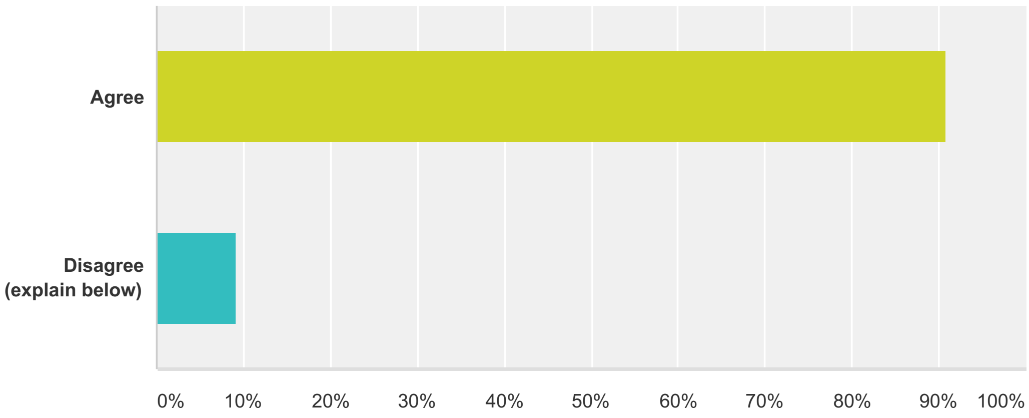
Q1 Your name (must be RDS PDP WG Member - not WG Observer - to participate in polls) If you are a WG Observer and wish to participate in polls, you must upgrade to WG Member to do so.

Answered: 24 Skipped: 0

#	Responses	Date
1	Rod Rasmussen	6/3/2017 12:43 PM
2	Thomas Lancaster	6/3/2017 3:19 AM
3	Rob Golding	6/2/2017 6:08 PM
4	Paul keating	6/2/2017 3:16 PM
5	Roger Carney	6/2/2017 2:13 PM
6	Sara Bockey	6/2/2017 1:12 PM
7	Andrew Sullivan	6/2/2017 12:43 PM
8	Greg Aaron	6/2/2017 12:41 PM
9	Vicky Sheckler	6/1/2017 10:33 AM
10	jonathan matkowsky	6/1/2017 8:05 AM
11	Maxim Alzoba	5/31/2017 2:02 PM
12	Scott Hollenbeck	5/31/2017 9:40 AM
13	Michael Hammer	5/31/2017 7:57 AM
14	Michael Peddemors	5/31/2017 7:56 AM
15	Chuck Gomes	5/31/2017 7:52 AM
16	Sam Lanfranco	5/31/2017 6:46 AM
17	Nathalie Coupet	5/31/2017 6:21 AM
18	John Bambenek	5/31/2017 6:07 AM
19	Patrick Lenihan	5/31/2017 5:34 AM
20	Vlad Dinculescu	5/31/2017 3:25 AM
21	Benny Samuelsen	5/31/2017 12:59 AM
22	Daniel K. Nanghaka	5/31/2017 12:24 AM
23	Tim Chen	5/30/2017 10:35 PM
24	Klaus Stoll	5/30/2017 10:11 PM

Q2 Last week, we discussed EWG principle #41: “A minimum set of data elements, at least in line with the most stringent privacy regime, must be accessible by unauthenticated RDS users.” This week, WG members considered several alternatives based on this EWG principle. After deliberation, WG members expressed support for the following proposed WG agreement; there were no objections raised by those on the call:“At least a defined set of "thin data" elements must be accessible by unauthenticated RDS users.”Please indicate whether you agree with this proposed WG agreement; if not, please explain using the Comment Box.

Answered: 22 Skipped: 2



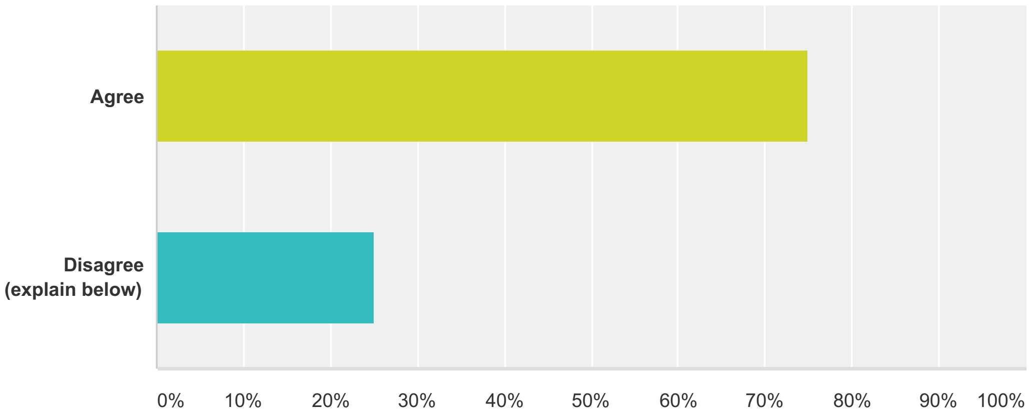
Answer Choices	Responses	
Agree	90.91%	20
Disagree (explain below)	9.09%	2
Total		22

#	Comment Box (use this box to provide rationale or your own alternative)	Date
1	Where "defined set" may be zero elements	6/2/2017 6:08 PM Golding
2	I object to limiting the discussion. No restrictions on access to thin data. I see no reason to restrict thin data and this merely continues the unecessary debate.	6/2/2017 3:16 PM Keating
3	I could live with this but the wording seems redundant, we are defining what thin data is so couldn't we simply say "Thin data must be accessible by unauthenticated RDS users."?	6/2/2017 2:13 PM Carney
4	This is a pretty weak agreement, note. I don't really care except I understand the worry about "most stringent privacy regime".	6/2/2017 12:43 PM Sullivan

5	Anything less than this position opens a pandora's box of implementation complications.	5/31/2017 6:46 AM	Lanfranco
6	Treat all nameserver data as PII and restrict public access accordingly. This will be a victory for privacy advocates everywhere, and will finally solve our privacy problems.	5/30/2017 10:11 PM	Stoll

Q3 Last week, we discussed EWG principle #45, bullet one: “To deter misuse and promote accountability, all data element access must be based on a stated purpose.” This week, WG members considered several alternatives based on this EWG principle. After deliberation, WG members expressed support for the following proposed WG agreement; there were no objections raised by those on the call:“RDS policy must state purpose(s) for public access to 'thin data.'”Please indicate whether you agree with this proposed WG agreement; if not, please explain using the Comment Box.

Answered: 24 Skipped: 0



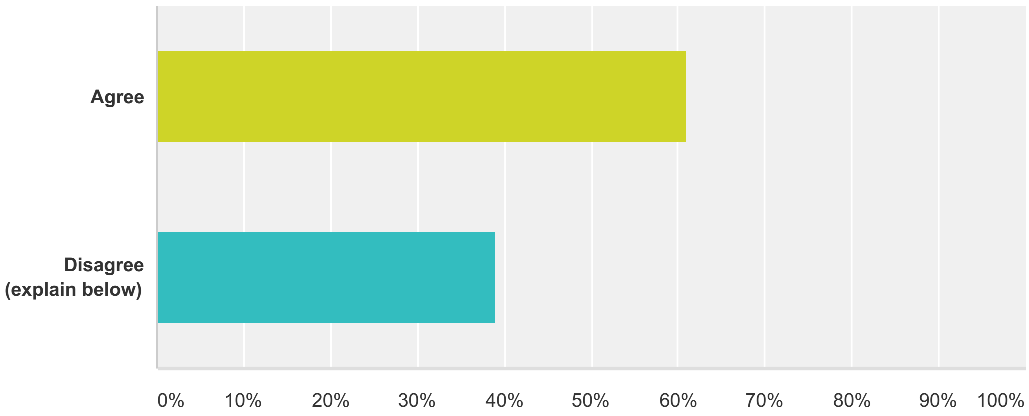
Answer Choices	Responses	
Agree	75.00%	18
Disagree (explain below)	25.00%	6
Total		24

#	Comment Box (use this box to provide rationale or your own alternative)	Date	
1	It is impossible to enumerate all the permissible purposes (a.k.a. uses, current and future). Rather, the goal may be to state some terms that outline prohibited uses. For example the sending of spam.	6/2/2017 12:41 PM	Aaron
2	The question of whether data should be accessible only for specific purposes, and whether the public needs access to the information only arises within the context of pseudonymous or personal data. I can't imagine a justification for us being asked to apply a data minimization principle to all information regardless of whether its an identifier.	6/1/2017 8:05 AM	Matkowsky
3	I think properly worded stated purposes address the concern of some regarding privacy requirements for various jurisdictions.	5/31/2017 7:57 AM	Hammer
4	Prefer SHOULD to MUST	5/31/2017 7:56 AM	Peddemors

5	Identifying the rationale for the fields in the "thin data" makes sense and could be accompanied with an FAQ listing best, and worst, uses of thin data.	5/31/2017 6:46 AM	Lanfranco
6	It is impossible to predetermine all legitimate uses. Even if you could, it is impossible to enforce queries based on legitimate uses. What's the point of stating such requirements if you can't verify or enforce them?	5/31/2017 6:07 AM	Bambenek
7	I disagree with the EWG principle to begin with. Thin data should not be gated in any way. Obviously we have to confirm the thin data elements in this process.	5/30/2017 10:35 PM	Chen

Q4 Last week, we discussed EWG principle #44: “Access must be non-discriminatory (i.e., the process must create a level playing field for all requestors, within the same purpose).” This week, WG members considered several alternatives based on this EWG principle. During deliberation, those on the call expressed both support and opposition to the following proposed WG agreement:"RDS policies for access to "thin data" must be non-discriminatory for all legitimate purposes."Please indicate whether you agree with this proposed WG agreement; if not, please explain using the Comment Box.

Answered: 23 Skipped: 1



Answer Choices	Responses	
Agree	60.87%	14
Disagree (explain below)	39.13%	9
Total		23

#	Comment Box (use this box to provide rationale or your own alternative)	Date
1	Agree with the concept but not the specified wording, there needs to be restrictions based on abuse, confirmed usage, authentication, technologies used etc	6/2/2017 6:08 PM Golding
2	I object to ¨for all legitimate purposes.¨ There should be no limitation.	6/2/2017 3:16 PM Keating
3	I can live with this, but I think it still really does not apply as there is no real way to discriminate if the data is publicly available to anyone.	6/2/2017 2:13 PM Carney
4	This is weak disagreement, but I think this requirement is silly. Since access is unauthenticated, that means anyone can get it, and there's no way to know or discriminate on the basis of purpose. So the requirement is a wheel that does no work.	6/2/2017 12:43 PM Sullivan

5	I agree that access must be non-discriminatory, but I am not sure we need to include "for all legitimate purposes" because this would imposes a data collection principle on data fields that are not personal identifiers.	6/1/2017 8:05 AM	Matkowsky
6	it might be better to finish the suggested line with "when accessed via RDS system", so the policy does not prevent different level of access to the same data via EPP, for example (where speeds of access might be different from public RDS service)	5/31/2017 2:02 PM	Alzoba
7	I am still not comfortable with including the phrase "legitimate purposes". Who decides legitimacy? How does one determine legitimacy of purpose based on a query or request?	5/31/2017 7:57 AM	Hammer
8	"for all legitimate purposes" should not turn into a complicated gated access. Might consider an FAQ approach (see #3 above)	5/31/2017 6:46 AM	Lanfranco
9	Legitimate purposes are not verifiable	5/31/2017 6:21 AM	Coupet
10	Same point as above. This statement is unnecessary based on my position on poll question #3/EWG #45	5/30/2017 10:35 PM	Chen
11	"Legitimate Purposes" need to be clearly defined	5/30/2017 10:11 PM	Stoll

Based on this feedback, here is a possible alternative agreement for WG consideration:

RDS policies for access to "thin data" must be non-discriminatory (i.e., RDS policies must not be designed to give anyone preferential access).