Report on the Public Workshop at ICANN63 in Barcelona

We had a lot of stakeholder consultation to do for this project, despite the fact that Perrin was active on two major WHOIS committees throughout the research period, namely the Expedited Policy Development Process, or the EPDP, and the RDS II Review Team, the second formal review of the WHOIS. However, during this regular work (3-5 teleconferences a week, and 3-5 face to face meetings each), the opportunity to discuss potential solutions and debate models is not always there. We decided to hold a workshop at the Barcelona conference (October 20-25, 2018) to see if we could gauge the interest in privacy standards.

The goals of that workshop were the following:

- To discuss the issue of standards as a way of meeting privacy compliance requirements, and explore whether stakeholders at ICANN were interested in standards development;
- To activate interest in civil society stakeholders in Canada, in what appears at first glance to be a rather abstruse topic unrelated to privacy protection;
- To explore the risks at ICANN in the models currently being discussed to meet the standard of GDPR, with a focus on the disclosure of personal information to third parties. It is worth noting here that at the time we prepared for the workshop, we were still arguing in the EPDP over whether the personal data held by the Registrars had been collected and processed for the purpose of release to third parties;
- To discover any other potential issues where further research would be beneficial to this project on standards development.

We cooperated with the Noncommercial Stakeholders Group (NCSG) to request a meeting room from ICANN, and were granted a full afternoon slot on Sunday October 21st, from 1:30 to 6:30. This was not an ideal time, since many of the participants we hoped to attract were busy in other meetings, notably the important Generic Names Supporting Organization (GNSO) Council working meeting which took place all day, and the Security and Stability Advisory Committee (SSAC) meetings, but we nevertheless managed to attract an excellent crowd, at times with individuals standing at the back of the room, and at one count over 60 people in the room. Because such meetings are enabled for remote participation by Adobe connect, and are recorded with MP3s available for download, and in this case 111 pages of transcripts provided, this is an excellent and ongoing resource available here [https://63.schedule.icann.org/meetings/901739]

We invited representatives of a number of stakeholder groups to participate, focusing on those who were struggling to meet GDPR compliance (the contracted parties), representatives of the Cybercrime fighting community both within companies (Microsoft) and in associations (the Anti Phishing Working Group), the Security and Stability Advisory Committee of ICANN (SSAC), and representatives of Canadian civil liberties groups (the Canadian Civil Liberties Association, and the Canadian Internet Policy and Privacy Information Centre). Ayden Ferdeline of the NCSG (also a member of both the GNSO Council and the EPDP) did an excellent job moderating the meeting and keeping us on time. We had to do some real-time juggling of the agenda to accommodate various individuals being double booked in other meetings, but the event unfolded seamlessly. The transcript of the meeting is available as indicated above; this section of the report will amplify some of that discussion so as to provide greater background on some of the standards, processes, and issues discussed.

Perrin presented a very brief overview of how standards were viewed by the data protection commissioners, and how the provisions of the GDPR for codes of conduct and certification worked. There was little uptake of this during the workshop, but it may be that stakeholders are well aware of these provisions in the GDPR. The precise sections of the GDPR are as follows, with commentary:

> Section 5 Codes of conduct and certification
>
> Article 40 Codes of conduct
>
> 1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.
>
> 2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:
>
> (a) fair and transparent processing; L 119/56 EN Official Journal of the European Union 4.5.2016 (b) the legitimate interests pursued by controllers in specific contexts;
>
> (c) the collection of personal data;
>
> (d) the pseudonymisation of personal data;
>
> (e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure se 10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9. 11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

ICANN has been engaged in discussions with the European Commission, and apparently with the members of the European Data Protection Board. There has been, on high level panels and discussions, the occasional mention of the possibility of ICANN developing a code of practice for RDS (unclear as to whether this would be for disclosure to third parties only, or for the entire life cycle of the personal data). To many stakeholders at ICANN, the only important part is access to the WHOIS data, so how the registrars, resellers and registries are managing the data may be of lesser importance, although it is certainly not to the registrants. In any case, such a code would fit in here. There has been no substantive discussion of this at the EPDP, to the best of our knowledge.

Article 41 Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being,

implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Note that in the ICANN situation, a code that presumably the community had developed, would have to be monitored by an independent body that was certified by the competent supervisory authority, namely a member of the EDPB under whose jurisdiction they fall. We doubt that ICANN org would qualify as such an independent body, for several reasons:

- While they understand how the DNS works, they are not sufficiently independent or without conflict of interest. ICANN is funded completely on the sales of domain names. They have a vested interest in the principal contracted parties not failing. They also have a strong vested interest in the public perception that there are no privacy breaches or unacceptable conduct at ICANN, lest there be a loss of confidence in the domain name system.
- ICANN has shown a remarkable lack of interest in data protection matters over the past 20 years. They have yet to declare whether they are a controller, joint controller, or nothing at all with respect to registrant personal data. They are therefore ill suited to take on the role of evaluating performance of other controllers and joint controllers under such a code, and obviously if they

eventually decide they share elements of that control, they would have further conflicts.

Article 42 Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account. L 119/58 EN Official Journal of the European Union 4.5.2016

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43 Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council (1) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

Perrin referred to ISO/IEC 17065/2012 briefly in her remarks at the workshop. This standard sets out the criteria that a certification body has to follow in order to correctly assess whether a code of conduct is being followed. The Article 29 Working Party wrote to ISO to ask it to make the standard publically available, but to the best of our knowledge they have not done so, although the 2012 version has been revisited and affirmed as 17065/2019.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority; 4.5.2016 EN Official Journal of the European Union L 119/59 (1) Regulation

(EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

Opinions may differ as to whether or not ICANN could set itself up as a certification body. This matter has not been publically discussed at ICANN, but we will bring the matter up in Phase 2 of the EPDP, which is due to start at the end of April 2019. However the kind of accreditation that we have discussed at the EPDP is not the accreditation of independent third party auditors, but the accreditation of third parties who wish to gain access to the protected personal data in a tiered data access system. That kind of accreditation is not really envisaged in the GDPR, although a code of conduct could specify all the privacy management practices and risk management techniques that would be required to ensure compliance with law. It is important to note here that while the WHOIS has been a globally operating system, and it seems foolish to set up anything else in today's Internet, local law applies in terms of criminal and civil law, so a centralized system would always have to defer to local knowledge, most likely to be resident at the level of the registrar or reseller.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Clearly under any kind of certification scheme, there would be much closer interaction with the data protection authorities in Europe than there is at the moment.

Returning to the workshop, Elliot Noss of Tucows, the largest Canadian registrar, discussed their experience of requests, now that they have followed the temporary specification, reduced drastically the exposure of personal information, and are

implementing the Registration Data Access Protocol (RDAP). The volume of requests for disclosure of data, with the exception of AppDetex requests, has been very low. Appdetex have recently sent correspondence to ICANN, complaining about contracted parties not complying with their requests for data. It has been Tucows experience that Appdetex has consistently failed to provide the information necessary to permit disclosure under the law, and they did not respond to requests for further information in order to comply with their requests. A letter from Tucows discussing this matter was just sent to the CEO [https://www.icann.org/en/system/files/correspondence/noss-to-marby-chalaby-hedlund-21oct18-en.pdf] in response to complaints of registrar inaction sent by AppDetex [https://www.icann.org/en/system/files/correspondence/milam-to-chalaby-marby-12oct18-en.pdf]. As Elliot pointed out in his remarks, it is difficult to get beyond the rhetoric of access available/access denied, so getting into the nitty gritty of what we need to comply with law is a faint hope at the moment.

Theo Geurts from Realtime Register, a Dutch company who acts as a wholesaler for other registrars, discussed how low the volumes of requests actually are, now that they have reduced access to registrant data in order to comply with Dutch data protection law. He also talked about how they managed law enforcement requests and could turn out a rapid response for life and death issues in under an hour.

Mark Svancarek from Microsoft, who represents the business community at the EPDP, discussed how Microsoft manages its trust centre, [https://www.microsoft.com/en-us/trustcenter/default.aspx] what standards they comply with and how they manage their own requests for data (as an organization with a major problem of domain spoofing and phishing attacks). Mark also discussed Microsoft's compliance with GDPR, and at a high level, how they do Data Protection Impact Assessments.

We did not discuss whether in fact any of these companies would benefit from adherence to a privacy management standard, whether self certified or certified through an independent body. There are probably more large companies who adhere to the Cloud Computing privacy standard ISO 17018 which appeared in 2018, than to more complete privacy management standards. Obviously, Canadian companies would have to adhere to CAN/CSA-Q830 because it is part of the law, but others are not similarly obliged. We did discuss briefly the merits of compliance to voluntary standards (self certification) versus the burdens of becoming certified and paying for audit.

Richard Wilhelm of the large legacy registry Verisign presented his slides [https://static.ptbl.co/static/attachments/191584/1540126728.pdf?1540126728] on the recently completed RDAP trial implementation. Verisign manages among other gTLDs the .com, still the largest generic top level domain in the world. He and fellow engineer Scott Hollenbeck have been working recently on the RDAP protocol at the Internet Engineering Task Force (IETF) and formerly (2012-2014) on the WEIRDS (Web

Extensible Internet Registration Data Service) group of the IETF. He confirmed that in their view, RDAP was capable of delivering a broad range of authentication and scope narrowing functions which would enable a more GDPR compliant disclosure mechanism. We discussed tiered versus layered access, and he confirmed that the term is as yet undefined in the IETF. There is confusion in the community as to what is meant by these two terms, including in the data protection community. At the moment, it appears that some people, when using the term "layered access" mean that once you are accredited as a member of a group (e.g. lawyer, cybercrime practitioner, law enforcement officer) you gain access to an entire layer of data. This would not be compliant with the GDPR or any other data protection law. "Tiered access" is really a synonym, but is taken to mean a much more fine-grained approach to data based on specific requests.

Greg Aaron, of the Anti Phishing Working Group, described some of the work the members of the Anti Phishing Working Group (APWG) do, and the different ways in which they assure trusted information sharing. The APWG is one of the oldest and most trusted groups focused on fighting cyber attacks on the Internet and the DNS, and they share information about known threats and actors.

Rod Rasmussen is the current SSAC Chair but spoke in his own right as the former owner of a security company that worked closely with government, law enforcement and private sector companies to defend against attacks. He mentioned various ISO and NIST standards that they routinely use, to protect themselves, to guarantee that they can get insurance for their business, and to ensure trust among clients and fellow security agents and companies. Once again, while the security researchers use available expected security standards, there appears to be no eagerness to embark on the development of privacy standards.

Patrik Falstrom is the former SSAC Chair but spoke as the technical director and head of security at Netnode, an NGO who operates the DNS for around 30 global countries, resident in Sweden. They take an EU approach to data protection. Patrik focused on issues of trust, and how certifying to standards does not necessarily mean compliance, you have to audit to determine whether you can trust the company that says it is compliant to standards. Patrik (joined by Rod Rasmussen) stressed that the last thing you want to do from a security perspective is move data around to a central repository.

At this point in the agenda, we got into a fairly open discussion of what the risks really were, how to decide on whether you could trust an organization or a request for data, and we had to cut this rather interesting discussion short to return to the agenda and hear from the civil liberties representatives.

Tamir Israel (on the adobe connect) represented the Canadian Internet Policy and Privacy Information Centre (CIPPIC) in Ottawa and Brenda McPhail represented the Canadian

Civil Liberties Association (CCLA) Brenda's slides focused on the key elements that civil society are looking for in terms of Charter rights and due process in law enforcement disclosure requests [https://static.ptbl.co/static/attachments/191586/1540126796.pdf?1540126796]. She pointed out the Supreme Court case in Canada that supported the claim that access to subscriber data, including name and address, was impermissible without a warrant. Tamir Israel joined to discuss the merits and limitations of the Mutual Legal Assistance Treaties (MLATS) which provide assurance that proper due process is being followed in cross border requests. Following a discussion of these issues, they both proposed a new concept that they agreed might be useful in the ICANN situation: data trusts. Tamir explained what a data trust was, what kinds of data trusts currently exist, and then we had a discussion about how it might work at ICANN to replace the formerly open WHOIS publication. We were running out of time, but there was a good exploration of what this concept meant and how it had arisen in the context of the Internet of Things and Smart Cities.

This brief summary of the workshop gives a flavour of the material we discussed. As researchers, we found it incredibly useful as a mechanism to have a real discussion about the nuts and bolts of what works and what doesn't in the application of standards to the problem. Based on the input received, we reached the following conclusions:

- Further standardization in ISO could possibly be useful to improve privacy management standards, but in the current climate of frenzied application of the GDPR (not just at ICANN but globally) it was a non-starter in terms of getting people and organizations to contribute time and money.
- The IETF is continuing work on RDAP, and the recent trial, pending requirement to implement RDAP at ICANN, and potential application to replace WHOIS was focusing the standards attention there.
- While we cannot expect ICANN to turn on a dime and abandon a twenty year history of basically ignoring data protection law, nevertheless progress in embracing the details and realities of data protection law has been depressingly slow. As Elliot Noss noted in his remarks, we were barely having an intelligent discussion of the issues at the EPDP in October. Embarking on a process of privacy standards development seemed beyond a faint hope.
- Data trusts are a rather new idea, although certain kinds of repositories have existed for years (e.g. credit reporting agencies, cancer registries). Some are government, some operate for profit, but all attempt to share personal information for the "public good" although this term is perhaps more applicable in a health reporting environment than a for profit situation. ICANN has a unique, multistakeholder (MS) model of a potential digital trust, where the data is not collected but the disclosure mechanisms could be controlled and managed in a

MS policy environment, but with independent oversight by a Board, and the participation/oversight of data protection commissioners. This concept seemed attractive, if it could potentially relieve contracted parties of the burden of compliance verification, meet the requirements of data protection authorities (who could be represented in the Board or certify the resultant code of practice by which the trust operated), and relieve ICANN of further liability.

- A further benefit of a data trust is that it could exist in Europe, thus solving an adequacy issue that ICANN would probably face as a California institution, and it could have a close relationship to existing law enforcement criminal intelligence sharing organizations such as Europol and Interpol, who have existing well established data protection procedures for information sharing.

We decided to focus our efforts on researching different models of data trusts, and applying potential working models to the situation at ICANN. Once we determine what is necessary for compliance with the GDPR (it is not clear to the NCSG that this has emerged from the EPDP first phase activity, let alone the second phase which we have not started) there could be more interest in specific standards. In the meantime, it is clear that the rather nebulous concept of data trusts could benefit from legal analysis and determination of roles and responsibilities. This could result eventuallyt in a standardization activity.