Privacy Team Summaries - drafted by gnso-rds-pdp-privacy@icann.org

This file consolidates summaries drafted by individual members of the RDS PDP Privacy Team, focusing on portions of each identified document relevant to ***Registration Directory Services privacy and data protection.***

TABLE OF CONTENTS

Privacy Team Summaries - drafted by gnso-rds-pdp-privacy@icann.org

1. WHOIS Conflicts with Privacy Laws – Chronology and Summary, including

ICANN Procedure For Handling WHOIS Conflicts with Privacy Law (2008)
GNSO Policy underlying current procedure
Review of the ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2014)
Summarized by: Metalitz

On Oct. 25, 2005, a Combined Whois Task Force convened by the GNSO council to (among other things) "determine how to resolve differences … when there are conflicts between a registrar's or registry's legal obligations under local privacy laws and their contractual obligations to ICANN," issued a report. The Task Force recommended as a consensus policy that ICANN "develop and publicly document a procedure for dealing with the situation in which a registrar or registry can credibly demonstrate that it is legally prevented by local/national privacy laws or regulations from fully complying with applicable provisions of its ICANN contract regarding the collection, display and distribution of personal data via WHOIS." The Task Force report went on to approve "well-developed advice" for such a procedure. The Task Force's report was approved by the GNSO council on November 28, 2005, and was reported to the ICANN board on January 18, 2006. The board adopted the consensus policy on May 10, 2006.

The consensus policy (which remains in force) adopts goals for the conflicts procedure, including early notice to ICANN staff; " resolving the conflict, if possible, in a manner conducive to ICANN's Mission, applicable Core Values and the stability and uniformity of the Whois system;" authorizing exceptions to contractual obligations for specific conflicts if they cannot otherwise be resolved; and preserving flexibility.

A staff-developed procedure for implementing the consensus policy was adopted effective Jan. 17, 2008. The procedure, which is also currently in force, sets out a six-step process, that begins with notification to ICANN staff of an action that "might affect [a contracted party's] compliance with the provisions of [its] contractual agreement with ICANN." The next step is a consultation process that "seek[s] to resolve the problem in a manner that preserves the ability of the registrar/registry to comply with its contractual WHOIS obligations to the greatest extent possible." In the third step, General Counsel Analysis and Recommendation, ICANN can provisionally refrain from enforcing certain contract provisions while the General Counsel prepares and posts a report to the Board that summarizes the conflict, the consultation process, and a recommended resolution. Board action on the report (as well as the justification for it) will "ordinarily be made public," along with related materials. The sixth step calls for "ongoing review" of the effectiveness of the procedure.

Although the procedure calls for annual review of the process, in fact no such review was formally undertaken before 2014. An Implementation Advisory Group formed to assist staff in this review submitted an initial report on October 5, 2015, which focused primarily on the first step of the procedure, and specifically on whether the trigger for invoking the procedure should be modified. The IAG reached preliminary agreement on expanding the existing trigger so that, even in the absence of "an investigation, litigation, regulatory proceeding or other government or civil action that might affect its compliance" with contractual obligations, a contracted party could invoke the procedure based on "a

written statement from the government agency charged with enforcing its data privacy laws indicating that a particular WHOIS obligation conflicts with national law." Two other proposed expanded triggers failed to achieve majority support within the IAG. Although public comments have been received on the IAG initial report, no final report has been issued to date.

2. Title: 2013 RAA's Data Retention Specification Waiver and Discussion Document (2014)

Summarized by: Metalitz

- Under the Data Retention Specification to the 2013 Registrar Accreditation Agreement (RAA), ICANN-accredited domain name registrars are obligated to "collect and securely maintain" specified data elements that are either obtained from registrants at the time of registration, or that are generated in connection with the registration process. The RAA requires that these data elements be retained by registrars either for two years following the end of the registrar's sponsorship of the domain name in question, or for 180 days following specified interactions between registrars and registrants, depending on the data involved. Note that one item listed in the Data Retention Specification (item 1.1.6) is "WHOIS Information, as set forth in the WHOIS Specification" to the RAA; and that some other items listed (e.g., items 1.1.1 through 1.1.5) overlap with data currently made publicly available via Whois, while others (e.g., items 1.1.7 and 1.1.8) do not. (In other words, the data elements covered by the Data Retention Specification form a superset of the data elements currently collected and made available via Whois.) The Data Retention Specification also provides a procedure for registrars to request waivers from some or all of these obligations, based on evidence that compliance with the obligations would violate applicable law.

- Public Comment Request: In March 2014, ICANN issued an announcement stating that, in the context of discussions about waiver requests under the Data Retention Specification, "some Registrars have requested that ICANN …. "describe potentially legitimate purposes for collection and retention of each data element" listed in the Data Retention Specification. This would "help provide guidance for Registrars both as to whether such elements may be lawfully collected, and, if so, for how long such elements might be lawfully retained."

- Discussion Draft: As noted in the Public Comment Request, ICANN drafted, and sought public comment on, a document listing "Potentially Legitimate purposes for Collection/Retention" of each data element listed in the Data Retention Specification. For item 1.1.6, covering WHOIS information, ICANN identified the following as a "potentially legitimate purpose":
    - "Data Enabling Registrar to populate and make available to the public community the WHOIS register both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP)
    - "Abuse mitigation"
    - "Facilitating domain name purchases and sales."

The Discussion Draft also provides "explanations" for some of these "potentially legitimate purposes," including the last two listed under the item above.

- Comments: Note that these documents may address a wider range of issues than those on which this PDP focuses, both because they encompass transactional data elements well outside the scope of the historic Whois, and because they deal with retention of the data after the expiration of the registration or the end of its sponsorship by a particular registrar.

- It is also not clear who responded to the public comment notice on the Discussion Document; what their comments were; and how if at all ICANN took these into account. In contrast to the usual notice appearing on the ICANN public comment page, it does not appear that any "comment forum" was published, nor any summary of the comments received. Finally, the current status of the ICANN-provided "potentially legitimate purposes" is unknown. Perhaps ICANN compliance could provide more information on these points.

3. Title: WHOIS Privacy/Proxy Abuse Study and WHOIS Privacy/Proxy Relay and Reveal Survey

Summarized by: Folly

WHOIS Privacy and Proxy Relays & Reveal – Pre-Study Feasibility Survey

According to http://gnso.icann.org/en/group-activities/other/whois/studies*: "This survey particularly assessed the feasibility of conducting a future in-depth study into communication Relay and identity Reveal requests sent for gTLD domain names registered using Proxy and Privacy services"*

The document recaps the following:
On March 7th of 2011, the GNSO council issued a motion to conduct a feasibility survey on the matter titled above. However, ICANN staff concluded after many investigations that it was too premature for such a survey to be conducted. Instead, a pre-survey was suggested with the aim to determine whether the launch of the full study is feasible and how. Actually many barriers to conduction a full survey were identified and among them we can name the difficulty to find diverse participants for a very large outreach and the fact that many of the willing participants are likely no able to provide all the data elements intended to be collected by the survey.

The goal of this pre-survey is mainly to determine study cost and duration associated with the full survey. So the proposed approach was to build a team of senior researchers with a solid background on the problem, study goals, and contacts needed for community outreach. The Interisle Consulting Group in Boston, MA, USA performed this survey and posted final results in August 2012. The report of this survey, available via this link, stated that a full study is feasible mainly if some strong decisions are taken to overcome the barriers cited in the pre-survey document.

Study on WHOIS Proxy/Privacy Abuse

The objective of this document was to answer a critical question submitted by ICANN on how to assess truth on the following hypothesis: "A significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via privacy or proxy services to obscure the perpetrator's identity". The study was conducted by the National Physical Laboratory of Cambridge, and directed by Dr Richard CLAYTON. The research found it useful, also, to consider the following hypothesis: "The percentage of domain names used to conduct illegal or harmful Internet activities that are registered via privacy or proxy services to obscure identity is significantly greater than the equivalent percentage of domain names used for entirely lawful Internet activities".

On the issue raised above, the research team concluded that when domains names are maliciously registered, privacy/proxy services are used more than the average. But some legal and harmless activities also use privacy/proxy services. When those types of services are not used in a malicious registration, 90% of the registrants cannot reached directly by phone.

4. Title: SAC055, WHOIS: Blind Men and an Elephant (September 2012)

Summarized by: Folly

This document is a comment made by the SSAC to the ICANN Board in order to advise on matters related to security and Integrity of the Internet's naming and address allocation systems. This document covers three main aspects including operational, administrative, and registration matters.

The Group compares the WHOIS problem to the tale of "the Blind men and the elephant" where each one of them touches the elephant, feels its body differently, and when it comes to comparison, everyone thinks the other is wrong. Consequently, there is a crucial need to understand the purpose of the domain name registration and elaborate an appropriate policy which must address the following questions:

- Why data are collected
- What purpose will the data serve
- Who collects the data?
- Where is the data stored and how long is it stored?
- Where is the data escrowed and how long is it escrowed?
- Who needs the data and why?
- Who needs to logs of access to the data and why?

The SSAC believed in the formation of an authorized committee to drive solutions to these questions and, then, derive a universal policy from the answers. The SSAC advises ICANN to do so, and a Review team was created.

Although many recommendations have been made to solve those issues, many questions still remained unsolved within the ICANN community. Moreover the creation of the universal policy by the Review

Team does not yield to the resolution of the most critical question concerning the purpose of the WHOIS. The review team even remarks that the term WHOIS is used differently by the community to mean different things, and a new taxonomy was proposed. The SSAC reviewed, also, issues related to Public Access to Domain Registration Data, Law Enforcement Access to Domain Registration Data, Intellectual Property Practitioner Access to Domain Registration Data, and Security Practitioner access to domain registration data.

Globally, the SSAC answers to the review team and all their recommendations have been categorized into three categories: high priority, medium priority, and Low priority.

For high priority recommendations which are critical to the successful completion of the medium and the low priority recommendations, we have:

- Strategic priority : ICANN CEO to create a domain name policy committee that includes the highest level of executive management
- Single WHOIS policy : to clearly state that the development of a uniform policy is critical priority
- Compliance : the policy committee to develop clear targets for compliance with respect to registration data accuracy; performance provisions

Medium priority recommendations include:

- Data accuracy
- Data access : privacy and proxy services
- Internationalized domain names

Low priority (can sometimes start at the same time with high priority recommendations) recommendations include:

- Outreach
- Data Access : common Interface
- Internationalized domain names
- Detailed and comprehensive Plan
- Annual Status reports

Regarding each aspect, the SSAC made a particular recommendation to the ICANN board.

5. Title: Privacy & Proxy Services Accreditation PDP Final Report (2015)

Summarized by: Metalitz

In recommending standards for the accreditation of services providing privacy or proxy registration of domain names, this Working Group addressed numerous issues dealing with privacy and data protection aspects of gTLD registration data policy. Some of the most relevant conclusions and recommendations in

the WG's Final Report (all of which achieved full consensus among the WG) include the following. Note that these recommendations have been approved unanimously by the GNSO Council, and as of April 2016 are pending before the ICANN board for action.

- Privacy/proxy ("P/P") services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals. Further, P/P registrations should not be limited to private individuals who use their domains for non-commercial purposes (Rec. 3).
- Contact data of p/p service customers should be validated and verified in a manner consistent with the requirements of the Whois Accuracy Program Specification of the 2013 Registrar Accreditation Agreement. (Rec. 5).
- P/P service providers must clearly communicate to their customers, in the service registration agreement, the rights, responsibilities and obligations of customers and services. Rec. 6.)
- P/P service providers must publish the criteria they will use to respond to requests to disclose (to a specific requester) or to publish (to the public in general) the identity or contact information of their customers. (Rec. 7).
- Published terms of service for P/P service providers must include "the specific grounds upon which a customer's details may be disclosed or published," including whether or not a provider will be notified of third-party requests for disclosure or publication, and whether customers will be allowed to cancel domain name registrations in lieu of disclosure or publication (Rec. 8).
- P/P service providers should be fully contactable and should designate an abuse point of contact. (Recs. 11-14).
- A uniform set of minimum mandatory criteria that must be followed for the purpose of reporting abuse and submitting requests (including requests for the Disclosure of customer information) should be developed. (Rec. 15).
- Minimum standards for the relaying of electronic communications from third parties to P/P service customers are established. (Recs. 16-17).
- The Working Group noted, and did not seek to alter, "the prevailing practice among p/p service providers to facilitate direct resolution of an issue between a third-party requester and a p/p customer, including through disclosure of some contact details of the customer." (Rec. 18)
- The WG developed an illustrative Disclosure Framework to apply to disclosure requests made to P/P service providers by intellectual property (i.e. trademark and copyright) owners. The proposal includes requirements concerning the nature and type of information to be provided by a requester; non-exhaustive grounds for a provider's refusal of a request; and the possibility of neutral dispute resolution in the event of a dispute. The Framework requires prompt notification to the customer of compliant requests to disclose contact information. The Framework aims to balance the interests of predictability and certainty (for requesters); flexibility and discretion (for p/p service providers); and

reasonable safeguards and procedures to protect the legitimate interests and legal rights of customers. (Rec. 19 and Appendix B.)

- While no similar Disclosure Framework was adopted by the WG for requests from law enforcement or consumer protection agencies, the WG made recommendations about features such a future-developed framework should contain, and recommended that "accredited P/P service providers should comply with express requests from law enforcement agencies not to notify a customer where this is required by applicable law. However, this recommendation is not intended to prevent providers from either voluntarily adopting more stringent standards or from cooperating with LEA." (Rec. 20).

Please note that a document extracting the recommendations from the Final Report, along with other information submitted to the ICANN board regarding the PDP, may be found at: http://gnso.icann.org/en/drafts/council-board-ppsai-recommendations-09feb16-en.pdf .

6. Title: Thick WHOIS PDP Final Report (2011-2013) and IRT Legal Review

Summarized by: Metalitz and Metalitz

Thick Whois PDP WG Final Report (2013)

The Working Group convened by ICANN which developed the proposed consensus policy requiring thick Whois architecture for all gTLD registries established a subgroup on the impact on privacy and data protection. The WG's final report stated that the "fundamental question before the thick Whois PDP WG is whether thin and thick registry models present different risks with respect to data protection and privacy." After reviewing the risks and benefits both for data at rest and data in motion, the WG concluded (see p. 30 of the final report):

"Data Protection: The WG finds that requiring thick Whois for all gTLD registries does not raise data protection issues that are specific to thin vs. thick Whois, as those that have been identified already exist in the current environment and should be considered as part of the broader Whois debate.

"Privacy: There are currently issues with respect to privacy related to Whois, and these will only grow in the future. Those issues apply to other gTLDs as well, and thus will need to be addressed by ICANN. Existing registry policy and practice allows flexibility when needed, and the new draft RAA provides similar options for registrars. None of these issues seem to be related to whether a thick or thin Whois model is being used. The support of the Registrar Stakeholder Group related to a thin-to-thick transition implies that they perceive no immediate issue. There are still WG participants who feel uneasy with the vast amounts of data that will need to be transferred across jurisdictional boundaries, but those have not translated into concrete concerns. So although privacy issues may become a substantive issue in the future, and should certainly be part of the investigation of a replacement for Whois, it is not a reason to not proceed with this PDP WG recommending thick Whois for all."

The WG included as one of its additional recommendations the following: "As part of the implementation process [of a thick Whois consensus policy] a legal review of law applicable to the transition of data from a thin to thick model that has not already been considered in the EWG memo is undertaken and due consideration is given to potential privacy issues that may arise from the discussions on the transition from thin to thick Whois, including, for example, guidance on how the long-standing contractual requirement that registrars give notice to, and obtain consent, from each registrant for uses of any personally identifiable data submitted by the registrant should apply to registrations involved in the transition." (See separate summary re this legal review.)

Finally, pp. 47-48 of the WG report include some privacy-related "observations" (not consensus recommendations), including that "as part of the development of the registration data directory system model currently in process, ICANN ensure that the ramifications of data protection and privacy laws and regulations with respect to Whois requirements be examined thoroughly." Specific suggestions include:

- "Examinations must include data collection, data disclosure, and data retention laws, as well as data quality requirements under data protection principles.
- "Given the dynamic nature of laws and contracts that may address what data protections should be in place, as well as increasing complexities, the examinations must be limited to: provisions that have the force of law at any given time, authoritative statements from relevant governments about those provisions, or contract provisions that are final."
- "Some level of real world review of the efficacy of data protection provisions must occur as part of any reviews."

Thick Whois IRT Legal Review

As noted above, the Thick Whois WG recommended a legal review on privacy issues as part of the implementation process (still underway) for the consensus policy on thick Whois that resulted from the WG's recommendations. That legal review, in which ICANN staff was assisted by expert outside counsel, is embodied in a June 2015 memorandum which concludes: "The analysis undertaken did not reveal any additional privacy issues not already considered by the Expert Working Group that would be implicated in the transition of data from a thin to a thick Whois model. To the extent that a contracted party finds that it is unable to comply with the Thick Whois policy requirements due to a conflict with its obligations under local privacy laws, such conflicts may be dealt with by exception through use of the Whois Conflicts Procedure, or requests to ICANN for an amendment to or waiver of certain provisions in the Registry Agreement or Registrar Accreditation Agreement." The memo also addresses the importance of consent of domain name registrants in satisfying data protection/privacy requirements, and concludes that "notwithstanding the concerns over the validity of consent and the ability of registrants to revoke consent, it is likely to be the most expedient way of addressing the transition to thick Whois." The memo also identifies "(i) privacy/proxy services, and perhaps (ii) thick Whois services where the data stays in the region subject to restrictions to avoid data transfer limitations" as other options (in addition to consent) for addressing data protection concerns regarding international transfer of data.

7. Correspondence: Article 29 WP on the data protection impact of the ICANN RAA (2013-2014)

https://www.icann.org/en/system/files/correspondence/namazi-to-kohnstamm-25mar14-en.pdf
https://www.icann.org/en/system/files/correspondence/kohnstamm-to-jeffrey-08jan14-en.pdf
https://www.icann.org/en/system/files/correspondence/jeffrey-to-kohnstamm-20sep13--en.pdf
https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-chehade-06jun13-en.pdf
Summarized by: Sheckler

- ***Letter from Jacob Kohnstamm, Article 29 Data Protection Working Party, to Messrs. Crocker and Chehade, ICANN, dated 6 June 2013***

The Working Party objected to a proposal for registrars to maintain certain personal data beyond a contract term, noting that in light of the diversity of registrars in terms of size and security measures, the benefits of maintain data for a lengthy period post-contract was disproportionate to risk for individuals and their rights to the protection of their personal data.

- ***Letter from John Jeffrey, ICANN to Jacob Kohnstamm, Article 29 Data Protection Working Party, dated 20 Sept. 2013***

ICANN noted that the 2013 RAA was supported by the GAC, that in its final form reduced the retention requirements from a prior proposal, created a dual-tiered system to data retention, and that there are legitimate reasons for maintaining data, such as for billing related matters, beyond law enforcement purposes. ICANN invited a discussion with the Working Party on a replacement whois system.

- ***Letter from Jacob Kohnstamm, Article 29 Data Protection Working Party, to John Jeffrey, ICANN, dated 8 January 2014***

The Working Party stated that the 2013 RAA did not address the concerns described in their 6 June 2013 letter, and regretted that ICANN did not acknowledge the Working Party correspondence as written guidance to support the waiver application of a registrar operating in Europe. The Working Party reiterated its concern that the 2013 RAA fails to specify a legitimate purpose which is compatible with the purpose for which the data was collected and for the retention of the data for the relevant periods.

- ***Letter from Cyrus Namazi, ICANN to Jacob Kohnstamm, Article 29 Data Protection Working Party, dated 25 March 2014***

ICANN noted that in its examination of various registrar waiver requests from the 2013 data retention requirements, it had learned that Member States of the EU may have differing interpretations of what is a “legitimate” purples in determining the length of time for which data may be lawfully retained. ICANN stated that it had started a public comment process to clarify the lawful and legitimate purposes for data collection and retention under the RAA, and was hopeful that this would help inform ICANN and find an acceptable resolution.

8. Correspondence: Article 29 WP on the data protection impact of the revision of the ICANN RAA concerning accuracy and data retention of WHOIS (2012)

https://www.icann.org/en/system/files/correspondence/kohnstamm-to-crocker-atallah-26sep12-en.pdf
https://www.icann.org/en/news/correspondence/chehade-to-kohnstamm-09oct12-en
Summarized by: Ali

The Working Party finds the proposed new requirement to annually re-verify both the telephone number and the e-mail address and publish these contact details in the publicly accessible WHOIS database excessive and therefore unlawful. Because ICANN is not addressing the root of the problem, the proposed solution is a disproportionate infringement of the right to protection of personal data.

9. Correspondence: Article 29 WP on ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2007)

http://gnso.icann.org/en/correspondence/cerf-to-schaar-24oct07.pdf
https://www.icann.org/en/system/files/files/cerf-to-schaar-15mar07-en.pdf
https://www.icann.org/en/correspondence/schaar-to-cerf-12mar07.pdf
Summarized by: Walsh

October 10, 2007, letter from ICANN Board to **Article 29 Working Party (A29WP)**

1) Subject: ICANN Procedure for Handling WHOIS Conflicts with Privacy Law

2) A29WP had submitted input for WHOIS draft procedures on handling conflicts with privacy laws

3) A29WP formally offers to review finalized text of the procedures

4) Makes the Working Party available for contact for further discussion on these topics especially related to EU and national data protection legislation

March 15, 2007, letter from ICANN Chairman of the Board to A29WP

1) Confirming receipt of A29WP and publication on the ICANN correspondence page.

2) A29WP commented on the following topics:

    a. "Draft Procedure for Handling Potential Conflicts between Whois Requirements and Privacy Laws"

        i. ICANN staff is to follow-up with A29WP should they need clarification on their concerns

    b. "Preliminary Task Force Report on Whois Services"

        i. Final task force was already concluded and submitted to GNSO Council, so A29WP concerns were brought to the Council as well

ii. GNSO will take up the next step on this issue

iii. ICANN welcomes A29WP comments on the "Final Task Force Report on Whois Service"

3) The A29WP supported the Operational Point of Contact proposal, which was recommended in the Final Report (by a narrow margin).

March 12, 2007, letter from A29WP to ICANN Board of Directors

1) Subject: Comments on the GNSO Whois Task Force Preliminary Task Force Report on Whois Services of 22 November 2006; and on the Draft ICANN Procedure for Handling Whois Conflicts with Privacy Law of 3 December 2006

2) Comments are in reference to:

   a. Impact on the EU Data Protection Directive (Directive 95/46/EC)

      i. Particularly the processing of personal data for domain name registration including making data available for WHOIS services

   b. Draft ICANN Procedure for Handling Whois Conflict with Privacy Law of 3 December 2006

3) Documents referenced:

   a. Opinion 2/2003 – on the application of the data protection principles in the WHOIS directories

   b. 22 June 2006 – letter to the Board of Directors detailing relevant data protection principles

   c. EU Data Protection Directive (article 2-d)

4) Noted privacy/data protection issues:

   a. **Legal and natural person differentiation**: there is a need to make a distinction between the two and a primary concern for those who are "private domain holders that use domains solely in a non-commercial context"

   b. **Direct access for bulk marketing**: "not in line with the purpose for which the directories were set up and are being maintained"

   c. **EU registrars conflicted position**: need to uphold EU data protection law and conflicts with the ICANN registrar accreditation agreement

      i. The main conflict: The accreditation agreement requires making registrant personal data available to third parties

ii. Registrars/registries are considered "data controllers" and therefore must "observe data protection rules set by the Data Protection Directive and national laws implementing it"

d. **Current and *actual* (not *potential*) conflicts** between WHOIS practice and EU data protection and privacy laws

e. Suggestions/ Comments

i. **Distinction between publicly accessible and inaccessible data (or tiered access)**: "Introducing a distinction between publicly accessible and publicly inaccessible data"

1. to address privacy and bulk marketing issues

ii. National privacy legislation is not negotiable

1. Re: ICANN wishes to negotiate with "local/national enforcement authority"

iii. **ICANN's current suggestions will not resolve the conflict** for registrars between ICANN accreditation and the EU Directive

iv. Solutions to the privacy/data protection issues "**should be solved through amendments to the registrar accreditation agreement**"

10. Correspondence: Article 29 WP on ICANN's WHOIS Database Policy (2006)

https://www.icann.org/en/system/files/files/schaar-to-cerf-22jun06-en.pdf
https://www.icann.org/en/correspondence/lawson-to-cerf-22jun06.pdf
https://www.icann.org/en/correspondence/parisse-to-icann-22jun06.pdf
https://www.icann.org/en/system/files/files/fingleton-to-cerf-20jun06-en.pdf
Summarized by: Folly

To sum up, all four documents are letters written to ICANN in order to make some remarks on WHOIS database policy and to advise ICANN on how best it can manage the database. All four documents constantly point out the real purpose of the WHOIS and what information should be collected, what you should be available to the public and what mechanisms need to be put in place to prevent spamming and or bulk information access.

11. Title: Article 29 WP 76 Opinion 2/2003 on the application of data protection principles to WHOIS directories

Summarized by: Walsh

1) Referenced documents or groups

a. ICANN Whois Task Force

b. International Working Group on Data Protection in Telecommunications

c. EU Data Protection Directive

    i. Article 6c

d. Opinion 5/2000 on The Use of Public Directories for the Reverse of Multi-criteria Searching services

2) Noted privacy/data protection issues & comments

a. There is "**improper use of the Whois data** in several countries"

    i. Proper use being – contacting a person technically responsible for another domain when there is a problem

b. DN **registration by private persons increases the importance** of the Whois discussion around privacy/data protection

c. Comments on data protection **apply to other domain name and IP address registries** including regional levels (i.e. RIPE and AP-NIC), not only Whois

d. The Data Protection Directive sets limits on data collection, which **data should be relevant and not excessive for the purpose**

    i. The meaning of "relevant and not excessive" may change **depending on who is registering** (private personal, legal person or companies)

e. Excessive data collection in the Whois database cannot be tolerated because some potential users consider it desirable

f. A29WP is **concerned about the searchability of the Whois and use as a Reverse Directory**, infringing privacy and data protection

g. Agrees in the need for **more accurate data** and limitation on access for bulk direct marketing

h. People should be able to register for DNs without personal details appearing in a "publicly available register"

3) Suggestions

a. It is "**essential to determine…the purpose of the Whois**" to avoid **extending its purposes in a way that creates data protection issues**

b. **Data minimization** – The amount and type of personal data collected and processes should be limited specifically to the purpose

c. **The right to object** provides individuals (private persons or those related to a company) the right to abstain from disclosing personal information

d. **Proportionality principle** – in line with this principle, Whois **directories should not have "all data directly available on-line to everybody",** and should look for "less intrusive methods" that would allow the Whois to serve its purpose

   i. The Principle: The content and form of the action must be in keeping with the aim pursued

   ii. Encourages researching **"privacy enhancing ways to run the Whois directories"** to protect the rights of individuals

12. Additional Article 29 WP Documents

Article 29 WP 5 Recommendation 2/97
Article 29 WP 33 Opinion 5/2000
Article 29 WP 41 Opinion 4/2001
Article 29 WP 56 Working Document 5/2002
Summarized by: Sheckler (p1)

- ***Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Recommendation 2/97, Report and Guidance by the International Working Group on Data Protection in Telecommunications ("Budapest – Berlin Memorandum on Data Protection and Privacy on the Internet") Adopted 3 Dec. 1997, available at Article 29 WP 5 Recommendation 2/97***

The Working Party found that the "Budapest – Berlin Memorandum on Data Protection and Privacy on the Internet" might contribute to the improvement of the protection of fundamental rights of individual, in particular their privacy, on a worldwide basis.

- ***Article 29 Data Protection Working Party, Opinion 5/2000 on the Use of Public Directories for Review of Multi-Criteria Searching Services (Reverse Directories) Adopted 13 July 2000, available at Article 29 WP 33 Opinion 5/2000***

Reverse or multi-criteria searches of public directories are lawful if the following conditions are met:

(i) subscriber provides specific and informed consent prior of the inclusion of his data in all kinds of public directories (telephony, email, etc.) used for reserve or multi-channel services;

(ii) the controller informs the subscriber in particular about the use of personal data in alphabetical directories, whether his personal data are planned to be used in reverse or multi-channel services and to what extent, his right to modify his decision to allow each specific data processing; and

(iii) the controller has implemented technical and organizational measures appropriate to the risks represented by the processing and the nature of the data protected (i.e. protect against fraudulent use).

- ***Article 29 Data Protection Working Party, Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime, Adopted 22 March, 2001, available at Article 29 WP 41 Opinion 4/2001***

The Working Party recommended that the Council of Europe, in promoting international cooperation in matters of cybercrime outside of its own membership, should pay attention to the protection of fundamental rights and freedoms, especially the right to privacy and personal data protection. It offered various specific recommendations to the draft convention noted above.

- ***Article 29 – Data Protection Working Party, Working Document on Determining the International Applications of EU Data Protection Law to Personal Data Processing on the Internet by non-EU based Web Sites, Adopted 30 May 2002, available at Article 29 WP 56 Working Document 5/2002***

The purpose of this document was to discuss international application of EU data protection laws to the processing, particularly collection, of personal data by non-EU based web sites. The Working Party opined that:

1. a high level of protection for individuals can only be ensure if web sites established outside of the EU but using equipment in the EU respect the guarantees of personal data processing and the rights of individuals recognized at the EU level and applicable to all websites established in the EU.

2. A program for the promotion of European data protection rules in a pragmatic way would help controllers in third countries better understand, implement and demonstrate privacy compliance.

13. Title: Article 29 WP 217 Opinion 4/2014
Summarized by: Perrin
To be provided

14. Title: Article 29 WP Opinion 1/2010
Summarized by: Perrin

Summary of Article 29 Data Protection Working Party Opinion 01/2010 on concepts of "controller" and "processor" 00264/10/EN WP 169 adopted Feb., 2010

This Opinion from the Article 29 group summarizes the interpretation of the concept of "data controller" and "data processor", which are key concepts in the Directive 95/46/EC and therefore present in all national data protection laws in the EU. The data controller was introduced as a concept in the Convention 108 (1981) but when the Directive appeared in 1991, finalized in 1995, the concept was broadened to allow for the existence of joint control, and the new concept of a data processor operating under instructions from the data controller. This takes into account the reality of modern ICTs, the existence of multiple organizations performing specific functions in the data processing life cycle, and plays an important role in allocating responsibility under the Directive.

Briefly, the determination of who the data controller is rests on the following issues taken from the definition in the Directive:

- "the natural or legal person, public authority or any other body"
- "which alone or jointly with others"
- "determines the purposes and means of the processing of personal data".

Concrete factual analysis is required in order to determine who actually determines the requirements surrounding the data processing. Whether the data processing is lawful or not is not relevant to the determination of who the controller is. A "processor" means "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller". Since the Directive provides for different accountabilities and responsibilities for the different roles, distinguishing which role an actor is playing is important. It is also important in determining which national law applies; for instance with respect to security measures for processing, it is the state wherein the data processor resides.

The opinion is helpful in interpreting the various letters and opinions which ICANN has received from the European Data Protection Authorities, as the responsibilities of data controllers and processors are implicit in those documents, not necessarily spelled out in detail.

15. **Title:** Article 29 WP 20 Opinion 3/1999

Summarized by: Ali

Relevant Sections Contained Within Referenced "Opinion No 3/99 on Public sector information and the protection of personal data" by the Working Party on the protection of individuals with regard to the processing of personal data.

One of the key aspects of this opinion is the availability of public sector information. At issue is a specific category of information held by public sector bodies known as "public" information, which would be made public subject to certain rules or for a particular purpose and based, implicitly or explicitly, on the State's desire for transparency with regard to its citizens.

The objective of this Opinion is to provide input for the discussion on the protection of personal data, a dimension which must be taken into consideration when undertaking to grant greater access to public sector data, where such data relates to individuals.

THE RULES ON DATA PROTECTION APPLY TO PERSONAL DATA WHICH HAVE BEEN MADE PUBLIC
Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data covers the principle of the right of public access to administrative documents and other factors which are relevant to the discussion The principle of purpose requires that personal data are collected for specific, explicit and legitimate purposes and are not subsequently processed in a manner which is incompatible with these purposes.

Personal data to be made public do not constitute a homogeneous category which can be dealt with uniformly from a data protection point of view. Instead, a step-by-step analysis is needed of the rights of the data subject and the right of the public to access the data respectively. While there may be public access to data, such access may be subject to certain conditions (such as proof of legitimate interest). Alternatively, the purposes for which the data may be used, for example for commercial purposes or by the media, may be restricted.

At this point it is worth mentioning that regardless of whether or not personal data are published, data subjects always has the right to access their data and, where necessary, to require that they be rectified or erased if they have not been processed in accordance with the Directive, and in particular if they are incomplete or inaccurate.

THE NEW TECHNOLOGIES CAN HELP STRIKE A BALANCE BETWEEN THE PROTECTION OF PERSONAL DATA AND THE PUBLICATION OF SUCH DATA
In addition to promoting access to public data, in particular by providing on-line access, the new technologies and some of the accompanying administrative measures can also help to ensure compliance with the main principles of data protection, such as end purpose, the principle of information, the right to object and the principle of security. However, these technologies do not provide an absolute guarantee against abuses of the principles of personal data protection described above.

Directive 95/46/EC recognises the right of data subjects to be informed about the processing of data concerning them and stipulates that at the very least they have the right to object to legitimate processing. Data subjects must therefore be informed about the commercial usage of data concerning them and must be able to object to such usage by simple and effective means.

Another possibility mentioned in the opinion was to obtain the data subject's consent for commercial usage. Data subjects must have given their consent unambiguously and in full knowledge of the facts, taking into account the fact that anyone applying for planning permission is required to submit a file which meets certain stipulations.

CONCLUSION:
Public access to data does not mean unfettered access: all Member States base their legislation on this philosophy. When personal data are made public, either by virtue of a regulation or because the data

subject himself authorises it, the data subject is not deprived of protection, ipso facto and forever. He is guaranteed such protection by law in accordance with the fundamental principles of the right to privacy.

In order to strike a balance between the right to privacy and the protection of personal data on the one hand, and the right of the general public to access public sector data on the other, conclusions must take account of the following factors and issues:

- a case-by-case assessment of whether personal data can be published/should be accessible or not, and if so, under what conditions and on which media (computerised or not, Internet dissemination or not, etc.);
- the principles of purpose and legitimacy;
- the obligation to inform the data subject;
- the data subject's right to object;
- the use of the new technologies to help protect the right to privacy.

These factors should be taken into account not just in situations where publication or access is already regulated, but also in situations where regulation does not appear necessary, with a view to satisfying the general public's demand for access to public sector information, including personal data.

16. Title: Council of Europe Declaration of the Committee of Ministers on ICANN, human rights and the rule of law (3 June 2015)

Summarized by: Sheckler

Among other things, this declaration states that:

- The Internet should be managed in the public interest.
- Member states have a primary legal and political obligation to protect human rights as enshrined in the European Convention on Human Rights (ETS No. 5).
- Member states have the obligation to protect society and individuals against crime and to uphold the rule of law on the Internet.
- ICANN should respect international human rights law. ICANN should ensure, when defining access and use of new gTLDs, that an appropriate balance is struck between economic interests and other objectives of common interest.

Member states, through their GAC representatives, play an important role in ensuring that ICANN's technical decisions take full account of international law and other public policy objectives. They should continue to engage with ICANN to ensure it assumes responsibility for respecting internationally recognized human rights laws and standards.

17. Title: Council of Europe's Treaty 108 on Data Protection

Summarized by: Kleiman

Council of Europe's Treaty 108 on Data Protections
(Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data)

Adopted: January 28, 1981

Signatories: Albania, Andorra, Armenia, Austria , Azerbaijan , Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, Ukraine, Uruguay and United Kingdom **(48 signatories from Western Europe, Eastern Europe and around the world).**

Synopsis (taken from the Council of Europe's webpage):
Council of Europe's Treaty 108 on Data Protections – Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data
This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data.

In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.

Restriction on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake.

The Convention also imposes some restrictions on transborder flows of personal data to States where legal regulation does not provide equivalent protection.

Summary of Articles of Treaty Particularly relevant to WG's Evaluation:
"Article 1 – Object and purpose
The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."

"Article 5 –Quality of data
Personal data undergoing automatic processing shall be:
a. obtained and processed fairly and lawfully;
b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

"Article 6 – Special categories of data
Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."

Scope
"Article 12 – Transborder flows of personal data and domestic law
1 The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed."

"Article 14 – Assistance to data subjects resident abroad
1 Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention."

Additional information:
This WG includes members of the Council of Europe, so I welcome their input, expertise and guidance on this treaty.

18. Title: Opinion of the European Data Protection Supervisor: Europe's role in shaping the future of Internet Governance (23 June 2014)

Summarized by: Ferdeline

This document calls for all Internet policy discussions to take into consideration the internationally-recognised, fundamental rights of privacy and data protection.

- Such rights are: 1) at the basis of users' online interactions, 2) should be protected online as well as offline, and 3) "are not negotiable".
- The current WHOIS system is named as "an example of a data protection issue which has to be addressed" because of its "authentication and data retention requirements." It must be replaced "with a solution taking account, inter alia, of privacy concerns."
- Data protection authorities must be represented in multi-stakeholder Internet governance processes and must ensure that respect for fundamental rights are assured for all users regardless of their means and capabilities. They should also work to ensure the harmonisation of data protection rules at a global level.
- Data controllers have a responsibility to: provide transparent and easily accessible and understandable information, should provide procedures and mechanisms for exercising a data subject's rights, must provide information on storage periods, must provide information on rights to lodge a complaint, and must provide information in relation to the international transfer of data and to the source from which the data is originating.
- Users have the right to be forgotten and to erasure. In balancing the right to erasure against the freedom of information, the former overrides the general public's right to be informed, unless the data subject plays a role in public life that justifies interference with his/her right to privacy.

- There is a close relationship between technological design and data protection. The principles of data protection-by-design and by-default could serve as significant enablers of trust on the Internet. Accordingly the inclusion of optimal data protection standards in the development of technology at the early design phase is encouraged.
- Conflicts of law arise in connection with the Internet, jeopardising users' rights to privacy and data protection, and these need to be solved. "Given the global and cross-border nature of the Internet, personal data is often transferred to and processed in jurisdictions other than those in which users have submitted their data, exposing them to the risk of lower or no data protection. In addition, controllers processing personal data on the Internet may be faced with conflicting laws and obligations and must choose between violating foreign obligations or EU data protection safeguards … which in consequence undermines the data protection safeguards afforded to users under EU law."
- Google v AEPD might provide some guidance on answering this question – in this judgement the Court of Justice of the European Union ruled that the presence of an establishment on the territory of an EU Member State and the relationship between the activities of that establishment and the data processing at issue can be used to decide the applicability of EU data protection law to a processing carried out online.
- "From a European perspective, we would encourage controllers processing the personal data of EU individuals on the Internet to increase the transparency and the amount of information they provide to users in relation to the law(s) they are subject to and the data protection rules they are bound to apply, including laws on access to data by government bodies, jurisdictions where data may be processed, and what safeguards have been implemented to protect users' data."

19. Title: ICANN's public consultation on 2013 RAA Data Retention Specification Data Elements and - Legitimate Purposes for Collection and Retention (17 April 2014)

Summarized by: Ferdeline

This document is a letter from the European Data Protection Supervisor to ICANN in response to its 2013 public consultation on the RAA Data Retention Specification Data Elements and Potentially Legitimate Purposes for Collection/Retention (' the draft Specification '). It states that:

- The draft Specification "falls short of compliance with European data protection law."
- "The draft Specification should only require collection of personal data which is genuinely necessary for the performance of the contract between the Registrar and the Registrant (e.g. billing) or for other compatible purposes such as fighting fraud related to domain name registration. This data should be retained for no longer than is necessary for these purposes. It would not be acceptable for the data to be retained for longer periods or for other, incompatible purposes, such as law enforcement purposes or to enforce copyright."

- The "retention of personal data originally collected for commercial purposes, and subsequently retained for law enforcement purposes … [is] invalid."
- ICANN is encouraged "to take a lead in ensuring that privacy and data protection are embedded by default, when new tools and instruments or new Internet policies are designed, for the benefit of all – not just European – Internet users."

20. Title: European Commission Website: Obligations of Data Controllers

Summarized by: Kleiman

Summary: The European Commission created a readable guide to the requirements of the EU Data Protection Law. For the purposes of the summary below, 3 interlinked pages of this guide have been used:

- Protection of Personal Data, http://ec.europa.eu/justice/data-protection/index_en.htm
- Who can Collect and Process Personal Data?, http://ec.europa.eu/justice/data-protection/data-collection/index_en.htm
- Obligations of Data Controllers, http://ec.europa.eu/justice/data-protection/data-collection/obligations/index_en.htm

Synopsis of Key Input

The material include a definition of "data controllers," specific obligations they undertake and specific rights of data subjects. The material below is largely direct quotes from the larger set of materials.

Definition of "Data controllers" – the persons or entities which collect and process personal data as "data controllers". Data controllers determine 'the purposes and the means of the processing of personal data'. This applies to both public and private sectors. Data controllers must respect the privacy and data protection rights of those whose personal data is entrusted to them.

Specific Obligations of the Data Controllers –

"Each data controller must respect the following rules as set out in the Directive:

- Personal Data must be processed legally and fairly;
- It must be **collected for explicit and legitimate purposes** and used accordingly;
- It must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;
- It must be **accurate**, and updated where necessary;
- Data controllers must ensure that data subjects can rectify, remove or block incorrect data about themselves;

- Data that identifies individuals (personal data) must not be kept any longer than strictly necessary;
- **Data controllers must protect personal data** against accidental or unlawful destruction, loss, alteration and disclosure, particularly when processing involves data transmission over networks. They shall implement the appropriate security measures;
- These protection measures must ensure a level of protection appropriate to the data."

Specific Rights of Data Subjects –
"If a data subject is of the view that his/her data has been compromised, he/she can send a complaint to the data controller. If the data controller's handling of a complaint is not satisfactory, the data subject can file a complaint to the national supervisory data protection authority."

Additional Information:
I defer to our European peers who are experts on the European Data Protection Directive to edit, add and further guide our understanding of this material.

21. Title: Draft Directive of the European Parliament (April 2016)

News: Data protection reform – Parliament approves new rules fit for the digital era
Draft Directive of the European Parliament (April 2016)

Summarized by: Samuels

So the updated EU data protection and privacy regulations are now agreed.
Some rules include: "…….

- a right to be forgotten,
- "clear and affirmative consent" to the processing of private data by the person concerned,
- a right to transfer your data to another service provider,
- the right to know when your data has been hacked,
- ensuring that privacy policies are explained in clear and understandable language, and
- stronger enforcement and fines up to 4% of firms' total worldwide annual turnover, as a deterrent to breaking the rules

- ……."

22. European Commission EU-US Privacy Shield related documents

European Commission News Announcement: EU-US Privacy Shield
Judgment of the Court (Grand Chamber) - Maximillian Schrems v Data Protection Commissioner
EU-U.S. Privacy Shield draft (full text, February 2016)
Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision of the Article 29 WP 238

Summarized by: Kleiman and Kimpian

Privacy Team Summaries - drafted by gnso-rds-pdp-privacy@icann.org

Announcement of Council of Europe summarizing the newly-adopted EU-US Privacy Shield for transborder data flows across the Atlantic from EU to US (submitted by Kleiman)

Original text of this timely, short announcement:
"The European Commission today issued a Communication summarising the actions taken to restore trust in transatlantic data flows since the 2013 surveillance revelations.

The European Commission has finalised the reform of EU Data protection rules, which apply to all companies providing services on the EU market. The Commission negotiated the EU-U.S. Umbrella Agreement ensuring high data protection standards for data transfers across the Atlantic for law enforcement purposes. The Commission achieved a renewed sound framework for commercial data exchange: the EU-U.S. Privacy Shield.

Today, the Commission also published a draft "adequacy decision" as well as the texts that will constitute the EU-U.S. Privacy Shield. This includes the Privacy Shield Principles companies have to abide by. Moreover, the Commission makes public the U.S. Government's written commitments on the enforcement of the arrangement.

The written commitments will be published in the U.S. Federal Register and include assurance on the safeguards and limitations concerning public authorities' access to data."

Summary of Schrems decision, Privacy Shield, the opinion of the WP29 on the EU-US Privacy shield draft adequacy decision and their relevance to ICANN activities (submitted by Kimpian)

Schrems decision

Background
The revelations made by Edward Snowden in June 2013 triggered a debate on the scope of surveillance activities performed by intelligence services, both in the United States and in the European Union. In particular, this debate focussed on the consequences of an "indiscriminate surveillance and …interception carried out…on a large-scale surveillance" for citizens' rights to respect of their privacy and to the protection of their personal data.

The Article 29 Working Party (WP29) has consistently stated that such surveillance is incompatible with the EU legal framework and that existing transfer tools are not the solution to this issue. Furthermore, in order not to reduce the protection granted, the fundamental right to personal data needs to be protected during the entire life cycle of the data. This includes when data is exchanged internationally. Therefore, the WP29 always considered that transfers to third countries will not be considered as safe, where the powers of state authorities to access information go beyond what is necessary in a democratic society.

On 6 October 2015, the Court of Justice of the European Union (CJEU) issued its preliminary ruling requested by the Irish High Court in proceedings between Mr Schrems and the Irish Data Protection Commissioner concerning the latter's refusal to investigate a complaint made by Mr Schrems relating to the interpretation, in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the

European Union, of Articles 25(6) and 28 of Directive 95/46/EC of 24 October 1995, and, in essence, to the validity of Commission Decision 2000/520/EC of 26 July 2000.

The CJEU declared the Safe Harbour decision invalid. According to this judgment, the Safe Harbour decision does not contain sufficient findings regarding the measures by which the United States ensure an adequate level of protection for the protection of private life and basic freedoms and rights of individuals, within the meaning of Article 25(6) of that Directive, by reason of its domestic law or its international commitments.

The CJEU identified various criteria that must be met in order to consider that a third country is adequate, especially in terms of effective legal protection against interference with EU fundamental rights, oversight and right of redress. In particular, it insisted on the scope of the derogations to EU fundamental rights and specified the necessity to limit such interference. The Court strongly reiterated the specificities of the data protection regime within the European Union. Similarly to previous recent decisions (e.g. Digital Rights Ireland case, Data Retention case), it has put the European Charter at the centre of its reasoning on international transfers

The Court ruling

The CJEU first of all answered the question which the Irish court had asked about DPA jurisdiction over data transfers (the procedural point), and then went on to rule that the Safe Harbour decision is invalid (the substantive point).

Following the Advocate-General's view, the Court ruled that national data protection authorities have to be able to consider claims that flows of personal data to third countries are not compatible with EU data protection laws if there is an inadequate level of data protection in those countries, even if the Commission has adopted a decision (such as the Safe Harbour decision) declaring that the level of protection is adequate. Like the Advocate-General, the Court based its conclusion on the powers and independence of those authorities, read in light of the EU Charter of Fundamental Rights, which expressly refers to DPAs' role and independence.

The Court admitted that the Directive is not clear on defining the 'adequate level of protection', so it had to interpret the rules. In the Court's view, there must be a 'high' level of protection in the third country; this does not have to be 'identical' to the EU standard, but must be 'substantially equivalent' to it. Otherwise, the objective of ensuring a high level of protection would not be met, and the EU's internal standards for domestic data protection could easily be circumvented. Also, the means used in the third State to ensure data protection rights must be 'effective…in practice', although they 'may differ' from that in the EU. Furthermore, the assessment of adequacy must be dynamic, with regular automatic reviews and an obligation for a further review if evidence suggests that there are 'doubts' on this score; and the general changes in circumstances since the decision was adopted must be taken into account.

Firstly the Court stated that within the EU, interference with privacy and data protection rights requires 'clear and precise rules' which set out minimum safeguards, as well as strict application of derogations and limitations. Those principles were breached where, 'on a generalised basis', legislation authorises 'storage of all the personal data of all the persons whose data has been transferred' to the US 'without any differentiation, limitation or exception being made in light of the objective pursued' and without

any objective test limiting access of the public authorities for specific purposes. General access to the content of communications compromises the 'essence' of the right to privacy. On these points, the Court expressly reiterated the limits on mass surveillance set out in last year's Digital Rights judgment (discussed here) on the validity of the EU's data retention Directive. Furthermore, the absence of legal remedies in this regard compromises the essence of the right to judicial protection set out in the EU Charter.

Secondly, the restriction upon DPAs taking action to prevent data transfers in the event of an inadequate level of data protection in the USA (in the context of Safe Harbour) was also invalid. The Commission did not have the power under the data protection Directive (read in light of the Charter) to restrict DPA competence in that way. Since these two provisions were inseparable from the rest of the Safe Harbour decision, the entire Decision is invalid.

Privacy Shield and opinion of WP29 on the EU – U.S. Privacy Shield draft adequacy decision

EU-US Privacy Shield

After two years of negotiations, the European Commission and the U.S. Department of Commerce reached on 2 February 2016 a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield. This new framework is to protect the fundamental rights of Europeans where their data is transferred to the United States and to ensure legal certainty for businesses.

The EU-U.S. Privacy Shield reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbour framework invalid.

The new arrangement due to provide stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities. The new arrangement includes written commitments and assurance by the U.S. that any access by public authorities to personal data transferred under the new arrangement on national security grounds will be subject to clear conditions, limitations and oversight, preventing generalised access. The newly created Ombudsperson mechanism will handle and solve complaints or enquiries raised by EU individuals in this context.

The EU-U.S. Privacy Shield addresses both the recommendations made by the Commission in November 2013 and the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbour framework invalid.

The new arrangement provides stronger obligations on companies in the U.S. to protect the personal data of Europeans. It requires stronger monitoring and enforcement by the U.S. Department of Commerce (DoC) and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities.

The new arrangement includes commitments and assurance by the US that the competencies under US law for public authorities to access personal data transferred under the new arrangement will be subject to clear conditions, limitations and oversight, preventing generalised access. The newly created

Ombudsperson mechanism will handle and solve complaints or enquiries raised by EU individuals in relation to possible access by national intelligence services.

The new agreement includes:

- Strong obligations on companies and robust enforcement: the new arrangement is designed to be more transparent and to contain effective supervision mechanisms to ensure that companies respect their obligations, including sanctions or exclusion if they do not comply. The new rules also include tightened conditions for onward transfers to other partners by the companies participating in the scheme.

- Clear safeguards and transparency obligations on U.S. government access: for the first time, the U.S. government has given the EU written assurance from the Office of the Director of National Intelligence that any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms. US Secretary of State John Kerry committed to establishing a redress possibility in the area of national intelligence for Europeans through an Ombudsman mechanism within the Department of State, who will be independent from national security services. The Ombudsman will follow-up complaints and enquiries by individuals and inform them whether the relevant laws have been complied with. All the written commitments will be published in the U.S. federal register.

- Effective protection of EU citizens' rights with several redress possibilities: Complaints have to be resolved by companies within 45 days. A free of charge Alternative Dispute Resolution solution will be available. EU citizens can also go to their national Data Protection Authorities, who will work with the U.S. Department of Commerce and Federal Trade Commission to ensure that unresolved complaints by EU citizens are investigated and resolved. If a case is not resolved by any of the other means, as a last resort there will be an enforceable arbitration mechanism. Moreover, companies can commit to comply with advice from European DPAs. This is obligatory for companies handling human resource data.

- Annual joint review mechanism: that will monitor the functioning of the Privacy Shield, including the commitments and assurance as regards access to data for law enforcement and national security purposes. The European Commission and the U.S. Department of Commerce will conduct the review and associate national intelligence experts from the U.S. and European Data Protection Authorities. The Commission will draw on all other sources of information available, including transparency reports by companies on the extent of government access requests. The Commission will also hold an annual privacy summit with interested NGOs and stakeholders to discuss broader developments in the area of U.S. privacy law and their impact on Europeans. On the basis of the annual review, the Commission will issue a public report to the European Parliament and the Council.

Art 29 opinion on the EU – U.S. Privacy Shield draft adequacy decision

Background

On 29 February 2016, the European Commission published a Communication, a draft adequacy decision and the annexed texts constituting a new framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield (hereinafter: Privacy Shield), which seeks to replace the

previous U.S. Safe Harbour invalidated by the Court of Justice of the European Union (hereinafter: CJEU) on 6 October 2015, in the Schrems case.

In accordance with Article 30(1)(c) of Directive 95/46/EC, the Article 29 Working Party (WP29) assessed these documents in order to give its opinion on the draft adequacy decision. The WP29 assessed both the commercial aspects and the possible derogations to the principles of the Privacy Shield for national security, law enforcement and public interests purposes.

The WP29 took into account the applicable EU data protection legal framework as set out in Directive 95/46/EC, as well as the fundamental rights to private life and data protection as encoded in Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental rights of the European Union. It also considered the Right to an effective remedy and to a fair trial laid down in Article 47 of the Charter, as well as the jurisprudence related to the various fundamental rights.

In addition, the analysis reflects the reasoning of the CJEU in the Schrems case regarding the Commission's margin of appreciation of an adequacy assessment. The check and controls of the adequacy requirements must be strictly performed, taking into account the fundamental rights to privacy and data protection and the number of individuals potentially affected by transfers.

The Privacy Shield needs to be viewed in the current international context, such as the emergence of big data and the growing security needs. The scope and range of collection and use of personal data has dramatically increased since the original Safe Harbour decision was issued in 2000. European data protection authorities strongly assert the importance of the principles they defend.

The WP29 first of all welcomes the significant improvements brought by the Privacy Shield compared to the Safe Harbour decision. It notes that many of the shortcomings of the Safe Harbour it had underlined in its letter of 10 April 2014 to Vice-President Reding have been addressed by the negotiators.

The fact that the principles and guarantees afforded by the Privacy Shield are set out in both the adequacy decision and in its annexes makes the information both difficult to find, and at times, inconsistent. This contributes to an overall lack of clarity regarding the new framework as well as making accessibility for data subjects, organisations, and data protection authorities more difficult. Similarly, the language used lacks clarity. The WP29 therefore urges the Commission to make this clear and understandable for both sides of the Atlantic.

With regard to the applicable law, the WP29 highlights that if the Privacy Shield adequacy decision is adopted on the basis of Directive 95/46/EC, it needs to be consistent with the EU data protection legal framework, both in scope and terminology. The WP29 considers a review must be undertaken shortly after the entry into application of the General Data Protection Regulation, in order to ensure the higher level of data protection offered by the Regulation is followed in the adequacy decision and its annexes.

<u>On the commercial aspects of the Privacy Shield</u>
The WP29's key objective is to make sure that an essentially equivalent level of protection afforded to individuals is maintained when personal data is processed subject to the provisions of the Privacy Shield. Although the WP29 does not expect the Privacy Shield to be a mere and exhaustive copy of the EU legal

framework it considers that it should contain the substance of the fundamental principles and as a result, ensure an 'essentially equivalent' level of protection.

Notwithstanding the improvements offered by the Privacy Shield, the WP29 considers that some key data protection principles as outlined in European law are not reflected in the draft adequacy decision and the annexes, or have been inadequately substituted by alternative notions.

For instance, the data retention principle is not expressly mentioned and cannot be clearly construed from the current wording of the Data Integrity and Purpose Limitation principle. Furthermore, there is no wording on the protection that should be afforded against automated individual decisions based solely on automated processing. The application of the purpose limitation principle to the data processing is also unclear. In order to bring more clarity in the use of several important notions, the WP29 suggests that clear definitions should be agreed between the EU and the U.S and be part of a glossary of terms to be included in the Privacy Shield F.A.Q.

Because the Privacy Shield will also be used to transfer data outside the US, the WP29 insists that onward transfers from a Privacy Shield entity to third country recipients should provide the same level of protection on all aspects of the Shield (including national security) and should not lead to lower or circumvent EU data protection principles. In case an onward transfer to a third country is envisaged under the Privacy Shield, every Privacy Shield organisation should have the obligation to assess any mandatory requirements of the third country's national legislation applicable to the data importer, prior to the transfer. In general, the WP29 concludes that onward transfers of EU personal data are insufficiently framed, especially regarding their scope, the limitation of their purpose and the guarantees applying to transfers to Agents.

Finally, although the WP29 notes the additional recourses made available to individuals to exercise their rights, it is concerned that the new redress mechanism in practice may prove to be too complex, difficult to use for EU individuals and therefore ineffective. Further clarification of the various recourse procedures is therefore needed; in particular, where they are willing, EU data protection authorities could be considered as a natural contact point for the EU individuals in the various procedures, having the option to act on their behalf.

<u>Derogations for national security purposes</u>
Interferences with the right to privacy and data protection can be justified since these fundamental rights are not absolute: interferences must be only unjustified to interferences will be considered as unlawful. Following the assessment of the jurisprudence, the WP29 comes to the conclusion that the requirements can be summarised in four European Essential Guarantees:

- Processing should be based on clear, precise and accessible rules
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
- An independent oversight mechanism should exist
- Effective remedies need to be available to the individual

The WP29 however notes that the representations of the U.S. Office of the Director of National Intelligence (ODNI) do not exclude massive and indiscriminate collection of personal data originating

from the EU. The WP29 recalls its long-standing position that massive and indiscriminate surveillance of individuals can never be considered as proportionate and strictly necessary in a democratic society, as is required under the protection offered by the applicable fundamental rights. Additionally, comprehensive oversight of all surveillance programmes is crucial. The WP29 takes note that there is a tendency to collect ever more data on a massive and indiscriminate scale in the light of the fight against terrorism. Given the concerns this brings for the protection of the fundamental rights to privacy and data protection, the WP29 looks to the forthcoming rulings of the CJEU in cases regarding massive and indiscriminate data collection.

Concerning redress, the WP29 welcomes the establishment of an Ombudsperson as a new redress mechanism. This may constitute a significant improvement for EU individuals' rights with regards to U.S. intelligence activities. However, the WP29 is concerned that this new institution is not sufficiently independent and is not vested with adequate powers to effectively exercise its duty and does not guarantee a satisfactory remedy in case of disagreement.

The annual joint review mechanism mentioned in the draft adequacy decision is a key factor to the overall credibility of the Privacy Shield and the WP29 greatly welcomes the opportunity this would present to review the adequacy decision. In this regard, the WP29 understands that national representatives of the WP29 will be able to take full part in the review process but asks for clarification of the exact arrangements.

Overall conclusion

The WP29 states that three major points of concern do remain, that will need to be addressed.

- The first concern is the lack of explicit provisions for data retention. This is an essential element of EU data protection law to ensure that data is kept for no longer than necessary to achieve the purpose for which the data were collected.

- Secondly, the WP29 understands from Annex VI that the U.S. administration does not fully exclude the continued collection of massive and indiscriminate data. The WP29 has consistently held that such data collection, is an unjustified interference with the fundamental rights of individuals.

- The third point of concern regards the introduction of the Ombudsperson mechanism. Even though the WP29 welcomes this unprecedented step creating an additional redress and oversight mechanism for individuals, concerns remain as to whether the Ombudsperson has sufficient powers to function effectively. As a minimum, both the powers and the position of the Ombudsperson need to be clarified in order to demonstrate that the role is truly independent and can offer an effective remedy to non-compliant data processing.

The WP29 notes the major improvements the Privacy Shield offers compared to the invalidated Safe Harbour decision. Given the concerns expressed and the clarifications asked, the WP29 urges the Commission to resolve these concerns, identify appropriate solutions and provide the requested clarifications in order to improve the draft adequacy decision and ensure the protection offered by the Privacy Shield is indeed essentially equivalent to that of the EU.

Relevance to ICANN and on the new RDS

The privacy and data protection principles as demonstrated above and interpreted by the CJEU and Art29 are to be followed and respected whenever data controller is processing data coming from EU, which doesn't necessarily mean that only registrars, registries which are based in they EU has to comply with them but every one having EU data processed. Furthermore US companies subscribing to Privacy Shield also have to comply with US governments' commitment which include "strong obligations on companies and robust enforcement" at the first place.

Therefore the current policy regulating ICANN's data processing activities, especially under the RDS seems not to grant sufficient efficiency neither for registries or registrars nor for registrants. The maintenance of the current system of attribution of waivers in individual cases in order to meet national or regional legal requirements for the respect of privacy and data protection or at least avoiding conflict with them seems to become in the future extremely burdensome and outdated. It is to be considered how the best the above explained principles can be integrated in ICANN's policies in order to have a privacy friendly model which can be used worldwide.

Several areas can be identified as of interest where particular attention is to be paid to the above detailed principles:

- defining the purpose of data processing and application of limitation principle
- data collection for LEA, national security access
- data retention policy
- data transfers, onward transfers
- automated data processing
- effective remedies granted to data subjects

Sources are provided in the section heading above.

23. Title: European Data Protection Directive, 1995

Summarized by: Kleiman

Full Document Title: **European Parliament and Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data**

Document Link: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046
Summary Link: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012
Year Issued: 1995

Signatories: The member states of the European Union at the time and those who entered the EU later: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK **(28 countries)**

Summary:
"This Directive applies to data processed by automated means (e.g. a computer database of customers) and data contained in or intended to be part of non automated filing systems (traditional paper files). It does not apply to the processing of data:

- by a natural person in the course of purely personal or household activities;
- in the course of an activity which falls outside the scope of Community law, such as operations concerning public security, defence or State security.

The Directive aims to protect the rights and freedoms of persons with respect to the processing of personal data by laying down the key criteria for making processing lawful and the principles of data quality.

Data processing is only lawful if

- the data subject has unambiguously given his consent; or
- processing is necessary for the performance of a contract to which the data subject is party; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party; or
- processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection.

The principles of data quality, which must be implemented for all lawful data processing activities, are the following:

- personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes. They must also be adequate, relevant and not excessive, accurate and, where necessary, kept up to date, must not be stored for longer than necessary and solely for the purposes for which they were collected;
- special categories of processing: it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. This provision comes with certain qualifications concerning, for example, cases where processing is necessary to protect the vital interests of the data subject or for the purposes of preventive medicine and medical diagnosis.

The person whose data are processed, the data subject, can exercise the following rights:

- right to obtain information: the controller must provide the data subject from whom data are collected with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data etc.);
- the data subject's right of access to data: every data subject should have the right to obtain from the controller;
- the right to object to the processing of data: the data subject should have the right to object, on legitimate grounds, to the processing of data relating to him/her. He/she should also have the right to object, on request and free of charge, to the processing of personal data that the controller anticipates being processed for the purposes of direct marketing. He/she should

finally be informed before personal data are disclosed to third parties for the purposes of direct marketing, and be expressly offered the right to object to such disclosures;

Other relevant aspects for data processing:

- exemptions and restrictions from data subject's rights: the scope of the principles relating to the quality of the data, information to be given to the data subject, right of access and the publicising of processing may be restricted in order to safeguard aspects such as national security, defence, public security, the prosecution of criminal offences, an important economic or financial interest of a Member State or of the European Union or the protection of the data subject;
- the confidentiality and security of processing: any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller. In addition, the controller must implement appropriate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access;
- the notification of processing to a supervisory authority: the controller must notify the national supervisory authority before carrying out any processing operation. Prior checks to determine specific risks to the rights and freedoms of data subjects are to be carried out by the supervisory authority following receipt of the notification. Measures are to be taken to ensure that processing operations are publicised and the supervisory authorities must keep a register of the processing operations notified.

Every person shall have the right to a judicial remedy for any breach of the rights guaranteed by national law applicable to the processing in question. In addition, any person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for the damage suffered.

Transfers of personal data from a Member State to a third country with an adequate level of protection are authorised. However, although transfers may not take place when an adequate level of protection is not guaranteed, there are a number of exceptions to this rule listed in the Directive, e.g. the data subject himself agrees to the transfer, in the event of the conclusion of a contract, it is necessary for public interest grounds, but also if Binding Corporate Rules or Standard Contractual Clauses have been authorised by the Member State.

The Directive aims to encourage the drawing up of national and Community codes of conduct intended to contribute to the proper implementation of the national and Community provisions.
Each Member State is to provide one or more independent public authorities responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to the Directive.

A Working Party on the Protection of Individuals with regard to the Processing of Personal Data is set up, composed of representatives of the national supervisory authorities, representatives of the supervisory authorities of the Community institutions and bodies, and a representative of the Commission."
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l14012

24. Title: IWG Common Position relating to Reverse Directories (Hong Kong, 15.04.1998)

Summarized by: Ali

It is in any case necessary to endow the persons with the right to be informed by their provider of telephone or e-mail service, at the time of the collection of data concerning them, or if they have already subscribed, by a specific means of information, of the existence of services of reverse search and - if express consent is not required - of their right to object, free of charge, to such a search.

25. Title: IWG Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet (Crete, 4./5.05.2000)

Summarized by: Ali

The Working Group notes that the "Working Party on the protection of individuals with regard to the processing of personal data" of Data Protection Commissioners in the European Union ("Article 29 Group") has addressed these issues extensively in their “Opinion 3/99 on Public Sector information and the Protection of Personal Data” and fully supports their findings.

26. Title: IWG Common Position on Privacy and Data Protection aspects of the Publication of Personal Data contained in publicly available documents on the Internet (Crete, 4./5.05.2000)

Summarized by: Ali

- The amount of data collected and made publicly available in the course of the registration of a domain name should be restricted to what is essential to fulfil the purpose specified. In this respect the Working Group has reservations against a mandatory publication of any data exceeding name (which might also be the name of a company and not of a natural person), address and e-mailaddress in cases where the domain name holder is not himself responsible for the technical maintenance of the domain but has this done through a service provider (as is the case with many private persons who have registered domain names).

- Any technical mechanism to be introduced to access the data collected from the registrants must furthermore have safeguards to meet the principle of purpose limitation and avoidance of the possibility to unauthorised secondary use of the registrant's data.

27. Title: IWG Common Position on Incorporation of telecommunications-specific principles in multilateral privacy agreements: Ten Commandments to protect Privacy in the Internet World (Berlin, 13/14.09.2000)

Summarized by: Ali

Data Austerity: Telecommunications infrastructure has to be designed in a way that as few personal data are used to run the networks and services as technically possible.

Virtual Right to be Alone: Nobody must be forced to let his or her personal data be published in directories or other indices. Every user has to be given the right to object to his or her data being collected by a search engine or other agents. Every user has to be given the right and the technical means to prevent the intrusion of external software into his own devices.

28. Title: IWG Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe (Berlin, 13/14.09.2000)

Summarized by: Ali

In this respect the Working Group fully supports the findings of the European Data Protection Commissioners Conference that such retention of traffic data by Internet service providers would be an improper invasion of the fundamental rights guaranteed to individuals by the European Convention on Human Rights. This goes also for storing data revealing the use of the Internet by individuals. Existing powers for tracing crimes should not be extended in a way that invades privacy until the need for such measures has been clearly demonstrated. The Working Group has in the past stated that any Interception of Private Communications should be subject to appropriate safeguards.

29. Title: NORC Study of WHOIS Privacy/Proxy Prevalence (2010)

Summarized by: Coupet

Domain names can be registered using a Whois privacy or proxy service, which helps limit the amount of users' personal information that is made public via registrar and registry Whois services. The sample of domain names registered under the top 5 gTLDs indicates that about 18% of them used this type of service. Among these, Whois proxy service registrations were the most common.

30. Title: EWG Research: Data Protection Considerations Applicable to Collection of gTLD Reg Data Memo

Summarized by: Coupet

[ED NOTE: This memo was prepared by ICANN legal for the Expert Working Group on gTLD Directory Services (EWG) to provide guidance on data protection considerations for system models then under consideration at the time the memo was prepared. The EWG's Final Report includes discussion of several possible system models which subsequently emerged for consideration by the EWG, following consideration of this memo. Excerpts from the memo provided by Coupet follow.]

"The selection, implementation and use of a specific Whois database structure (i.e., centralized or federated) should be informed by applicable legal principles of "personal data" protection, but no uniform definition of "personal data" exists and there are various disparities between existing regimes. These differences in data projection regulation raise significant jurisdictional concerns, as well as potential regulatory obstacles on the global collection, processing, and transfer of gTLD registration data

that need to be considered when structuring, implementing, and administrating the Whois database replacement platform.

- Notwithstanding the territorial nature of data privacy laws, many such laws have extraterritorial reach.

- The administration of the Whois database may thus implicate the laws of (i) the country where the Whois database platform is located, (ii) the country where the data owner/licensor/controller (controller) is located (i.e., where the registrar, registry, and possibly the Whois database administrator are located to the extent such entities dictate the processing of gTLD registration data), and (iii) the country where the data subjects (e.g., registrants) are located

- The controlling and most relevant law to consider is the law where the data subject (i.e., registrant) resides, as the ultimate goal of data protection laws is the protection of individual personal data. Hence, the application of data protection laws will depend greatly on (i) where gTLD registration data will be located, (ii) whether ICANN (or the entity administering the database) will be viewed as a controller or processor of such data, and hence have direct compliance obligations, (iii) the obligations imposed on registrars/registries under their agreements with ICANN with respect to gTLD registration data, and (iv) the extent to which local data protection laws apply to registrants.

- The distinction between data controller and data processor is important, as controllers are required to comply with applicable data protection laws, and must impose certain data protection obligations on data processors. Processors are required to abide by the instructions of controllers.

- This will influence the data location and transfer considerations for the Whois replacement platform, whether as a centralized or federated model, and whether the Whois replacement database administrator and/or registrars conduct themselves as controllers in connection with gTLD registration data.

- The most comprehensive data protection and privacy compliance legal framework remains to be the E.U. Data Protection Directive (E.U. Directive), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data => baseline for data protection compliance

Data controllers must process personal data in accordance with the following relevant data privacy and protection principles:

- Purpose limitation: legitimate purposes only.
- Data quality and proportionality: accurate and up to date.

- Transparency: notification of data providers
- Security and confidentiality: protection measures
- Rights of access, rectification, deletion and objection by data subjects
- Sensitive data: additional security measures
- Direct marketing: “opt-out” must be possible
- Data retention: limited time to satisfy the purpose
- Accountability: for data collectors

The transfer of personal data from registrars to ICANN or the designated operator under a centralized model, or the sharing of data between registrars under a federated model, will therefore likely require data subject consent. Data transfers between ICANN or a designated operator and the registrars likely also require that certain contractual obligations be imposed throughout the system.

Choice of accountability and liability of the data controller or the data processor for any data breach or violation of local laws depends on the dependance (or independence) of the processor towards the controller in both models. Sanctions: Regulatory fines, criminal sanctions, and injunctions on data processing. International transfers of personal data in violation of local data protection laws could also lead to an injunction on data transfers, hampering the effectiveness of the Whois database replacement platform. The availability of such penalties under local data protection regimes will potentially fuel local registrar/registry opposition to a Whois database replacement platform under either of the proposed models.

Again, in some countries the transfer of personal data from registrars to ICANN or the designated operator under a centralized model, or the sharing of data between registrars under a federated model, likely will require the consent of the data subjects. Data transfers between ICANN or the designated operator and the registrars likely also require that certain contractual obligations be imposed throughout the system.

Other issues:

1) various registrars provide an upgraded fee-paying subscription service that addresses personal data privacy and may wich to continue with this source of revenues

2) considerable secure storage capacity. Cloud computing may introduce heightened data security concerns and complicate proportionality in processing, international transfer restrictions, and data storage.

Conclusion: While technical, political and other considerations will inform the implementation of the Whois database replacement platform, both models under consideration raise critical data privacy issues that must be considered. “

Privacy Team Summaries - drafted by gnso-rds-pdp-privacy@icann.org

31. Title: EWG Research: WHOIS Privacy and Proxy Service Provider Practices Survey

Summarized by: Coupet

Summary of practices that providers claim to use [in 2014] (11 offered P/P services out of 47 responses). However, this summary is not statistically representative of all providers. Services offered: combination of privacy, proxy, and registration services. Registrars and Resellers also offered BOTH Privacy and Proxy services out of the 11. 7 providers published customer contact information on their website, but just two of those explicitly included a phone number. Ten providers supplied links to their P/P service contracts and Customer service is available by phone, email, and Live Chat.

Other practices reported:

- P/P Service Contracts and Customer Support
- Protecting Customer Contact Details
- Relaying Customer Correspondence
- Validating Customer Contact Details
- Conditions of Service
- Handling of Inquiries
- Transfer, Renewal and Suspension Procedures
- Complaint Handling
- Escrow, Logging and Automation

Finally, one provider that did not want his identity disclosed offered this further comment for consideration by the EWG and PPSAI WG: *"You can make all the policies you like, but all that will happen if you try to 'regulate' or 'accredit' privacy services is that every domain name registered will simply show as care-of the registrar and NO information will be put into a public Whois about anything."*

32. Title: EWG Recommendations for a Next-Generation RDS, especially

Section 6a, Data Protection Principles**,** Section 6b, Principles for Data Access by Law Enforcement, Section 7, Improving Registrant Privacy, Annex H, Model for Relay and Reveal

Summarized by: Samuels

[The following text] summarizes that portion of the EWG's Report pertaining to privacy, inclusive of the FAQs. Much of what is said can be gleaned from Pages 11-12 and Section VI of the report. Here goes:

The EWG explicitly adopted that for the next generation RDS, registrants have a right to privacy and the reasonable expectation for the protection of their personal data, even when jurisdictions do not have data protection laws. We explicitly recommended adoption of a policy framework of 'privacy from the start' and implement mechanisms to introduce, harmonize and routinely reinforce this perspective; privacy by design. We recommended adoption of several overarching legal principles as framework:

Privacy Team Summaries - drafted by gnso-rds-pdp-privacy@icann.org

"Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject,
- collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,
- adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed, and
- accurate and kept up-to-date as required for the specified purposes.

Lawful processing, including transfer and disclosure can be – subject to the relevant jurisdiction – based on:

- consent of the data subject,
- the necessity for the performance of a contract to which the data subject is party, and
- the necessity for compliance with a legal obligation to which the controller is subject."

In addition, the Group adopted as principle the aright of the data subject to accessthe information and a right to rectify inaccuracyin the information kept on them.The report then outlined several ways privacy would be embraced and even enhanced in the next generation RDS:

- ICANN adopt and disseminate a privacy policy
- Add and use standard contract clauses that are harmonized with privacy and data protection laws and codified in policy
- A “rules engine” to apply data protection laws by jurisdiction
- a pre-validated Contact Directory which offers unique Contact IDs to deter personal data fraud
- a centralized interface from whence to access all gTLD registration data- gated dataset beyond a small subset of RD for publication
- RDAP or EPP to access gTLD data in the several registration data stores
- purpose driven access to data inside the gate and only to users who disclose their identity, are authenticated, request gated data for a previously determined permissible purpose and are accountable. This includes law enforcement.
- An accredited Privacy/Proxy Service for general use
- An accredited Secure Protected Credentials Service for persons at risk and in instances where free speech rights may be denied or speakers persecuted.

33. Materials: EWG Tutorials and FAQs

EWG Tutorial Pages 28-30
EWG FAQs 31-38
Summarized by: Coupet

EWG Tutorial

EWG's Final Report

- Details a proposed next-generation Registration Directory Service (RDS)
- Strikes a balance between accuracy, access, and accountability
- Collects, validates and discloses gTLD data for permissible purposes only
- Leaves minimum data publicly available
- Safeguards the rest through a new paradigm: purpose-driven gated access
- Introduces new contracted parties to
    - Validate Contact Data
    - Accredit RDS Users

Contact Data can contain

- Third-party PBC's information, authorized for use by this Domain Name
- Forwarding addresses, supplied by an accredited Privacy Service
- Proxy's information, supplied by an accredited Proxy Service
- Registrant's own information, if no other choice is made
- Each Contact Holder can opt to gate data not needed for purpose(s)

Data Protection Principles

- Compliance challenges growing rapidly for WHOIS, exacerbated by new gTLDs
- Mechanisms must be adopted to facilitate routine legally compliant data collection and transfer between RDS ecosystem actors handling personal data, including

    1. Standard Contract Clauses that are harmonized with privacy and data protection laws, codified in a policy and enforced through contracts
    2. "Rules Engine" to apply data protection laws
    3. RDS Storage Localization to implement a high level of data protection

Privacy Principles

- In addition to compliance with data protection laws, the RDS ecosystem must accommodate needs for privacy by including:
    - An accredited Privacy/Proxy Service
    - An accredited Secure Protected Credentials Service
- There Accreditation and rules for the provision and use of accredited Privacy/Proxy services

- Outside of domain names registered via accredited Privacy/Proxy Services, Registrants must assume responsibility for the domain names they register

Secure Protected Credentials (Slide 30 – refer to diagram)
For persons at risk, and in instances where free-speech rights may be denied or speakers persecuted

EWG FAQs

Summary: P/P services with accreditation and rules to provide anonymity. Contact ID publicly available. Rules engine. Validation and authentication of Registrants, and Purpose-based Contatcs (PBC) with gated access.

- There should be accreditation for privacy/proxy service providers and rules regarding provision and use of accredited privacy/privacy services. The RDS has been designed to leverage accredited privacy/proxy services to address routine privacy needs, incorporating new data elements to facilitate provider identification, customer contact, and abuse reporting.

- The RDS accommodates needs for anonymity by offering an accredited "secure protected credentials" service for persons at risk, and in instances where free-speech rights may be denied or speakers persecuted.

- As with other systems that collect personal data, proper system design, security measures, audits and oversight would be needed to minimize data breach risk. Insider abuse should be deterred through security policy, implementation, enforcement and third-party auditing.

- Mechanisms should be adopted to facilitate routine legally compliant data collection and transfer between actors within the RDS ecosystem. To accomplish this, RDS actors will be held to standard contract clauses that are harmonized with data protection and privacy laws, codified in RDS policy, and implemented through a "rules engine" that applies policy as appropriate for each jurisdiction.

- To improve both accountability and reachability, validated Registrant, Administrative, Technical, Abuse, and Legal Contacts would be required for all new domain names. However, Registrants would have many ways to be accountable without publishing personal data, including inexpensive/free accredited Privacy Services and new third-party contact options. To deter identity theft, a Contact ID could not be used within a domain name registration without authorization.

- While the RDS would require every registered domain name to be associated with Contact IDs as needed to satisfy permissible purposes, Purpose-Based Contact (PBC) data elements would NOT be publicly available to everyone. The Contact ID for each PBC would be publicly accessible to all, but PBC names and addresses would only be accessible to authenticated requestors, authorized to access RDS data for the specific purpose associated with each Contact.

- No requestor would ever have unfettered access to the entire data set. The RDS does not use a one-size-fits-all "gate." Requestors and their registration data needs vary; so would gated access policies. Like most on-line services that hold private data, the RDS would apply policy-defined permissions,

driven by requestor identity and stated purpose, with uniformly-enforced terms of service, backed by more consistent measures to deter and mitigate abuse.

- The RDS should store data in jurisdiction(s) where law enforcement is globally trusted. Interpol should accredit its own members.

34. Title: EWG Member Statements/Blogs by Ajayi and Perrin

Summarized by: Coupet

Summary of Blog by Ajayi provided by Coupet
Concerned with data accuracy. Nothing on privacy.

Excerpts provided by Coupet from Statement published by Perrin
"There are three questionable basic outcomes:

- Legal contact requirement: address and phone number are mandatory to provide, and published outside the gate, in the publically available data.
- The default, if one is a simple registrant who does not want to hire a lawyer or other actor to assume the role of legal contact and publish their details in the RDS, to publishing registrant information, notably address and phone number in the RDS outside the gate.
- The inclusion of a principle of consent (28), whereby a registrant may consent to the use or processing of her gated information for the permissible purposes enumerated for accredited actors behind the gate.

Rules engine that enforces jurisdiction, with respect to the privacy rights of individuals who are protected by personal data protection law.

- But it only protects individuals, and occasionally legal persons in some jurisdictions, and only where data protection is in place, and would find the presence of name, address and phone number in a public directory to be in conflict with data protection law. Not all data protection regimes would find, or have found, that directory information must be protected.
- Secondly, it is not clear enough for me how that rules engine would encode rights.
- A third problem with the rules engine, is that it proposes to address regimes with data protection law only….what happens to organizations that have a constitutional right to privacy for the purposes of free speech and freedom of association, such as in the United States?
- Finally, is it fair to individuals in jurisdictions where their countries have not enacted data protection law? Does ICANN, in the monopoly administration of a public resource, not have a responsibility to set standards on an ethical basis, based on sound best practice?

Two inadequate remedies:

- Hire a privacy proxy/service provider, or proxy contact, if you do not want your contact data published in the public portion of the RDS
- The rules engine will enforce data protection rights, and place this data behind the gate.

Consent principle.

- Consent must be read in the context of legitimacy of purpose, proportionality, rights to refuse, rights to withdraw consent, specificity of purpose and use, and soon. To offer individuals and

organizations the opportunity to consent to the use of their sensitive, gated data, for all the permissible purposes, that can be read as providing blanket consent to accredited users behind the gate. If you understand the risks, you will hire a proxy service. From the perspective of an elite North American, this looks like a no brainer, just hire a proxy.
- However, we have a responsibility to examine this from the perspective of a global eco-system.

Recommendations:
- Gate the legal contact information for individuals and organizations who wish to protect their private data
- Consent needs to be meaningful, specific, explicit and for legitimate purposes. A blanket consent as envisioned here does not meet these requirements"

35. Title: Process Framework for a PDP on Next-Generation RDS

Summarized by: Coupet

Input to PDP WG on Privacy

- EWG Principles Sect 6&7
- P/P Provider Survey
- WHOIS P/P Abuse Study-Data Protect/Privacy Memo
- GNSO PPSAI WG Report

PDP WG Phase 1: Privacy Policy Requirements

- Privacy/Proxy Needs
- At-Risk Reg Needs
- Data Protection Laws

PDP WG Phase 2: Privacy Policy Functional Design

- Overarching DP Policy
- DP LawCompliance
- Privacy/Proxy Policies-Secure Protected Creds

PDP WG Phase 3: Privacy Implementation and Coexistence Guidance on

- RDS Privacy Policy Needs
- Detailed Legal Analysis
- P/P Accreditation Needs
- SPC Provider Criteria

36. Title: Human Rights Council - Report by the UN Special Rapporteur on the right to privacy

Summarized by: Coupet

The balance between privacy and security might start to tip again in favor of privacy, across borders.

In the resolution the Council emphasizes that Human Rights need to be protected under all circumstances, at all times and in all environments.

In a world which benefits greatly from an Internet without borders, the SRP's consultations indicate widespread support for a general principle of

- Safeguards without borders
- Remedies across borders

Positing privacy as an enabling right as opposed to being an end in itself, the SRP is pursuing an analysis of privacy as an essential right which enables the achievement of an over-arching fundamental right to the free, unhindered development of one's personality.

The vast revenues derived from the monetisation of personal data to the extent that it has become a marketable and tradable commodity mean that the incentive for changing the business model simply on account of privacy concerns is not very high.

While not necessarily the primary target of cyber-security and cyber-espionage measures, the ordinary citizen may often get caught in the cross-fire and his or her personal data and on-line activities may end up being monitored in the name of national security in a way which is unnecessary, disproportionate and excessive.

Importance of determining the balance, on the one hand, use of data for the benefit of society under the principles of OpenData and, on the other hand, the established principles we have developed to date with a view to protecting fundamental rights like privacy, autonomy and the free development of one's personality. It will be seen that, in many cases, the debate on privacy cannot be usefully divorced from that on the value of autonomy or self-determination. Germany: since 1983, rise to a constitutional right to "informational self-determination".

Individual complaints: Every so often, and as the mandate will become known, the SRP has received and will presumably continue to receive complaints from individual members of the public residing in a given national territory or from civil society actors of alleged infringements of privacy rights.

There is no binding and universally accepted definition of privacy. As reaffirmed by the Human Rights Council in resolution28/16 article 12 of the Universal Declaration of Human Rights (UDHR) and article 17 of the International Covenant on Civil and Political Rights (ICCPR)constitute the basis of the right to privacy in international human rights law. For the passage of time and the impact of technology, taken together with the different rate of economic development and technology deployment in different geographical locations means that legal principles established fifty years ago(ICCPR) or even thirty-five years ago (e.g. the European Convention on Data Protection) let alone seventy years ago (UDHR) may need to be re-visited, further developed and possibly supplemented and complemented to make them more relevant and useful to the realities of 2016.

Properly speaking, it is not helpful to talk of "privacy vs. security" but rather of "privacy and security" since both privacy and security are desiderata... and both can be taken to be enabling rights rather than ends in themselves.

Brazil and Germany have the right to privacy written into their constitution and it is the SRP's contention that a) such aright to dignity and the free, unhindered development of one's personality should be considered to be universally applicable and b) that already-recognised rights such as privacy, freedom of expression and freedom of access to information constitute a tripod of enabling rights which are best considered in the context of their usefulness in enabling a human being to develop his or her personality in the freest of manners.

Conclusions:

- Privacy has never been more at the forefront of political, judicial and personal consciousness than in2016;
- The tensions between security, corporate business models and privacy continue to take centre stage but the last twelve months have been marked by contradictory indicators: some governments have continued, in practice and/or in their parliaments to take privacy-hostile attitudes while courts world-wide but especially in the USA and Europe have struck clear blows in favour of privacy and especially against disproportionate, privacy-intrusive measures such as mass surveillance or breaking of encryption.

37. Title: Judgement on preliminary ruling under Article 267 TFEU from Audiencia Nacional (Spain)

Summarized by: Coupet

Summary: The right to be forgotten. In May 2014, the European Court of Justice ruled against Google in Costeja, a case brought by a Spanish man, Mario Costeja González, who requested the removal of a link to a digitized 1998 article in La Vanguardia newspaper about an auction for his foreclosed home, for a debt that he had subsequently paid.[40] He initially attempted to have the article removed by complaining to the Spanish Data Protection Agency, which rejected the claim on the grounds that it was lawful and accurate, but accepted a complaint against Google and asked Google to remove the results.[41] Google sued in the Spanish Audiencia Nacional (National High Court) which referred a series of questions to the European Court of Justice.[42] The court ruled in Costeja that search engines are responsible for the content they point to and thus, Google was required to comply with EU data privacy laws.[43][44][45] On its first day of compliance only (May 30, 2014), Google received 12,000 requests to have personal details removed from its search engine.

38. Title: Africa Union Convention on Cybersecurity and Personal Data Protection

Summarized by: Mutung'u

Adopted: July 2014
Status: awaiting ratification by at least 15 State Parties to take effect

State Parties that have ratified: to be confirmed (reports indicate that 5 states have deposited ratification instruments, the latest being Senegal).

African Union Convention on Cyber Security and Personal Data Protection

Preamble
"The Member States of the African Union:

Guided by the Constitutive Act of the African Union adopted in 2000.....

Considering that the establishment of a regulatory framework on cyber-security and personal data protection takes into account the requirements of respect for the rights of citizens, guaranteed under the fundamental texts of domestic law and protected by international human rights Conventions and Treaties, particularly the African Charter on Human and Peoples' Rights;.....

Stressing that at another level, the protection of personal data and private life constitutes a major challenge to the Information Society for governments as well as other stakeholders; and that such protection requires a balance between the use of information and communication technologies and the protection of the privacy of citizens in their daily or professional lives, while guaranteeing the free flow of information;"

Summary of Relevant Articles of the Convention
Chapter II is dedicated to personal data protection. Article 8 calls upon States to establish legal frameworks for "strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data."

It is important to note that like many instruments from Africa, the Convention envisages not only protection of human rights but also people's rights. Article 8 (2) for example requires that the legal mechanism established under Article 8 (1) "ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State, the rights of local communities and the purposes for which the businesses were established."

Other provisions are the basic principles for data processing. These are:

- consent and legitimacy of personal data processing
- lawfulness and fairness of personal data processing
- purpose, relevance and storage of processed personal data
- accuracy of personal data
- transparency of personal data processing
- confidentiality and security of personal data processing

Data subject rights are: Right to information, right of access, right to information, right to object and right to rectification/erasure.

Data controllers obligations are confidentiality, security, storage and sustainability.

39. Relevant National Laws or Court Rulings that may apply to gTLDs, including

US Supreme Court Case - McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995)
The Constitution of the State of California (USA): Article 1, Section 1
Massachusetts Right of Privacy, MGL c.214, s.1B
US Judicial Redress Act of 2015
Ghana Protection Act, 2012
South Africa's Act No. 4 of 2013: Protection of Personal Information Act

Title: US Supreme Court Case - McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995)
Summarized by: Kleiman
To be provided

Title: The Constitution of the State of California (USA): Article 1, Section 1
Summarized by: Kleiman

Synopsis:
"California Constitution, Article 1, section 1.The state Constitution gives each citizen an "inalienable right" to pursue and obtain "privacy." (Summary from website of Attorney General of California).

Full text:
CALIFORNIA CONSTITUTION ARTICLE 1
DECLARATION OF RIGHTS SECTION 1.

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

Additional Information:
The law firm of Dorsey & Whitney published a memo re: the California Constitution which included:

"While there is no express right to privacy in the United States Constitution, the U.S. Supreme Court recognized the right for the first time in *Griswold v. Connecticut* 381 U.S. 479 (1965). In contrast, the California Constitution was amended in 1972 to *expressly* provide for a right to privacy:

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, **and privacy**. *California Constitution, Article 1, Section 1 (emphasis added).*

In contrast to the right to privacy recognized in the U.S. Constitution which requires state action, the right to privacy under California law is generally understood to encompass actions by private individuals and entities which violate a privacy right."

Dorsey & Whitney LLP, *A primer on California privacy law: how things are different in the golden state,* http://www.lexology.com/library/detail.aspx?g=dbde88f6-68ed-46a2-8834-359651f5f371

Title: Massachusetts Right of Privacy, MGL c.214, s.1B
Summarized by: Kleiman

Synopsis:
Like the US State of California, Massachusetts provides its citizens with a right to privacy.

Full text:
Massachusetts Laws
MGL c.214, s.1B Right of Privacy

Section 1B. A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.

Additional Information:
Code of Massachuetts Regulations: 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH
***
Purpose and Scope
(1) Purpose
This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

More at: http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

Title: US Judicial Redress Act of 2015
Summarized by: Kleiman

Enacted: Signed into law by President Obama on Feb 24, 2016

Synopsis:
This newly-adopted law authorizes the US attorney general to extend the protections of the Privacy Act of 1974 to the citizens of designated foreign countries. Citizens of the EU, for example, may bring complaints against US companies to their Data Protection Commissioners or to a new forum to be established at the US Federal Trade Commission. Passage of this Act was considered by EU diplomats as a requirement for acceptance of the new EU-US Privacy Shield – for current cross-border data flows.

The Judicial Redress Act provision reference the US Privacy Act of 1974, 5 US Code § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of

information about individuals that is maintained in systems of records by federal agencies. It empowers Americans to challenge U.S. companies' disclosure of their private data to the government, as well as the government's use of the data and any inaccuracies in resulting federal records about them

The rights granted to US citizens in 1974 are granted to European Union citizens and others in this new law.

Title: Ghana Protection Act, 2012 Act 843
Summarized by: Mutung'u

Assented: l0 May 2012

Ghana Data Protection Act
Short Title
An Act to establish a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of 7 personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters.

Summary of Relevant Sections of the Act
Privacy of the individual
Section 17 lays out the privacy principles for processing data which are: accountability, lawfulness of processing, specification of purpose, compatibility of further processing with purpose of collection, quality of information, openness, data security safeguards, and data subject participation.

In addition, section 18 requires a person who processes personal data to ensure that such processing is done under three conditions: without infringing the privacy rights of the data subject; in a lawful manner; and in a reasonable manner.

Other provisions on privacy are that foreign data subjects data to be processed in accordance with their country of origin. In addition the principles of purpose (necessity, relevance and non excessive), consent justification and objection, right to object, specificity, making data subject aware of purpose of collection, retention, further processing, quality of information, security, access to information and correction of data are provided for.

Sections 37-45 provide for processing of personal data while sections 60 to 74 spell out the exemptions under the Act. These include national security, crime and taxation, health, education and social work, professional privilege and confidential references given by a data controller.

Additional information:
There are several countries in Africa with data protection/privacy laws. These include Angola, Benin, Burkina Faso, Gabon, Ghana, Lesotho, Mali, Mauritius, South Africa and Tunisia. Ghana is a sample of the other African laws.

Title: South Africa's Act No. 4 of 2013: Protection of Personal Information Act, 2013
Summarized by: Mutung'u

Assented: 26 November 2013

South Africa Protection of Personal Information Act
Short Title
An Act to promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith.

Summary of Relevant Sections of the Act
2. Purpose of Act.
The purpose of the Act is to—
(a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—
(i) balancing the right to privacy against other rights, particularly the right of access to information; and
(ii) protecting important interests, including the free flow of information within the [South Africa] and across international borders;
(b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;
(c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and
(d) establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfill the rights protected by this Act.

4. Conditions for lawful processing of data
There are eight conditions for the lawful processing of personal information by or for a responsible part. These are: accountability, processing limitation (including minimality), purpose specification (including limitations on retention), further processing limitation, information quality, openness, security safeguards and data subject participation.

5. Rights of data subjects
Data Subjects have the right for their data to be collected according to the eight conditions set out in section 4. In addition, they have the following rights: notification when their data is being sought, to be notified that data about them has been accessed, access to their information, correction, destruction, deletion of their information, object to processing of their information and to institute complaints among other rights.

The law in Chapter 3 Part B (Sections 27-33) deals with special personal information, publication of which is prohibited.

Chapter 7 deals with dispute resolution and the regulator may issue codes of conduct for players. Chapter 9 captures the issue of transborder information flows. Data from South Africa may only be exported to a third party with a legal framework for lawful processing of information.

Additional information:
This is an important law as most of the gTLDs in Africa are based in South Africa. Additionally, many African countries benchmark with South African law when making their laws.

40. Book: Global Tables of Data Privacy Laws and Bills (Greenleaf, 4rd Edition, January 2015)

Summarized by: Kleiman

Countries with comprehensive data protection laws that regulate data collected by the private sector:
Albania, Andorra, Angola, Argentina, Armenia, Australia, Azerbaijan, Bahamas, Belgium, Benin, BES Islands, Bosnia & Herzegovina, Bulgaria, Burkina Faso, Canada, Cape Verde, Chile, Columbia, Costa Rica, Cote d'Ivoire, Croatia, Curacao,Cyprus, Czech Republic, Denmark, Dominican Republic, Dubai IFC, Estonia, Faroe Islands, Finland, France, Gabon, Georgia, Germany, Ghana, Gibraltar, Greece, Greenland, Guernsey, Hong Kong SAR, Hungary, Iceland, India, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Kazakhstan, Korea/South, Kosovo, Kyrgyz Republic, Latvia, Lesotho, Liechtenstein, Lithuania, Luxembourg, Macao SAR, Macedonia, Madagascar, Malaysia, Mali, Malta, Mauritius, Mexico, Moldova, Monaco, Montenegro, Morocco, Netherlands, New Zealand, Nicaragua, Norway, Paraguay, Peru, Philippines, Poland, Portugal, Qatar FC, Romania, Russia, San Marino, Senegal, Serbia, Seychelles, Slovakia, Slovenia, South Africa, Spain, St Lucia, St Maartens, Sweden, Switzerland, Taiwan, Trinidad & Tobago, Tunisia, Ukraine, UK, Uruguay and Vietnam.

Synopsis:
Professor Greenleaf has been publishing tables on global data protection law since 2011. In 2011, he and his staff found "an unexpectedly high finding of 76 countries" with comprehensive data privacy laws. In 2012, the country was 89 countries. In 2013, it was 99. *Now, the January 2015 Tables show that number of countries which have now enacted comprehensive private sector data privacy laws has risen to 109 over the past eighteen months* – with 22 Bills for new Acts pending since the last table.

These data protection laws worldwide lead to Professor Greenleaf's recent conclusion: "Countries without data privacy laws [are] now in the minority."

Additional information:
Information in these comprehensive tables includes: Country, name of privacy law, year of adoption, and name of the DPA – data protection authority.

41. Article: Global data privacy laws 2015: 109 countries, with European laws now a minority (Greenleaf)

Summarized by: Kleiman

Full citation: Greenleaf, Graham, Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority (January 30, 2015). (2015) 133 Privacy Laws & Business International Report, February 2015; UNSW Law Research Paper No. 2015-21. Available at SSRN: http://ssrn.com/abstract=2603529

Synopsis:
The findings of Professor Greenleaf, longtime compiler of global data protection and privacy laws, to him, are a little surprising. In 2015, the number of countries with comprehensive data protection laws ***surpassed those*** without data protection laws – for a total of 109 countries. Those adopting comprehensive data protection laws recently include: the Dominican Republic, Kazakhstan, South Africa, Mali, Cote d'Ivoire, Lesotho and Madagascar. Further, the pace continues as about 20 countries currently evaluate adoption.

Professor Greenleaf shares several conclusions from his years of research and publication:

- "Countries without data privacy laws now in a minority."
- "Future growth: Heading toward ubiquity." "Global growth is likely to continue beyond 2020.

He adds that: "[b]y 2023, 50 years after enactment of the first such national data privacy law in Sweden, by far the majority of countries (but not all) are likely to have such laws, as are most of their neighbours and most of those with whom they trade: this will be global ubiquity."

The fast growth are recently has been Africa.

Additional Information:
Greenleaf's article describes that by the end of this decade the number of countries with data privacy laws, all of which have a strong 'family resemblance' will be between 66% and 80% of all independent jurisdictions globally.

This article can be ready in accompaniment with Professor Greenleaf's *Global Tables of Data Privacy Laws and Bills (4th Ed, January 2015) – separately listed in our Working Group summaries* – and found at http://ssrn.com/abstract=2603502

(Quick note that countries with laws covering parts of their private sector (e.g., credit reporting or medical records) did not meet the criteria for Greenleaf's study or global privacy laws table compilation.)

42. WorldLII Database of National Data Privacy Legislation

Summarized by: Coupet

Important database for the construction of the 'rules engine'. [From EWG Report recommendations:] RDS actors will be held to standard contract clauses that are harmonized with data protection and privacy laws, codified in RDS policy, and implemented through a "rules engine" that applies policy as appropriate for each jurisdiction.