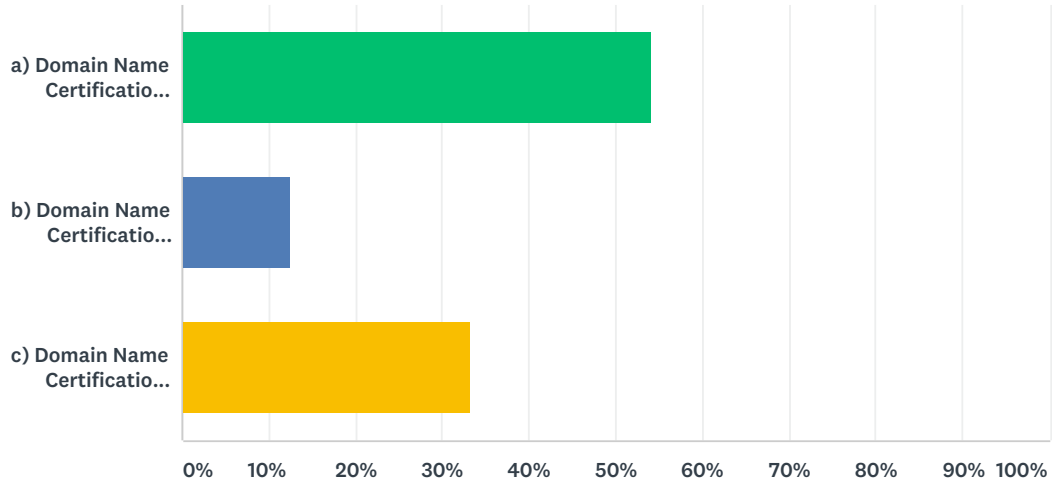
Q1 1. Your name (must be RDS PDP WG Member - not WG Observer - to participate in polls) If you are a WG Observer and wish to participate in polls, you must upgrade to WG Member to do so. Please do NOT participate in this poll if you are a WG Observer who has not upgraded to WG Member.

Answered: 27 Skipped: 0

#	RESPONSES	DATE
1	Stephanie Perrin	1/14/2018 6:58 AM
2	Steve Metalitz	1/13/2018 1:20 PM
3	Greg Mounier EUROPOL	1/13/2018 10:26 AM
4	Tom Lancaster	1/12/2018 6:10 PM
5	John Bambenek	1/12/2018 5:43 PM
6	Mason Cole	1/12/2018 5:13 PM
7	Nathalie Coupt	1/12/2018 4:17 PM
8	Sara Bockey	1/12/2018 1:06 PM
9	Vicky Sheckler	1/12/2018 12:13 PM
10	Brian Winterfeldt	1/12/2018 11:23 AM
11	Craig Urness	1/12/2018 10:08 AM
12	Evan Smith	1/12/2018 10:08 AM
13	Gary Campbell	1/12/2018 9:00 AM
14	Rod Rasmussen	1/12/2018 8:56 AM
15	Klaus Stoll	1/12/2018 7:47 AM
16	andrew sullivan	1/12/2018 7:27 AM
17	Ayden Férdeline	1/11/2018 12:43 AM
18	Benny Samuelsen	1/10/2018 6:09 PM
19	Michael Peddemors	1/10/2018 3:33 PM
20	Kal Feher	1/10/2018 2:40 PM
21	Sam Lanfranco	1/10/2018 12:09 PM
22	Michael Hammer	1/10/2018 11:38 AM
23	Greg Aaron	1/10/2018 11:11 AM
24	Chuck Gomes	1/10/2018 11:04 AM
25	Paul Keating	1/10/2018 10:20 AM
26	Krishna Seeburn (Kris)	1/10/2018 9:31 AM
27	Marco Schmidt	1/10/2018 9:30 AM

Q2 2. Domain Name Certification: Last week's poll and discussion during this WG call was based on the following draft definition of Domain Name Certification produced by the drafting team:Information collected by a certificate authority to enable contact between the registrant, or a technical or administrative representative of the registrant, to assist in verifying that the identity of the certificate applicant is the same as the entity that controls the domain name.Following discussion of this purpose, last week's poll results, and refinement of possible agreement text, most of those on the 9 January call expressed support for the following possible WG agreement:Domain Name Certification is NOT a legitimate purpose for requiring collection of registration data, but may be a legitimate purpose for allowing some data to be collected, and/or for using some data collected for another purpose. In this poll, the term "collection" includes not only data collected from registrants, but also data derived or implied or otherwise supplied by the registrar or registry. Do not assume that collection implies public or non-public access to that data or who will have access; this will be deliberated separately later. Please indicate below which statement below best reflects your level of agreement. Simply skip this question if you wish to abstain.

Answered: 24 Skipped: 3



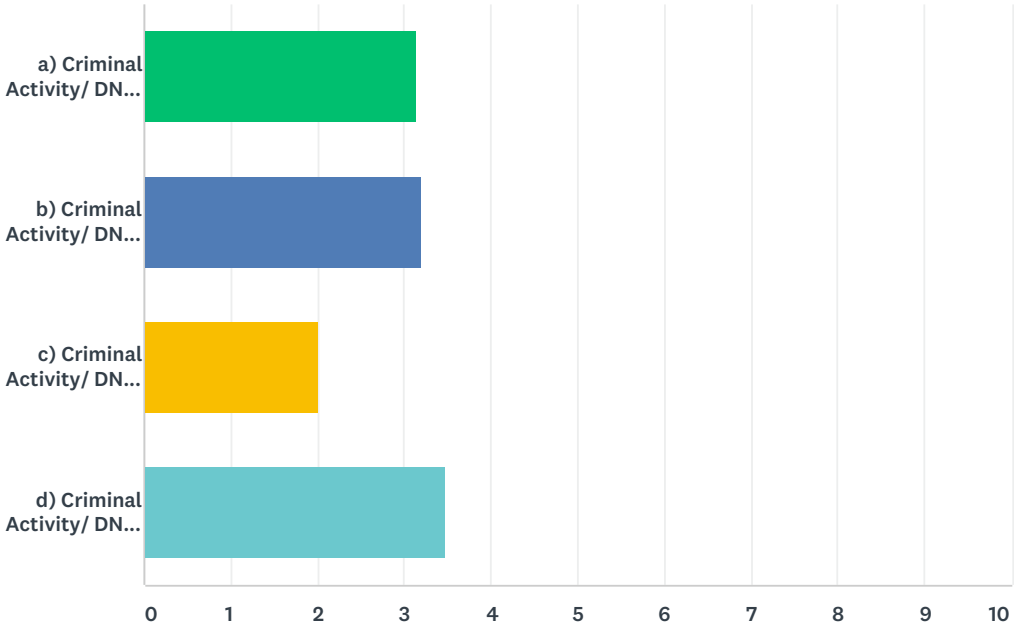
ANSWER CHOICES	RESPONSES	
a) Domain Name Certification is NOT a legitimate purpose for requiring collection of registration data, but may be a legitimate purpose for allowing some data to be collected, and/or for using some data collected for another purpose.	54.17%	13
b) Domain Name Certification is NOT a legitimate purpose for requiring collection of registration data, but I wish to propose an alternative statement in the comment box below.	12.50%	3

c) Domain Name Certification IS a legitimate purpose for requiring collection of some registration data. (Please provide rationale and essential data in the comment box below.)	33.33%	8
TOTAL		24

#	PLEASE PROVIDE YOUR RATIONALE FOR DISAGREEING WITH THE POSSIBLE WG AGREEMENT OR PROPOSED ALTERNATIVE:	DATE
1	Domain name certification is not a legitimate purpose for requiring collection of registration data. It may be a valid reason to permit the voluntary collection of relevant data, for such a purpose.	1/14/2018 6:58 AM
2	The mission of ICANN and the purpose of DNS is to enable transparency so not only business interests can protect their IP, but consumers can be protected by the very real threats to their privacy and security by those who would impersonate legitimate entities in the attempt to further criminal means.	1/12/2018 5:43 PM
3	Domain Name Certification is NOT a legitimate purpose for requiring collection of registration data. Any additional uses/other purposes for registration data must be specific and legitimate, and only limited data for said specific, legitimate purpose should be provided.	1/12/2018 1:06 PM
4	one purpose of collecting the data is for transparency and accountability purposes. Domain name certification falls within this purpose.	1/12/2018 12:13 PM
5	If the CA cannot contact the registrant, then it is impossible to address issues related to fraud, security, and/or data compromises. This is a 'relationship' as defined by many similar and related definitions, and entities with a 'relationship' MUST be able to both identify the other party in the relationship, and communicate with the party.	1/10/2018 3:33 PM
6	DNS and WHOIS are part of an ecosystem. To consider it in isolation from that ecosystem provides incorrect scoping as a basis for answering the above and arriving at the conclusion that it is not a legitimate purpose.	1/10/2018 11:38 AM
7	While not currently an "obligation" under the string of agreements originating from ICANN and extending to Registries, registrars and ultimately to registrants, it should be. Certification is an important element of overall Internet and domain space security. ICANN should begin the process of adding additional obligations to the relevant agreements.	1/10/2018 10:20 AM

Q3 3. Criminal Activity/DNS Abuse Investigation: Discussion during this WG call was based on the following draft definition of Criminal Activity/DNS Abuse Investigation produced by the drafting team:Information to be made available to regulatory authorities, law enforcement, cybersecurity professionals, IT administrators, automated protection systems and other incident responders for the purpose of enabling identification of the nature of the registration and operation of a domain name linked to abuse and/or criminal activities to facilitate the eventual mitigation and resolution of the abuse identified: o Domain metadata (registrar, registration date, nameservers, etc.)o Registrant contact informationo Registrar contact Informationo DNS contact, etc.Following discussion of this purpose and refinement of possible agreement text, most of those on the 9 January call expressed support for the following possible WG agreement:Criminal Activity/ DNS Abuse – Investigation is NOT a legitimate purpose for requiring collection of registration data, but may be a legitimate purpose for using some data collected for other purposes.A few on the call supported an alternative version of this possible WG agreement which allows for optional data collection, similar to the possible WG agreement reached for Domain Name Certification. In this poll, the term "collection" includes not only data collected from registrants, but also data derived or implied or otherwise supplied by the registrar or registry. Do not assume that collection implies public or non-public access to that data or who will have access; this will be deliberated separately later. Note this purpose is limited to Investigation of Criminal Activity/DNS Abuse. Purposes associated with Notification and Reputation will be deliberated separately later. Please rank the statement(s) below to reflect views on this possible agreement, with "1" indicating your top choice and"2" indicating your second choice (if any). Choose N/A for any statement that you do not support. Simply skip this question if you wish to abstain.

Answered: 26 Skipped: 1



	1	2	3	4	N/A	TOTAL	SCORE
a) Criminal Activity/ DNS Abuse – Investigation is NOT a legitimate purpose for requiring collection of registration data, but may be a legitimate purpose for using some data collected for other purposes.	29.17% 7	16.67% 4	12.50% 3	4.17% 1	37.50% 9	24	3.13
b) Criminal Activity/ DNS Abuse – Investigation is NOT a legitimate purpose for requiring collection of registration data, but may be a legitimate purpose for allowing some data to be collected, and/or for using some data collected for another purpose.	16.67% 4	41.67% 10	4.17% 1	0.00% 0	37.50% 9	24	3.20
c) Criminal Activity/ DNS Abuse – Investigation is NOT a legitimate purpose for requiring collection of registration data, but I wish to propose an alternative statement in the comment box below.	5.26% 1	5.26% 1	5.26% 1	15.79% 3	68.42% 13	19	2.00
d) Criminal Activity/ DNS Abuse – Investigation IS a legitimate purpose for requiring collection of some registration data. (Please provide rationale and essential data in the comment box below.)	56.52% 13	0.00% 0	13.04% 3	4.35% 1	26.09% 6	23	3.47

Q4 If applicable, please provide your rationale for disagreeing with the possible WG agreement or proposed alternative:

Answered: 10 Skipped: 17

#	RESPONSES	DATE
1	Investigation of criminal activity/DNS abuse is not a legitimate purpose for the collection of registration data, but is a legitimate purpose for data collected/generated for other legitimate purposes to be released under proper authority.	1/14/2018 6:58 AM
2	Transparency and accountability are important functions of the RDDS, concerns that are particularly strong in the case of investigation of criminal or abusive activities carried out through registration or use of domain names. Information identifying and providing jurisdictional information and contactability of the registrant (and perhaps of other contacts) must be collected to enable such investigation. (Leaving to one side of course the circumstances and terms and conditions under which such data would be disclosed or accessed.) Allowing this information to be used only to the extent it is being collected for some other purpose potentially sacrifices the availability of such data when it is needed to safeguard public safety and deal expeditiously with abuse. If it is no longer needed to be collected for the "other" purpose then it would no longer exist for this purpose. (b) is deficient because it necessarily implies that investigation might not be a legitimate purpose for allowing ANY data to be collected. A modification of (b) that may be worth considering: "Investigation is NOT a legitimate purpose for requiring collection of registration data, but IS a legitimate purpose for allowing some data to be collected, and/or etc." But even this formulation is suspect because it seems to forbid even special purpose registries in highly regulated or sensitive sectors (e.g., medical, financial fiduciary) from requiring the collection of information needed to prevent or investigate abuses.	1/13/2018 1:20 PM

3	There are plenty of legal reasons/grounds - including ICANN's Bylaws and GDPR provisions - to argue that in fact, investigating criminal activity and DNS Abuse IS a legitimate purpose for requiring the collection of registration data. Some of these legal reasons/grounds have been mentioned during the discussion on the mailing list and during the call on 9th January. Unfortunately, I think that the possible WG agreement does not reflect the correct conclusions that should be drawn from these reasons and I specifically disagree with the conclusion that we should make a distinction between 1) the purpose of collecting the data and 2) the purpose for using the data collected for other purposes (manage domain registrations). The reason why I disagree with making this distinction is that it leads to artificially reduce the importance of a perfectly valid and legitimate purpose, acknowledged by ICANN Bylaws: to address malicious abuse of the DNS (ICANN's mandate is to "ensure the stable and secure operation of the internet's unique identifier systems" + WHOIS data is essential for "the legitimate needs of law enforcement" and for "promoting consumer trust."). Here is a list of reasons why I think that investigating criminal activity and DNS Abuse IS a legitimate purpose for requiring the collection of registration data and why requiring collection of data to prevent crime is NOT beyond ICANN's mandate: 1) ICANN's Bylaws support the conclusion that WHOIS services should serve the legitimate needs of law enforcement and promote consumer trust and as noted in Hamilton memo #3: "it would be incorrect to state that the only purpose of the Whois services is to manage domain name registrations." 2) ICANN's Bylaws, revised in 2016, make clear that ICANN's mandate is to "ensure the stable and secure operation of the internet's unique identifier systems." Further, ICANN's Bylaws include a commitment to preserve and enhance "the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet." 3) Finally, ICANN's commitments and required reviews emphasize that it must "adequately address" issues related to "consumer protection, security, stability, resiliency [and] malicious abuse." 4) Regarding registration data specifically, ICANN's Bylaws recognize that WHOIS data is essential for "the legitimate needs of law enforcement" and for "promoting consumer trust." The GAC has also recognized these important purposes in its recent advice reflected in the Abu Dhabi Communiqué, noting that WHOIS data is used for a number of legitimate activities including: assisting law enforcement authorities in investigations; assisting businesses in combatting fraud and safeguarding the interests of the public; and contributing to user confidence in the Internet as a reliable means of information and communication. In addition, ICANN Bylaws require it to use commercially reasonable efforts to enforce its policies relating to the Registration Directory Service, while exploring structural changes to improve accuracy and access to generic top-level domain registration data, as well as considering safeguards for protecting such data. In fact, to the extent law enforcement and cyber security professionals use publicly available WHOIS data to detect and combat threats to the infrastructure of the DNS, the collection and disclosure of this data to these groups is essential to ICANN's core mandate: the security of the DNS and the Internet. These public and legitimate interests are consistent with the GDPR, which permits processing (including collection) of data where necessary for the performance of a task carried out in the public interest or for the purposes of the legitimate interests pursued by the controller or by a third party, subject to conditions, Art. 6(1)(e) and (f). The third Hamilton memo also supports this conclusion: "Processing of Whois data by law enforcement agencies for such law enforcement purposes should constitute a legitimate interest that motivates processing of personal data in accordance with Article 6.1(f) GDPR. I include below for your reference the corresponding recitals explicitly mention in the GDPR: * "preventing fraud"; * "ensuring network and information security," including the ability of a network or information system to resist "unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services," and * reporting possible "criminal acts or threats to public security" to authorities.	1/13/2018 10:26 AM
4	Assuming registrars ensure that data provided during domain registration is accurate and full, then it can provide an invaluable resource when investigating abuse or criminal activity where the domain was registered by the attacker. Even outside of this, frequently this data can be used to connect an attackers' illegitimate activity to their legitimate activity which can ultimately help with identification of criminals. Similarly, in cases where a legitimate domain is being abused, this data can be used (albeit rarely) to get in contact with the domain owner to inform them of this fact.	1/12/2018 6:10 PM
5	The mission of ICANN and the purpose of DNS is to enable transparency so not only business interests can protect their IP, but consumers can be protected by the very real threats to their privacy and security by those who would impersonate legitimate entities in the attempt to further criminal means. Further limiting this information would eliminate the ability of investigators to reach out to the victims themselves when their infeastructure is compromised.	1/12/2018 5:43 PM

6	Criminal Activity/DNS Abuse - Investigation is NOT a legitimate purpose for requiring collection of registration data. Any additional uses/other purposes for registration data must be specific and legitimate, and only limited data for said specific, legitimate purpose should be provided.	1/12/2018 1:06 PM
7	one purpose of collecting the data is for transparency and accountability purposes. Use for investigations into wrongdoing falls within this purpose.	1/12/2018 12:13 PM
8	Law enforcement and cyber-security professionals rely on registration data as a tool to identify and combat criminal activity and DNS abuse. Although we cannot speak directly on behalf of law enforcement or cyber-security professionals, we understand that, at a minimum, the following data elements would be essential: registrant name, physical address, email address, name servers, registrar name, technical contact (name, address, email, phone), administrative contact (name, address, email, phone).	1/12/2018 11:23 AM
9	I believe more effort should be in clarifying this yet. I dont' have additional information at this time, but I have concerns. The category seems to be too constrained. I believe the title 'Criminal Activity/DNS Abuse' is wrong.. but the concept is right. Especially as this applies to investigation of issues that might NOT be technically 'criminal' in nature, but may be harassing, or socially unacceptable or other 'unwanted' behavior by a segment of the population or groups.. each who might have their own 'investigative' teams.	1/10/2018 3:33 PM
10	Requiring collection of data (including domain contacts) for public safety and legal purposes is as justifiable as for any other purpose, and is allowable under GDPR if balanced against access etc. (Who has access to the data after collection is a separate matter.) Also, it does not make sense to collect relevant data after a problem has occurred -- that would be an impractical and farcical situation. See the third Hamilton memo: "...it would be incorrect to state that the only purpose of the Whois services is to manage domain name registrations.... 2.6.2 Processing of Whois data by law enforcement agencies for such law enforcement purposes should constitute a legitimate interest that motivates processing of personal data in accordance with Article 6.1(f) GDPR. ... [2.7.1] It can be argued that there exists a legitimate interest for entities and private individuals to be able to identify a domain name holder for inter alia the following purposes: (i) In the event of potential fraudulent actions.... (iii) In the event of infringement of copyrights, patents or other intellectual property rights. (iv) In relation to the purchase of goods and services...." Etc.	1/10/2018 11:11 AM