomes	Completion	PSWG Topic Lead	Relevant Stakeholders/Processes/Work Products
1.1	DNS Abuse Reporting	Drive development of effective abuse reporting tools and processes promoting effective policy approaches and proactive industry self-regulation and enabling effective contractual compliance enforcement by ICANN	Q4 2018	Iranga Kahangama (US FBI)	– ICANN Domain Abuse Activity Reporting Project – ICANN Identifier Technology Health Index – ICANN gTLD Marketplace Health Index – SSAC - Establish collaboration mechanisms – Statistical Analysis of DNS Abuse – GAC DNS Abuse Reporting Principles
1.2	DNS Industry Due Diligence and Prevention	Work with DNS Industry stakeholders and ICANN to: develop tools and mechanisms to prevent abuse in gTLDs; and facilitate law enforcement investigations across borders	2018/2019	Iranga Kahangama (US FBI)	– ICANN Specification 11 3(b) Advisory – ICANN Security Framework for Registries to Respond to Security Threats – GNSO New gTLD Subsequent Procedures PDP – ICANN Privacy/Proxy Services Accreditation
1.3	Consumer Safeguards	Assist in the developments of ICANN's Safeguards to protect the public; contribute to and follow-up on relevant ICANN Reviews, Review recommendations and implementation, and liaise with the the Consumer Safeguards Director, as appropriate, to work together to achieve our mutual goal to safeguard consumers	2018/2019	Laureen Kapin (US FTC)	– ICANN CCT Review Team – Implementation of Recommendations – ICANN SSR 2 Review Team – GNSO New gTLD Subsequent Procedures PDP – ICANN Privacy/Proxy Services Accreditation

No.	Work Topic	Description/Expected Outcomes	Completion	PSWG Topic Lead	Relevant Stakeholders/Processes/Work Products
1.4	Accountability	Review data available on DNS abuse, particularly data available through ICANN's ongoing data collection systems such as DAAR, highlight this data for ongoing policy development efforts so that future policy is informed by relevant data; Ensure that provisions from the contracts related to DNS Abuse are applied and enforced, as well as reviewed and improved, where needed	Ongoing	[TBD]	– ICANN Contractual Compliance team and mechanisms – GNSO New gTLD Subsequent Procedures PDP – GNSO Next-Generation Registration Directory Services (RDS) PDP – Development of best practices (e.g. Spec 11) – Raising awareness within and outside the ICANN Community (incl. cross-community sessions during ICANN meetings)
1.5	Preventing Exploitation of DNS to Perpetuate Abuse	Identify how the DNS is used to perpetuate abuse (including but not limited to DDOS, Botnets, and facilitating distribution of illegal materials such as those associated with counterfeit drugs and child sexual abuse). Consider building upon the ICANN Beijing Communiqué safeguards and development of policies for subsequent gTLD rounds; support proactive action.	Q3 2018	Cathrin Bauer-Bulst (European Commission)	– ICANN Domain Abuse Activity Reporting Project – GNSO New gTLD Subsequent Procedures PDP – .KID/.KIDS New gTLDs String Contention – ICANN Auction Proceeds Cross-Community Working Group

STRATEGIC GOAL 2 - PRESERVE AND IMPROVE DOMAIN REGISTRATION DIRECTORY SERVICES EFFECTIVENESS

Ensure continued accessibility and improved accuracy of domain registration information that is consistent with applicable privacy regulatory frameworks

No.	Work Topic	Description/Expected Outcomes	Completion	PSWG Topic Lead	Relevant Stakeholders/Processes/Work Products
2.1	Access to gTLD Registration Data	Ensure maintenance of swift and effective access to gTLD Registration data for the legitimate needs of civil and criminal law enforcement (including consumer protection authorities) to protect the public and support the public interest	Q2 2018	Laureen Kapin (US FTC)	– ICANN Whois Compliance with GDPR – ICANN Procedure for Handling Whois Conflict with Privacy Laws
2.2	Next Generation Protocols and Policies	Guide the exploration of protocols and policies through active participation in relevant processes and timely input, including on law enforcement requirements for accessing layered RDS	2018/2019	Gregory Mounier (Europol)	– ICANN RDAP Pilot Program – GNSO Next-Generation Registration Directory Services (RDS) PDP
2.3	Registration Data Accuracy	Continue driving initiatives geared towards increasing the quality of gTLD registration data, including by highlighting and leveraging data quality requirements in data protection legislation	Q4 2018	[TBD]	– ICANN WHOIS Accuracy Reporting System (ARS) – ICANN WHOIS Accuracy Program Specification and Registrar Across Field Address Validation – GNSO Next-Generation Registration Directory Services (RDS) PDP – GNSO New gTLD Subsequent Procedures PDP – ICANN Privacy/Proxy Services Accreditation
2.4	Performance of ICANN's Mission in relation to RDS	Monitor ICANN's performance of its key bylaw responsibilities with regards to accuracy, access and protection of gTLD registration data	2019	Cathrin Bauer-Bulst (European Commission), Lili Sun (Interpol), Thomas Walden (US DEA)	– ICANN RDS Review Team

STRATEGIC GOAL 3 - BUILD EFFECTIVE AND RESILIENT PSWG OPERATIONS

No.	Work Topic	Description/Expected Outcomes	Completion	PSWG Topic Lead	Relevant Stakeholders/Processes/Work Products
3.1	Define Strategy and Workplan	Define Strategy and Workplan in alignment with PSWG Terms of Reference, GAC guidance and priorities, and ICANN Bylaws, taking into account current challenges and opportunities	Q1 2018	Cathrin Bauer-Bulst (European Commission)	– PSWG Terms of Reference – PSWG Strategy and Workplan – Relevant GAC Advice and Principles – New ICANN Bylaws
3.2	Strengthen Leadership	Establish a strong and resilient leadership structure to ensure sustained and coherent PSWG activities	Q2 2018	Cathrin Bauer-Bulst (European Commission)	– Endorse Co-chair selection criteria – Select New Co-chair – Workload distribution among Topics Leads – Invite new Topic Leads
3.3	Strengthen Membership	Provide regular and predictable structure of meetings to address the needs of various GAC and PSWG Stakeholders interested in PSWG activities; ensure outreach to stakeholders unable to (regularly) attend ICANN face-to-face meetings; identify opportunities for contribution to the work of the group in supporting the GAC	Q2 2018	[TBD]	– Weekly leadership meetings – Monthly working group meetings – Intersessional face-to-face feetings – Ad hoc topical meetings and webinars for PSWG and GAC Members – Outreach activities – Newsletter
3.4	Reporting and Coordination with the GAC	Ensure alignment of PSWG focus and activities with GAC priorities and GAC consensus decision making, by providing regular opportunities for GAC/PSWG leadership coordination and ensuring GAC review and possible endorsement of key PSWG work products	Continuous	[TBD]	– PSWG Activity Report to the GAC – GAC briefings and webinars – GAC endorsement procedure – Establish effective liaison with GAC Leadership

STRATEGIC GOAL 4 - DEVELOP PARTICIPATION IN PSWG WORK AND ENSURE STAKEHOLDER INPUT

No.	Work Topic	Description/Expected Outcomes	Completion	PSWG Topic Lead	Relevant Stakeholders/Processes/Work Products
4.1	Continually Assess Operational Needs and Seek Expert Input	Identify current and future policy issues and opportunities in support of the operational needs of public safety agencies. Seek expert input from public safety agencies, through PSWG Members and relevant international organization and forums, to inform contributions to the GAC and relevant ICANN processes	Continuous	[TBD]	– Input from GAC – Input from PSWG members – Outreach of PSWG members in their agencies, governments and regions – Dedicated meetings, webinars and/or conference calls on key topics
4.2	Develop Awareness of PSWG by Government Agencies	Communicate regularly on PSWG activities and achievements that are relevant to national government's priorities in order to secure commitment for effective PSWG membership participation	2019	[TBD]	– PSWG quarterly newsletter – GAC capacitybBuilding workshops – PSWG monthly calls – Outreach of PSWG members within their agencies, governments and regions
4.3	Lowering arriers to Participation	Provide opportunities for effective participation for GAC and PSWG Members, at varying levels of expertise, into PSWG work initiatives	Q3 2018	[TBD]	– PSWG Newsletter and regular calls – Leverage GAC website, including access to non-public content for PSWG members – Repository of ongoing PSWG initiatives, briefings and work products – Internal Position Drafting Procedure

No.	Work Topic	Description/Expected Outcomes	Completion	PSWG Topic Lead	Relevant Stakeholders/Processes/Work Products
4.4	Develop Onboarding Program	Create tools, information materials and training opportunities for new participants to ICANN and the PSWG to enable them to quickly become effective in a new environment and contribute with their experience and positions; create mentor/buddy system for new members, especially those attending ICANN meetings for first time	Q2 2018	Sara Marcolla (Europol)	– Updated Law Enforcement Guide to ICANN – Onboarding package – Mentoring System – ICANN Meetings Introduction Program – ICANN introduction presentation at intersessional meeting

ATTACHMENT 3: PSWG Intersessional Chair's Conclusions

Please see document starting next page, with selected attachments included (a full version of the document is available on the GAC Website).

GAC PUBLIC SAFETY WORKING GROUP (PSWG)

PSWG Intersessional Meeting – 12-13 February 2018
Chair's Conclusions

I. OBJECTIVES

The Public Safety Working Group of ICANN's Governmental Advisory Committee (GAC), together with cybercrime experts from 25 EU Member States and 3 associated States participating in the EMPACT Programme (European Multidisciplinary Platform against Criminal Threats), met to address the the impact of the impending reform of the Whois service and protocol, which may entail loss of public access to Whois data. This reform is set to address long-standing data protection concerns, which have become more acute with the coming into effect of the EU General Data Protection Regulation (GDPR) in May 2018.

While the focus was on Whois, this meeting was also an opportunity for law enforcement representatives to familiarize themselves with the activities of ICANN and how, within ICANN, law enforcement can influence the development of policies that are applied through contracts, across the domain industry. It also served to provide an introduction to the DNS abuse mitigation work of the GAC PSWG.

II. WHOIS IS CRITICAL FOR LAW ENFORCEMENT INVESTIGATIONS

The public availability of worldwide Whois data from which law enforcement agencies and other legitimate users have benefited for many years, has been the subject of concerns by data protection authorities since 2003. To better protect the privacy of domain name registrants, there is a plan to move to a "layered access" model where personal data (and as likely implemented, even some corporate data) will no longer be publicly accessible.

Several models under consideration in the ICANN community are proposing a wide range of solutions in terms of:

- data collection requirements (what data is collected from registrants of domain name)
- accessibility of data by third parties (including law enforcement among other legitimate users)
- retention of collected data (for maintenance of historical records in particular)

The GAC, the European Commission and the US Government have advised[1] ICANN to adopt solutions that preserve current legitimate uses of public Whois data to the maximum extent possible in compliance with data protection rules, while providing for swift and practical access to non-public data for law enforcement.

As illustrated by the German Federal Criminal Police Office (BKA) and Europol, domain registration data made available through the Whois system is critical to law enforcement investigations. While the quality and accuracy of such data is uneven, it is almost always instrumental in generating investigative leads and ultimately attributing crime. Participants also identified the value of Whois data to identify victims of cybercrime. Examples cited included domain owners in cases of hijacked domains (using past Whois data) and in cases of compromised domains (using present-day Whois data). Law enforcement also referred to the use of Whois to identify a child victim of sexual abuse which was rescued using information on the domain name registrant committing the abuse and sharing images of it.

[1] See actual contributions from the GAC, the European Commission (commissioner's letter, comments) and the US Government.

III. LAW ENFORCEMENT NEEDS TO RETAIN FULL ACCESS TO WHOIS DATA, WHILE PROVIDING APPROPRIATE DATA PROTECTION SAFEGUARDS

Participants in the meeting have identified specific needs and challenges that need to be addressed in the implementation of the new GDPR-compliant Whois system, including:

- **Scope of personal data collection**: investigations show that all data elements can prove valuable, while the data minimization and proportionality principles of the GDPR may require a reduction of the amount of data available
- **Practicability of access to non public data**: modalities of access to non-public data need to be consistent across all Top-Level Domains (TLDs) and commensurate with high rates of access needed by law enforcement for specific types of investigations (e.g. botnets)
- **Cross-referencing, search capabilities and historical records of Whois data**: law enforcement agencies need replacements for third-party services (such as those available from Domain Tools) that used to rely on the public availability of all Whois data. This includes new features of Whois, as well as appropriate data retention specifications (including for changes of registration information).
- **Confidentiality of requests for non-public data**: while law enforcement generally recognize the greater trustworthiness of registries compared to registrars, requests for non-public data by law enforcement should not be identifiable by concerned parties in order to avoid compromising investigations
- **Cybersecurity firms access**: trusted partners in cybercrime investigations need to retain access to full data
- **National accreditation of law enforcement agencies to access gated data**: national accreditation would be preferable to a centralised accreditation system as it is best left to national governments to assess which law enforcement agencies should be granted which competences. However, this could present challenges because each nation has a distinct set of law enforcement entities. Some nations have thousands of law enforcement entities at the federal, state, and local levels. Implementing such an accreditation system could take considerable, time, effort, and resources.

IV. NEXT STEPS IN WHOIS COMPLIANCE WITH GDPR

The PSWG in collaboration with the GAC is preparing to assist in providing feedback and guidance regarding the selected model soon to be chosen by ICANN and implementation thereof.

To that effect, the PSWG is currently refining a set of Law Enforcement Requirements for a Future Layered Access Model which it has started discussing with interested parties in the industry and the technical community. Further outreach is planned to other parts of the community. These requirements could form a basis for discussions also with data protection and technical experts to determine data protection-compliant solutions and identify the most privacy-protective means of implementation.

V. PSWG WORK PLAN AND OUTREACH

Law enforcement participants also discussed the workplan of the PSWG which lays out the future work for the period 2018-2019 in order to achieve its 4 strategic objectives:

1. Developing capabilities of the ICANN and Law Enforcement communities to prevent and mitigate abuse involving the DNS as a key resource
2. Ensuring continued accessibility and improved accuracy of domain registration information that is consistent with applicable privacy regulatory frameworks
3. Building effective and resilient PSWG operations
4. Developing participation in PSWG Work and ensuring appropriate stakeholder input

A number of opportunities for improving the outreach of the PSWG to law enforcement practitioners have been identified, including:

- Informing about opportunities for contributions to ICANN public comments
- Offering webinar on issues of interest to law enforcement as well as material explaining the role of the PSWG in ICANN's multi-stakeholder model
- Creating a law enforcement Internet governance mailing list to support the involvement of law enforcement representatives that are not yet members of the PSWG
- Creating a monthly PSWG newsletter that provides updates on current activities and issues of interest
- Identifying opportunities for input to PSWG work

VI. LIST OF PARTICIPANT COUNTRIES (ALPHABETICAL ORDER)

Austria
Belgium
Bulgaria
Canada
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Luxemburg
The Netherlands
Norway
Poland
Portugal
Romania
Slovenia
Spain
Sweden
Switzerland
United Kingdom
United States
Zambia

ANNEXED DOCUMENTS

1. Agenda of day 1 of the meeting (12 February 2018)
2. Agenda of day 2 of the meeting (13 February 2018)
3. Draft Proposal for minimum requirements for LEA access to a future layered access model to non-public domain registration data (as of 9 February 2018)
4. Draft PSWG Work Plan (as of 26 February 2018)
5. PSWG presentation material (selected meeting slides)
6. Presentation of ICANN (meeting slides)

EUROPEAN COMMISSION
DIRECTORATE-GENERAL MIGRATION and HOME AFFAIRS

Directorate D: Security
Unit D.4 : Cybercrime

Brussels, 5 January 2018
HOME.D.4/CBB

Members of the ICANN GAC PSWG
Members of the EMPACT Priority on Cyber Attacks

Subject: **GAC PSWG intersessional meeting on the future of WHOIS and DNS abuse mitigation**

Dear PSWG members, dear EMPACT participants,

For many years, law enforcement agencies (LEAs) have relied on WHOIS services, which provide publicly available domain name registrations information. The WHOIS is a key tool to investigate and attribute crime. Data Protection Agencies have long identified issues with the public availability of personal data contained in the WHOIS; nonetheless, the ICANN community has not yet managed to come to agreement on any replacement policy, and LEA access to such data has been largely unaffected. This is now set to change fundamentally in the coming months, before the entry into effect of the EU GDPR on 25th May 2018.

To discuss the latest developments around WHOIS and DNS abuse, their impact on public safety stakeholders, and possible measures to mitigate this impact, the European Commission would like to invite you to **Brussels, Belgium**, for an intersessional ICANN Governmental Advisory Committee Public Safety Working Group (GAC PSWG) meeting which will take place on **12th February 2018**. This workshop will bring together members of the GAC PSWG and representatives of EU Member States' law enforcement agencies participating in the EMPACT priority on cyber attacks; it should result in a better understanding of the needs of these two groups and concrete measures to take them into account. The language of the meeting will be English; no translation will be provided.

We will also use this opportunity to review progress on measures for prevention and mitigation of Domain Name System abuse and identify next steps, as well as to discuss the work plan and outreach for the GAC PSWG. This should also extend to how better to integrate public safety stakeholders unable to participate in face-to-face ICANN meetings.

Please find enclosed the draft agenda of the day. If you intend to participate, please register until 18th January 2018 using the following form: https://ec.europa.eu/eusurvey/runner/PSWG.

The European Commission will reimburse one participant per EU Member State for EMPACT members and up to 15 members of the PSWG (topic leads have priority; the remaining reimbursements will be attributed according to the time of registration [first come, first serve]). Please do not make your own booking for travel or hotel; our contractor will be in touch with you to arrange your travel.

For the EMPACT participants, please note for your travel plans that Europol plans to organise a related workshop on 13 February in Brussels for which you may wish to stay on. Further information on this workshop will be provided by Europol directly.

Please contact our functional mailbox HOME-NOTIFICATIONS-D4@ec.europa.eu for any questions regarding the registration or reimbursement.

We look forward to discussing these important issues with you and count on your numerous and active participation in the event.

Yours sincerely,

Cathrin Bauer-Bulst

Cathrin BAUER-BULST
Deputy Head of Unit
Co-Chair, GAC PSWG

Encl.: Agenda of the workshop on 12th February 2018.

PSWG Intersessional Meeting on 12th February 2018

Agenda

Time: Monday, 12th February 2018, 10:00 h to 18:00 h.

Place: Albert Borschette Congress Center (CCAB), Room 1B, rue Froissart 36, 1040 Etterbeek.

Participants will have to undergo a security check which includes a visual inspection with X-rays.

Time	Issue	Leader
10:00 h	Welcome and opening of the workshop	Cathrin BAUER-BULST (EC)
10:10 h	Presentation of the WHOIS model(s) received (and possibly chosen) by ICANN	TBD
10:30 h	Needs of law enforcement (LE)	Grégory MOUNIER (Europol)
11:00 h	Coffee break	
11:20 h	Discussion of the model(s) and their fulfilment of LE needs (part 1)	Cathrin BAUER-BULST (EC)/Laureen KAPIN (US FTC)
12:50 h	Lunch break	
13:40 h	Discussion of the model(s) and their fulfilment of LE needs (part 2)	Cathrin BAUER-BULST (EC)/Laureen KAPIN (US FTC)
14:40 h	DNS abuse mitigation	Iranga KAHANGAMA (US FBI)
15:40 h	Coffee break	
16:00 h	PSWG Work Plan and Outreach	Cathrin BAUER-BULST (EC)/Grégory MOUNIER and Sara MARCOLLA (Europol)
18:00 h	Closing	Cathrin BAUER-BULST (EC)

The Hague, 25/01/18
EDOC#941193-v2

AGENDA

GAC PSWG-EMPACT meeting on the future of WHOIS and DNS abuse mitigation – Day 2: RDAP

Date(s)	13 February 2018	Start: 9:00	End: 13:00

Place **DG HOME, Falcone/Borsellino on the ground floor of the LX46 building.**

Participants **EUCTF delegates, Private Partners, DG HOME, ICANN EC3 staff**

Time	Subject	Responsible
09:00 – 09:10	Welcome note and opening of the meeting	Gregory Mounier EUROPOL Cathrin Bauer-Bulst DG HOME
09:10 – 10:00	Presentation of the RDAP pilot project	Francisco Arias ICANN
10:00 – 11:00	RDAP Implementation - Verisign	Marc Anderson and Rick Wilhelm Verisign
11:00 – 11:30	Coffee Break	
11:30 – 12:45	Discussion: LEA requirements	Tour de table
12:45 – 13:00	Conclusion End of meeting	Gregory Mounier EUROPOL

Background paper

Minimum requirements for LEA access to a future layered access model to domain registration data

1. Aim

- To receive feedback from the EU law enforcement community on practical requirements for LEA access to non-public WHOIS information.
- To prepare the discussion with VERISIGN on the RDAP pilot programme on 13th February 2018.

Do you have experience using gated/layered access systems, e.g. on the basis of credentials assigned to you personally or to your organisation? Which requirements exist for your organisation? Could you please prepare comments on the minimum requirements proposed on page 3 (part 4)?

2. Background

For many years, law enforcement agencies (LEAs) have relied on WHOIS services, which provide publicly available domain name registrations information to investigate and attribute crime online.

Data Protection Agencies have taken issue with the public availability of personal data contained in the WHOIS[1]; nonetheless ICANN policy related to WHOIS in gTLDs has not evolved significantly as the community did not manage to come to agreement on any replacement policy, and LEA access to such data has been largely unaffected.

This is now set to change fundamentally with the entry into effect of the EU GDPR on 25 May 2018. A growing body of legal opinions[2] recognizes that collection and publication of personal data contained in the WHOIS database is unlawful and that compliance with GDPR will likely involve reducing the number of data elements collected and implementing purpose-based access to differentiated subsets of the remaining registration data, also known as **layered access.**

As a consequence, while the legitimacy of law enforcement access to registration data, including personal data, for investigations purposes is generally not challenged, LEA access to such data will be affected, both from a practical and from a legal perspective. Practically speaking, there will be fewer data elements and therefore fewer leads available. Cross-referencing data elements across different registrations, e.g. to identify which other domains a bad actor may have registered using the same information, would likely no longer be possible.

Currently under consideration are the following models:

[1] https://www.icann.org/en/system/files/correspondence/falque-pierrotin-to-chalaby-marby-06Dec17-en.pdf

[2] https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf; https://gnso.icann.org/en/drafts/wsgr-icann-memorandum-25sep17-en.pdf

- a model where every WHOIS lookup would require an individualized request justifying the purpose for access, specific data elements sought, etc., possibly validated by a judge;
- a model where some form of authentication would be provided, allowing access for law enforcement by means of logins and passwords. Such access might be provided through a centralized clearinghouse logging access requests and verifying proportionality.

While such models are advantageous from a data protection perspective, they might create a number of challenges and risks for law enforcement. In particular, individualized access requests would be difficult to fathom in view of the fact that one cyber unit might make as many as 50,000 lookups a week. Tracking and tracing law enforcement activity might reveal sensitive data, potentially compromising investigations if revealed or illegally accessed.

In addition, while law enforcement access is not contested, it is unclear whether and how other relevant actors would maintain current levels of access. This concerns in particular cybersecurity authorities, private sector companies and academic researchers; consumer protection authorities, or IP right holders.

3. Recent developments[3]

Based on consultations with contracted parties, European data protection authorities, legal experts, and interested community stakeholders, ICANN proposed on 12 January 2018, **three potential interim compliance models** with ICANN agreements and policies in relation to the EU's GDPR.[4] **All three models introduce a variation on layered access to WHOIS data.** The variations of the three models revolve around geographic scope (EU-centric or global), scope of publication of data elements, and third party access to non-public data.

In line with GDPR requirements, ICANN defines five distinct purposes for the WHOIS system, including two specific purposes related to law enforcement needs and investigating cybercrime.

a. *Supporting a framework to address issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection; and*

b. *Providing a framework to address appropriate law enforcement needs.*

Regarding law enforcement access to non-public data, ICANN proposed three options:

i) Self-certification of legitimate interest to be approved by each registry/registrar;

ii) Certification programme to be developed in consultation with the GAC[5];

iii) Court order or legal requirement.

ICANN requested feedback on these interim potential compliance models by 29 January 2018. It intends to decide on and **publish a single model by mid-February 2018**.

[3] For an overview of the WHOIS reform issue please see p.11 of the Progress report.

[4] https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf

[5] Governmental Advisory Committee of ICANN where all EU Member States are represented together with the European Commission: https://gacweb.icann.org/display/gacweb/GAC+Representatives

This model will then serve as the standard for ICANN itself and for compliance with the WHOIS obligations under the Registrar and Registry contracts. In practical terms, it will be the one and only WHOIS model.

Among the many contributions received by ICANN, please note the following:

- **GAC Comments** (prepared by the PSWG): https://www.icann.org/en/system/files/files/gdpr-comments-gac-icann-proposed-compliance-models-29jan18-en.pdf
- **European Commission**: https://www.icann.org/en/system/files/correspondence/avramopoulos-et-al-to-marby-29jan18-en.pdf
- **United States:** https://www.icann.org/en/system/files/files/gdpr-comments-usg-icann-proposed-compliance-models-29jan18-en.pdf
- **UK NCA:** https://www.icann.org/en/system/files/files/gdpr-comments-nca-icann-proposed-compliance-models-29jan18-en.pdf
- **WIPO:** https://www.icann.org/en/system/files/files/gdpr-comments-wipo-icann-proposed-compliance-models-29jan18-en.pdf
- **Registrar Stakeholder Group:** https://www.icann.org/en/system/files/files/gdpr-comments-rrsg-icann-proposed-compliance-models-29jan18-en.pdf
- **A group of contracted parties (including Donuts, GoDaddy and others):** https://www.icann.org/en/system/files/files/gdpr-comments-contracted-icann-proposed-compliance-models-29jan18-en.pdf
- **IPC:** https://www.icann.org/en/system/files/files/gdpr-comments-ipc-icann-proposed-compliance-models-29jan18-en.pdf
- **ECO Association:** https://www.icann.org/en/system/files/files/gdpr-comments-eco-icann-proposed-compliance-models-29jan18-en.pdf

4. Proposal for minimum requirements for LEA access to a future layered access model to domain registration data:

In order to guarantee EU LEA access to essential WHOIS data, the PSWG is seeking to define a **set of minimum requirements** to guarantee timely LEA access to the appropriate elements of a **GDPR-compliant Registration Directory Services (RDS).**

These minimum requirements might also be used as a joint input from the LEA community to the RDAP pilot program currently underway, testing a replacement protocol to WHOIS and which will allow for gated access[6].

Because a layered access model implies **credentialing**, **authenticating** and **authorizing users** to access data that is not made public and may be hosted in foreign jurisdictions, below is a first series of draft minimum requirements for a future layered access model for discussions.

2.1. Basic principles

[6] https://community.icann.org/display/RP/RDAP+Pilot

- The different **legitimate purposes** for which processing of registration data takes place should be clearly and explicitly set out in the policy rules that apply to such processing, from collection to storage and access of data.
- Processing of WHOIS data for law enforcement purposes, e.g. investigating and countering serious crime, fraud, consumer deception, intellectual property violations, and other law violations, constitutes a legitimate interest for processing of personal data. The processing of personal data shall be lawful and necessary for the performance of a task carried out by a competent authority for law enforcement purposes, in line with applicable data protection legal framework.
- These purposes should therefore **cover the legitimate need for law enforcement access to WHOIS data[7] to sustain public interests** such as cybersecurity; the stability, reliability and resilience of the network; preventing and fighting crime; protecting intellectual property rights, copyright and consumer rights; and other rights recognised in the domestic legal order.
- Registrants should be **informed in a clear and easily understandable manner** about these purposes and the related data processing when making, updating or extending registrations in line with the principle of transparency.

2.2. Necessary data elements

- The model should give nationally-accredited actors, **access to all the WHOIS data necessary for the fulfilment of their task**, subject to the requirements that should be clearly stated in the processing policy of WHOIS data.
- This includes **all current registration information available, public and non-public, personal and non-personal**, including email and phone number of registrant, name and postal address of technical and administrative contacts, and billing details, which should continue to be collected by registries and registrars.

2.3. Accreditation system

- **Accreditation** of Law Enforcement and Public Safety agencies which have a legitimate need to access WHOIS data for the purposes mentioned in 2.1, should be carried out at **national level** instead of being carried out centrally, e.g. at European or global level.
- The accreditation system should **ideally guarantee access for other relevant actors**, based on the specific purposes defined pursuant to point 2.1 for processing, including accessing of WHOIS data, comprising non-public elements. This concerns in particular cybersecurity authorities, private sector companies and academic researchers, consumer protection authorities, or intellectual property right holders.
- States should keep an **updated list of public *(and private entities)* located in their respective jurisdiction**, which are allowed to access non-public WHOIS data on the basis of relevant domestic legislation. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or

[7] As recognised by ICANN's Bylaws (ICANN Bylaws Article One, Section 1.1; Section 1.2 (a) Commitments and Core Values; Registration Directory Services Review, §4.6(e)

otherwise processed and to what extent the personal data are or will be processed. Therefore, the list of the public and private entities should be published in a Register which is made accessible to the public.

- This system could be based on the **certification programme** described by ICANN in relation to the second model of the interim GDPR compliant WHOIS system[8], provided that programme can accommodate the minimum requirements described in this document. The set of requirements for the issuance of certificates should be clear and transparent.

2.4. Authentication of access

- Authentication mechanisms should be compatible with the rate of look-ups expected from authorised users.
- Nationally-accredited requestors (with a legitimate need to access non-public WHOIS data based on domestic law) should be provided with the necessary level of access to requested WHOIS data through a **unique set of credentials**.
- Access WHOIS data needs to be maintained regardless of location of storage. This could be achieved in practice through a **centralised federated access system**, e.g. hosted by ICANN.

2.5. Access policy, data location and confidentiality

- Nationally-accredited entities with a legitimate need to access non-public WHOIS data on the basis of domestic law, **should have permanent access to WHOIS data on a query basis**. Access should not be based on individualised requests justifying the purpose for access, specific data elements sought, nor should it be required to provide a subpoena or any other order from a court or other judicial authority to gain access to non-public WHOIS data.[9]
- There should be sufficient guarantees in place to ensure the implementation of the principle of accountability and purpose limitation. The logging and documentation of the queries and safety of the searches should be made available to the competent oversight authorities for the purposes of verifying the lawfulness of data processing, monitoring and auditing and ensuring proper data integrity and security.
- To ensure confidentiality of the requests, WHOIS data look-ups by nationally-accredited and authenticated actors should be anonymised, possibly through a system of hashes, be logged by them for audit purposes and they should not be limited by the number of lookups or time.

2.6. Accuracy and validity of data

- As stipulated by the **EU data protection legal framework** and in line with the obligations of contracted parties under their contracts with ICANN, personal data shall be accurate and kept up to date.

[8] See p. 7 of https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf

[9] Previously covered under section 2.3

- Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (retroactive database data correction with regards to the factual data situation found out during the investigation). To comply with the data quality principle, reasonable steps should be taken to ensure the accuracy of any personal data obtained.

2.7. Data Retention and Record of historical WHOIS data

- In order to ensure the availability of historical WHOIS data, the WHOIS system model should allow access to historical domain data retrospectively. Historical domain and IP ownership information[10] is necessary for the success of investigation by LEA and other parties, and thus an adequate retention policy for historical data should be implemented.
- Such records should also be searchable in such a way as to allow for cross-referencing of information, e.g. where the same data set was used to register several sites.
- In line with the storage limitation principle, data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, or scientific or historical research purposes.

[10] For example as offered by Domaintools.