Q1 What is your name?

Answered: 352 Skipped: 0

#	Responses	Date
1	Andrew Ayer	7/7/2015 8:00 PM
2	Anonymous	7/7/2015 7:57 PM
3	d d	7/7/2015 7:19 PM
4	Gary e. Miller	7/7/2015 7:09 PM
5	Homer	7/7/2015 6:40 PM
6	k k	7/7/2015 6:26 PM
7	Drew Bagley, Esq.	7/7/2015 5:56 PM
8	Noam Rabinovich	7/7/2015 5:11 PM
9	Darin Wick	7/7/2015 4:53 PM
10	a	7/7/2015 4:46 PM
11	Joseph Robarts	7/7/2015 4:23 PM
12	dd	7/7/2015 2:15 PM
13	Scott Robison	7/7/2015 2:03 PM
14	b	7/7/2015 1:52 PM
15	John	7/7/2015 1:06 PM
16	Carolyn Wade	7/7/2015 12:25 PM
17	Travis D. Johnson	7/7/2015 12:07 PM
18	Sandy Siththanandan	7/7/2015 11:54 AM
19	Robert Lukitsh	7/7/2015 9:25 AM
20	Stefan Gründer	7/7/2015 6:36 AM
21	Violet	7/7/2015 6:36 AM
22	Geoffrey Thomas	7/7/2015 1:28 AM
23	T. P. Suhr	7/6/2015 10:47 PM
24	Jeremiah Senkpiel	7/6/2015 10:25 PM
25	c.p.g.	7/6/2015 8:37 PM
26	Thomas Smoonlock	7/6/2015 6:36 PM
27	Lara Pollack	7/6/2015 5:44 PM
28	Joseph Robarts	7/6/2015 4:24 PM
29	Luke Lambert	7/6/2015 12:52 PM
30	Elaine Pruis	7/6/2015 11:35 AM
31	Mason Cole	7/6/2015 11:35 AM
32	Shahed Ahmmed	7/6/2015 10:52 AM
33	John T. Patterson	7/6/2015 10:47 AM
34	Dylan Henderson	7/6/2015 10:37 AM
35	vanda scartezini	7/6/2015 10:23 AM
36	Saurabh Pande	7/6/2015 10:16 AM
37	David Li	7/6/2015 10:04 AM
38	Justin	7/6/2015 9:55 AM
39	Michelle Matel	7/6/2015 9:51 AM
40	Justin Steele	7/6/2015 9:51 AM
41	Paul Hart	7/6/2015 8:39 AM
42	Andres Rodriguez	7/6/2015 8:06 AM
43	alisa harris	7/6/2015 7:24 AM
44	Gladys Portales	7/6/2015 4:09 AM
45	Adam Miller	7/6/2015 3:14 AM
46	Robert	7/6/2015 3:10 AM
47	Alessandro Strada	7/6/2015 3:02 AM
48	Rohit Bhute	7/6/2015 2:32 AM
49	Jody Frankowski	7/6/2015 1:59 AM

50	tyh	7/6/2015 1:13 AM
51	Darin McGill	7/6/2015 12:52 AM
52	Byunghoon Choi	7/5/2015 11:58 PM
53	Duncan Burke	7/5/2015 10:51 PM
54	Charles	7/5/2015 8:23 PM
55	Sebastien Brossier	7/5/2015 5:22 PM
56	Pedro Valles	7/5/2015 3:32 PM
57	John Carr	7/5/2015 12:09 PM
58	Michelle Knight	7/5/2015 2:22 AM
59	Tim Kramer	7/5/2015 2:06 AM
60	Michael Ho	7/5/2015 1:36 AM
61	Aaron Adams	7/5/2015 12:03 AM
62	Hannah Ellison	7/4/2015 2:31 PM
63	steve smith	7/4/2015 1:31 PM
64	Cory Myers	7/4/2015 1:00 PM
65	Alex Bennett	7/4/2015 12:25 PM
66	Rob Vonderhaar	7/4/2015 1:47 AM
67	Andrew Merenbach	7/4/2015 1:09 AM
68	Craig Hartnett	7/3/2015 11:23 PM
69	Joseph Robarts	7/3/2015 6:26 PM
70	Robin Adrianse	7/3/2015 4:25 PM
71	Jawala	7/2/2015 6:37 PM
72	Jarett Millard	7/2/2015 5:50 PM
73	Kat Walsh	7/2/2015 4:35 PM
74	Marius Gavrilescu	7/2/2015 1:21 PM
75	Callen Shaw	7/2/2015 12:49 PM
76	Ann Bouchard	7/2/2015 12:43 PM
77	Aaron Dalton	7/2/2015 9:18 AM
78	Stephen Black Wolf	7/2/2015 8:41 AM
79	Iain McNeil	7/2/2015 6:16 AM
80	Marek Teichmann	7/2/2015 4:31 AM
81	David Wyn Davies	7/2/2015 3:34 AM
82	Jason Jacyszyn	7/2/2015 1:02 AM
83	Lucien Parsons	7/1/2015 9:09 PM
84	Ron Farage	7/1/2015 7:25 PM
85	Gabby Taylor	7/1/2015 7:09 PM
86	M. B.	7/1/2015 6:50 PM
87	Nicole Mirror	7/1/2015 6:37 PM
88	Adam Creighton	7/1/2015 6:33 PM
89	Chris	7/1/2015 6:01 PM
90	Cory Weaver	7/1/2015 5:49 PM
91	Reid Baker	7/1/2015 4:52 PM
92	Tim Mensch	7/1/2015 4:32 PM
93	Bruno Aguiar de Melo	7/1/2015 4:08 PM
94	Andrew Friedman	7/1/2015 3:43 PM
95	Nalle Söderholm	7/1/2015 3:42 PM
96	Belinda Van Sickle	7/1/2015 3:24 PM
97	Kathy	7/1/2015 2:12 PM
98	Adrian James	7/1/2015 8:53 AM
99	Jessica Gockley	7/1/2015 8:45 AM
100	Arthur Zonnenberg	7/1/2015 8:17 AM
101	Bertrand Siffert	7/1/2015 6:01 AM
102	Baylis Shanks	7/1/2015 4:45 AM
103	Mario Heilmann	7/1/2015 4:14 AM

104	Ryan Kozak	7/1/2015 2:40 AM
105	C	6/30/2015 10:41 PM
106	Sam Willardstone	6/30/2015 9:53 PM
107	Noah Greenstein	6/30/2015 9:14 PM
108	Roman Ivanov	6/30/2015 7:15 PM
109	Nicol	6/30/2015 7:10 PM
110	Nicol	6/30/2015 7:05 PM
111	Birger Schacht	6/30/2015 2:50 PM
112	Trevor D. Cook	6/30/2015 1:03 PM
113	Anand S	6/30/2015 10:36 AM
114	Jonathan C	6/30/2015 7:49 AM
115	Nicolai Pogadl	6/30/2015 7:00 AM
116	Sam Fu	6/30/2015 6:51 AM
117	Aitor Zabala	6/30/2015 4:32 AM
118	Adam Wilcox	6/29/2015 6:25 PM
119	Barry Brown	6/29/2015 4:12 PM
120	Eric Entzel	6/29/2015 3:52 PM
121	Robert Sternbaum	6/29/2015 3:41 PM
122	Jason Burns	6/29/2015 3:01 PM
123	Alexander Lent	6/29/2015 2:51 PM
124	John Stetson	6/29/2015 2:08 PM
125	John Stetson	6/29/2015 2:08 PM
126	Mitchell	6/29/2015 1:28 PM
127	Lucas Stadler	6/29/2015 1:01 PM
128	Sean	6/29/2015 9:42 AM
129	Leah B	6/29/2015 9:26 AM
130	Cosimo	6/29/2015 9:19 AM
131	Denton Jacobs	6/29/2015 8:59 AM
132	Drew Mayo	6/29/2015 8:16 AM
133	Jason Weinberg	6/29/2015 7:32 AM
134	Gregory Antonellis	6/29/2015 7:03 AM
135	Ben Bullock	6/29/2015 6:53 AM
136	Jeff	6/29/2015 5:51 AM
137	Eugene Koller	6/29/2015 5:39 AM
138	Nicholas Helke	6/29/2015 5:09 AM
139	Puneeth	6/29/2015 4:31 AM
140	Filipe Rodrigues	6/29/2015 4:30 AM
141	Hardi Kõvamees	6/29/2015 3:09 AM
142	Joe	6/29/2015 2:54 AM
143	Markus Ewald	6/29/2015 2:45 AM
144	Mike	6/29/2015 2:42 AM
145	Terence Kennedy	6/29/2015 2:05 AM
146	Shane T	6/29/2015 12:07 AM
147	Ben Bowman	6/29/2015 12:01 AM
148	Sander Venneslan	6/28/2015 11:44 PM
149	Jeremy	6/28/2015 11:35 PM
150	Clayton Falzone	6/28/2015 11:06 PM
151	Henry Todd	6/28/2015 10:28 PM
152	Dave	6/28/2015 10:20 PM
153	anon	6/28/2015 9:40 PM
154	Jason Owen	6/28/2015 9:28 PM
155	Kevin Zheng	6/28/2015 9:01 PM
156	anon	6/28/2015 8:44 PM
157	John Smith	6/28/2015 8:30 PM

158	Scott Jordan	6/28/2015 8:25 PM
159	Finn Ellis	6/28/2015 8:23 PM
160	Alex Wyndham	6/28/2015 6:47 PM
161	Robin Hood	6/28/2015 6:36 PM
162	Nikolaj Balin	6/28/2015 6:14 PM
163	Allen	6/28/2015 6:09 PM
164	Aaron Holmes	6/28/2015 5:51 PM
165	Aaron Rainbolt	6/28/2015 5:48 PM
166	Dan Stutzman	6/28/2015 4:45 PM
167	Alan	6/28/2015 4:40 PM
168	Test	6/28/2015 4:24 PM
169	Nick O'Dell	6/28/2015 4:13 PM
170	Raya Desawade	6/28/2015 3:40 PM
171	Jo	6/28/2015 3:38 PM
172	Koop Lawson	6/28/2015 3:12 PM
173	Robin Ertbernine	6/28/2015 3:07 PM
174	Frank	6/28/2015 2:42 PM
175	Jeb Rosen	6/28/2015 2:27 PM
176	Charles	6/28/2015 1:56 PM
177	Rhonda Holscher	6/28/2015 1:54 PM
178	Anonymous Turtle	6/28/2015 1:50 PM
179	Private	6/28/2015 1:46 PM
180	Philipp Antoni	6/28/2015 1:45 PM
181	Steven Marcalain	6/28/2015 1:44 PM
182	Kenneth Godwin	6/28/2015 1:20 PM
183	James Bergstrom	6/28/2015 1:16 PM
184	Pepe	6/28/2015 12:59 PM
185	Daniel Langer	6/28/2015 12:51 PM
186	Thorin Faulk	6/28/2015 12:38 PM
187	Lucas Szwarcberg	6/28/2015 12:27 PM
188	Alex Xu	6/28/2015 12:22 PM
189	Michael O.	6/28/2015 12:22 PM
190	Gregory Leffler	6/28/2015 12:07 PM
191	David	6/28/2015 11:42 AM
192	Cort Wee	6/28/2015 11:35 AM
193	Andres Rama	6/28/2015 11:33 AM
194	Jason L. Shiffer	6/28/2015 11:33 AM
195	Ben Hass	6/28/2015 11:23 AM
196	Paul	6/28/2015 11:19 AM
197	Matthew R. Steno	6/28/2015 11:05 AM
198	Steve	6/28/2015 10:59 AM
199	Jeffrey I. Schiller	6/28/2015 10:43 AM
200	Marty Dill	6/28/2015 10:37 AM
201	Stuart Axon	6/28/2015 10:13 AM
202	D. Miedema	6/28/2015 10:08 AM
203	-	6/28/2015 10:05 AM
204	Jesus H	6/28/2015 9:57 AM
205	Harish	6/28/2015 9:56 AM
206	Joe	6/28/2015 9:20 AM
207	Dirk Kelly	6/28/2015 9:15 AM
208	Thomas Forbes	6/28/2015 9:09 AM
209	Steve Jackson	6/28/2015 8:41 AM
210	That's exactly what's none of your business here.	6/28/2015 8:23 AM
211	Ben Neades	6/28/2015 8:16 AM

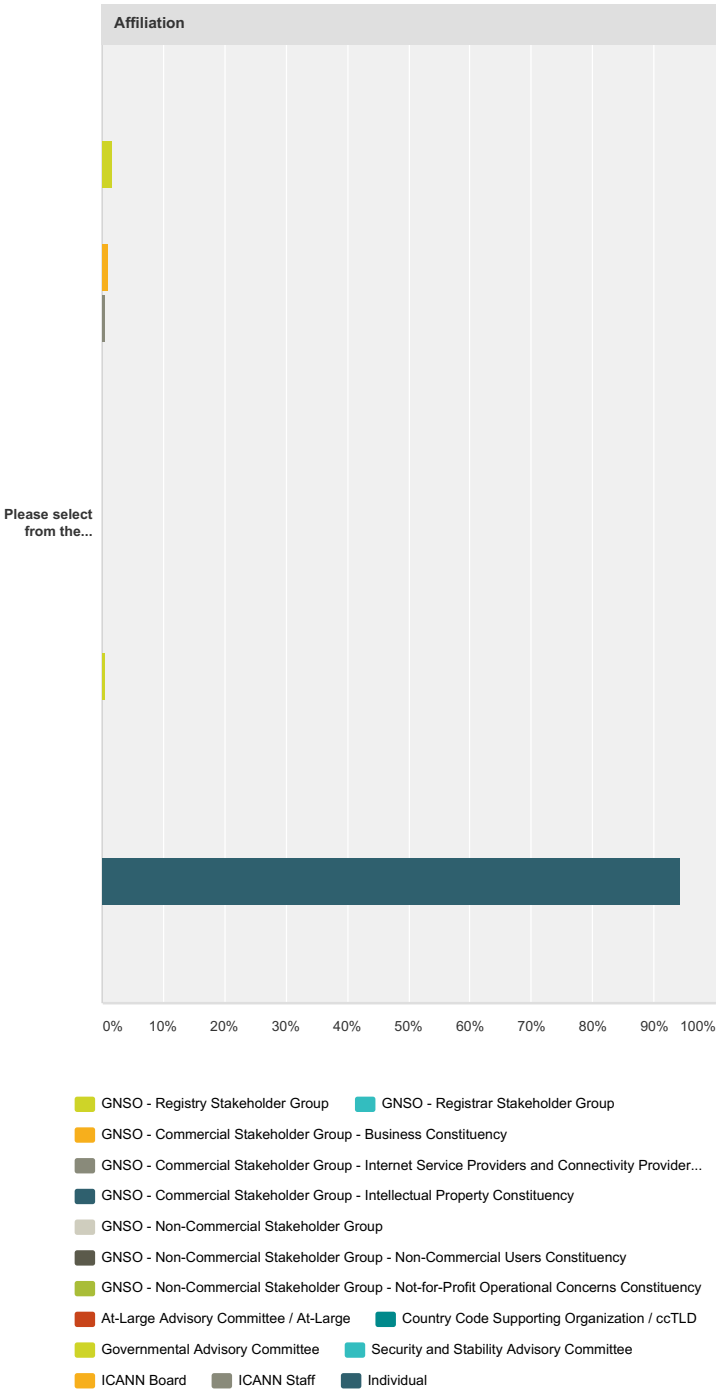
212	dsadsdas dasa	6/28/2015 7:54 AM
213	Pirijan Ketheswaran	6/28/2015 7:48 AM
214	Hugo Jobling	6/28/2015 7:47 AM
215	Christopher Smith	6/28/2015 7:42 AM
216	Andres Perez	6/28/2015 7:30 AM
217	Ivan Timokhin	6/28/2015 7:21 AM
218	Ashley	6/28/2015 7:16 AM
219	Emil Rivera	6/28/2015 7:07 AM
220	Henrik Olsen Grimestad	6/28/2015 6:40 AM
221	R. Poss	6/28/2015 6:12 AM
222	Paul Robenson	6/28/2015 6:06 AM
223	Amal Raj	6/28/2015 6:02 AM
224	Russell Wallace	6/28/2015 5:57 AM
225	Fg	6/28/2015 5:44 AM
226	Shantanu Gupta	6/28/2015 5:06 AM
227	Sam P.	6/28/2015 5:04 AM
228	Petter Fuling	6/28/2015 4:41 AM
229	Petter Fuling	6/28/2015 4:39 AM
230	Aaron Emigh	6/28/2015 4:19 AM
231	TS	6/28/2015 4:11 AM
232	Vasian	6/28/2015 4:10 AM
233	John Berry	6/28/2015 4:09 AM
234	Ryan Scheel	6/28/2015 3:47 AM
235	Simon Kissane	6/28/2015 3:36 AM
236	Killian De Volder	6/28/2015 3:30 AM
237	Tommy	6/28/2015 3:30 AM
238	Nicola Paolucci	6/28/2015 3:25 AM
239	Brian Manton	6/28/2015 3:12 AM
240	James Ford	6/28/2015 3:03 AM
241	Jim Thorpe	6/28/2015 3:02 AM
242	Andrew Munsell	6/28/2015 2:58 AM
243	Not your business.	6/28/2015 2:57 AM
244	Gabriel De Luca	6/28/2015 2:53 AM
245	Jiulun Du	6/28/2015 2:41 AM
246	Scott McClung	6/28/2015 2:39 AM
247	gfd djjkk	6/28/2015 2:29 AM
248	Abhijit Menon-Sen	6/28/2015 2:14 AM
249	Tiru Srikantha	6/28/2015 1:38 AM
250	Antoine Roy-Gobeil	6/28/2015 1:31 AM
251	Philip Hooge	6/28/2015 12:58 AM
252	Reginald A Carey	6/27/2015 10:30 PM
253	John Doe	6/27/2015 9:49 PM
254	Jimmy Hastings	6/27/2015 8:44 PM
255	Christopher	6/27/2015 6:18 PM
256	Sperry Russ	6/27/2015 5:45 PM
257	Joey Foo	6/27/2015 3:43 PM
258	name witheld	6/27/2015 12:24 PM
259	Kevin Szprychel	6/27/2015 12:23 PM
260	Dusty Carrier	6/27/2015 11:51 AM
261	Sylvain Chevalier	6/27/2015 11:12 AM
262	Lauren Ellenberg	6/27/2015 8:32 AM
263	Zak Millar	6/27/2015 5:57 AM
264	Graeme Pietersz	6/27/2015 5:13 AM
265	A W	6/27/2015 2:29 AM

266	Aaron Mason	6/26/2015 11:47 PM
267	Lisa Ugray	6/26/2015 11:27 PM
268	Arturo Rangel	6/26/2015 10:41 PM
269	Gabe Edwards	6/26/2015 10:20 PM
270	Miquel Burns	6/26/2015 10:15 PM
271	VInce Mammoth	6/26/2015 8:22 PM
272	Michael DeWaal	6/26/2015 6:30 PM
273	Peter Hancock	6/26/2015 2:49 PM
274	Brook	6/26/2015 1:55 PM
275	Richard Craig	6/26/2015 1:37 PM
276	Adrian Valeriu Ispas	6/26/2015 12:47 PM
277	Dan M	6/26/2015 11:49 AM
278	Lee Holland	6/26/2015 10:01 AM
279	Scott Parker	6/26/2015 8:04 AM
280	Brian Renak	6/26/2015 6:58 AM
281	Dave Stead	6/26/2015 6:38 AM
282	Stepan Dousek	6/26/2015 5:13 AM
283	Mike Darby	6/26/2015 3:51 AM
284	Sam	6/26/2015 3:49 AM
285	Marc Whittemore	6/26/2015 2:40 AM
286	Steve gunther	6/26/2015 1:30 AM
287	Kenneth Jarvis	6/26/2015 1:11 AM
288	Anon	6/26/2015 12:45 AM
289	Rahman Mahmoud	6/25/2015 9:21 PM
290	Jason Linz	6/25/2015 9:18 PM
291	Douglas Allen	6/25/2015 9:17 PM
292	Arin Bakht	6/25/2015 8:57 PM
293	Omar Ray	6/25/2015 8:25 PM
294	Editeur	6/25/2015 8:21 PM
295	Charles Demers	6/25/2015 7:20 PM
296	Joseph Robarts	6/25/2015 6:51 PM
297	Josh Hancock	6/25/2015 6:50 PM
298	Mike Fewings	6/25/2015 6:14 PM
299	Bill Rookard	6/25/2015 5:03 PM
300	David Garfield	6/25/2015 4:27 PM
301	test	6/25/2015 3:37 PM
302	Daniel Bahlert	6/25/2015 3:32 PM
303	Tom Ledoux	6/25/2015 3:29 PM
304	Marc Schauber	6/25/2015 3:21 PM
305	Royce Whitaker	6/25/2015 3:21 PM
306	J Wilson	6/25/2015 2:53 PM
307	Dr. M. Klinefelter	6/25/2015 2:34 PM
308	Patrick	6/25/2015 1:29 PM
309	Joe Sondow	6/25/2015 1:12 PM
310	William Ramirez	6/25/2015 12:49 PM
311	Ryan Gard	6/25/2015 9:01 AM
312	Pierre Far	6/25/2015 7:25 AM
313	Joseph Williams	6/24/2015 8:39 PM
314	Janice	6/24/2015 8:04 PM
315	Andrew Rueckert	6/24/2015 7:50 PM
316	Michael Ekstrand	6/24/2015 7:44 PM
317	Stu George	6/24/2015 7:24 PM
318	Tina S.	6/24/2015 6:45 PM
319	B Bradford	6/24/2015 4:24 PM

320	Maeve Garigan	6/24/2015 3:05 PM
321	Zoe Quinn	6/24/2015 2:34 PM
322	Brent Heuss	6/24/2015 2:13 PM
323	Terri Stumme	6/24/2015 1:21 PM
324	Rachel Whitlatch	6/24/2015 1:12 PM
325	Misti Wolanski	6/24/2015 12:38 PM
326	Gen Mail	6/24/2015 11:18 AM
327	Roxana	6/24/2015 11:02 AM
328	Karen	6/24/2015 10:53 AM
329	Luis	6/24/2015 10:06 AM
330	Dan Balla	6/24/2015 9:39 AM
331	Daniel Klan Mc Kiernan	6/24/2015 2:06 AM
332	Misha Stevens	6/24/2015 12:45 AM
333	koen jacobs	6/24/2015 12:15 AM
334	Emma Johnson	6/23/2015 1:06 PM
335	james	6/23/2015 11:21 AM
336	Jeff Walsh	6/22/2015 6:43 PM
337	Alex K	6/22/2015 3:09 PM
338	Richard Ober	6/22/2015 2:45 PM
339	Doug Gimenez	6/22/2015 2:44 PM
340	Mariana Martínez	6/22/2015 1:28 PM
341	Reagan Lynch	6/22/2015 12:00 PM
342	Michael Cariaso	6/22/2015 11:53 AM
343	Leah Bozhilova	6/22/2015 8:09 AM
344	Kelly Andersson	6/21/2015 7:04 PM
345	John Lawrence	6/20/2015 10:00 PM
346	Liam	6/20/2015 2:09 PM
347	Terri Stumme	6/18/2015 9:49 AM
348	CUI	6/8/2015 2:50 AM
349	g	6/1/2015 4:29 PM
350	devendrra	5/20/2015 2:10 AM
351	ll	5/6/2015 2:44 PM
352	thin	5/5/2015 6:45 PM

Q2 What is your affiliation (e.g. name of ICANN Supporting Organization, Advisory Committee, Stakeholder Group, Constituency, individual)

Answered: 352 Skipped: 0



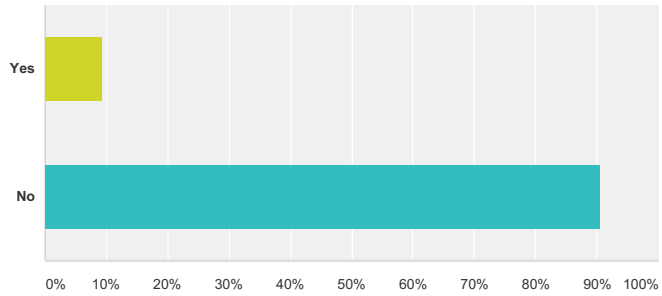
Affiliation	GNSO - Registry Stakeholder Group	GNSO - Registrar Stakeholder Group	GNSO - Commercial Stakeholder Group - Business Constituency	GNSO - Commercial Stakeholder Group - Internet Service Providers and Connectivity Providers	GNSO - Commercial Stakeholder Group - Intellectual Property Constituency	GNSO - Non-Commercial Stakeholder Group	GNSO - Non-Commercial Stakeholder Group - Non-Commercial Users Constituency	GNSO - Non-Commercial Stakeholder Group - Not-for-Profit Operational Concerns Constituency	At-Large Advisory Committee / At-Large	Country Code Supporting Organization / ccTLD	Governmental Advisory Committee	Security and Stability Advisory Committee	ICAN Boar

Please select from the drop-down menu	**1.70%** 6	**0.28%** 1	**1.14%** 4	**0.57%** 2	**0.28%** 1	**0.28%** 1	**0.28%** 1	**0.00%** 0	**0.28%** 1	**0.00%** 0	**0.57%** 2	**0.00%** 0	**0.00**

#	Other (please specify)	Date
1	Secure Domain Foundation	7/7/2015 5:56 PM
2	Fraud detection company	7/7/2015 5:11 PM
3	sd	7/7/2015 2:15 PM
4	Donuts	7/6/2015 11:35 AM
5	Donuts Inc.	7/6/2015 11:35 AM
6	Children's Rights NGO	7/5/2015 12:09 PM
7	Senior legal counsel	7/1/2015 6:01 AM
8	NearlyFreeSpeech.net Customer	6/30/2015 10:41 PM
9	cyber security professional	6/29/2015 7:03 AM
10	Website owner, software engineer	6/28/2015 11:23 AM
11	Jeffries	6/28/2015 9:20 AM
12	Domain owner	6/28/2015 8:23 AM
13	I hold several domains	6/27/2015 12:24 PM
14	CTO/COO of Federally Certified Woman Owned Business	6/26/2015 6:30 PM
15	Poesies.net	6/25/2015 8:21 PM
16	Cofounder of Crash Override Network	6/24/2015 2:34 PM
17	individual	6/24/2015 12:15 AM
18	Web developer/manager for 30+ clients	6/21/2015 7:04 PM
19	domain name dispute resolution service provider ADNDRC Beijing Office	6/8/2015 2:50 AM

Q3 Are you completing this survey on behalf of your group? If yes, please specify which group if different from your listed affiliation.

Answered: 343 Skipped: 9

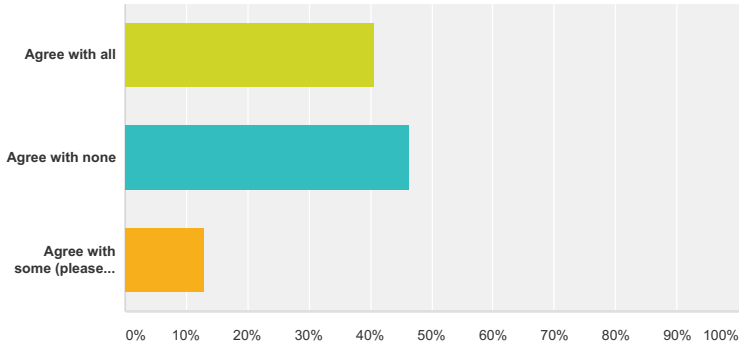


Answer Choices	Responses	
Yes	**9.33%**	32
No	**90.67%**	311
Total		**343**

#	If yes, please specify which group if different from your listed affiliation.	Date
1	EverCompliant	7/7/2015 5:11 PM
2	International AntiCounterfeiting Coalition	7/7/2015 12:07 PM
3	Donuts Inc.	7/6/2015 11:35 AM
4	Children's Charities' Coalition on Internet Safety	7/5/2015 12:09 PM
5	My company - Slitherine Ltd	7/2/2015 6:16 AM
6	IGDA	7/1/2015 4:08 PM
7	cbits.net	7/1/2015 8:53 AM
8	NearlyFreeSpeech.net Customer	6/30/2015 10:41 PM
9	The american people	6/29/2015 7:32 AM
10	humans	6/28/2015 6:36 PM
11	Online Privacy	6/27/2015 9:49 PM
12	Private, woman owned business	6/26/2015 6:30 PM
13	LegitScript, LLC	6/18/2015 9:49 AM

Q4 Please indicate if you agree or disagree with the WG's recommended definitions for the following terms: Disclosure, Publication, Person, Law Enforcement Authority, Relay, Requester (Section 1.3.1 Recommendation 1).

Answered: 140 Skipped: 212



Answer Choices	Responses	
Agree with all	**40.71%**	57
Agree with none	**46.43%**	65
Agree with some (please indicate which you agree and disagree with, and if possible, why, in the box below)	**12.86%**	18
Total		**140**

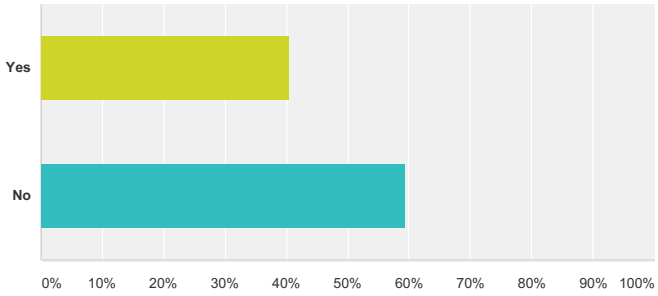
#	Additional Comments	Date
1	Please add a definition for Privacy and a definition for Proxy services.	7/6/2015 11:43 AM
2	clear statements. No need to rewrite.	7/6/2015 10:33 AM
3	While the other definitions are reasonable, the definition of "Law Enforcement Authority" fails to define "or similar authorities designated from time to time"; it also fails to define "jurisdiction" as to level (in the United States, local, state or federal; presumably any level of government can designate any authority for the purpose of this definition.	7/5/2015 1:46 AM
4	This seems fine in general, though I worry about the breadth of "other similar" in the definition of "Law Enforcement Authority" being extended to cover private parties with only thin connections to legitimate government action.	7/2/2015 4:55 PM
5	The definition for "law enforcement authority" is insanely broad. What does a "quasi-governmental" authority even look like? And while we're on the topic, "publication" is problematic because I see no reason for a public WHOIS database anyway.	7/2/2015 9:25 AM
6	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
7	I do not know about all the provisions and recommendations. I only know that I am utterly opposed to my information being available on the Internet to anyone who has access to a computer! Please maintain the privacy of the individual/businessowner who opts for privacy!!!	7/1/2015 6:57 PM
8	I own a woman-owned home-based business in the video game industry. I am also the Executive Director of 501c(3) non-profit professional organization for women working in video games. Women in my industry have been the target of death threats, rape threats, threats to their families and homes by people with access to home addresses through domain name registration. I have had domain names for my business and my non-profit registered to my address since 2005. It is imperative that criminals and the insane do not have access to my home address through ICANN. The FBI has been following my colleagues to protect them from potential murder and rape due to these threats. Do not be a part of the disclosure of personally identifying information that could lead to the worst kinds of personal crime and death. The liability for ICANN is huge.	7/1/2015 3:29 PM
9	1) Lack of privacy is life threatening. Even Europe and Canada have hate speech laws that outlaw basic free speech. Not even to mention the majority of undemocratic countries. Free private speech is an overriding good. 2) All emails I ever published on whois are spammed to death to the point of being useless. If someone notifies me, I will not notice. Private registration mostly gets respected by spammers. Spam is extremely serious as it disrupts normal channels of communication. 3) Even commercial providers can have an interest in provacy. They might be selling books, or sex toys. Or gay literature in countries where such endeavor carries a death penalty. 4) if it ain't broke, don't fix it. Leave as is.	7/1/2015 4:48 AM
10	Stop trying to break a system that is working fine already.	6/29/2015 2:10 PM
11	I disagree with the definition of Law Enforcement Authority (hereafter LEA) as being too vague and requiring too much interpretation. Providing and interpreting a definition of LEA is outside of ICANN's scope and area of expertise. It is my opinion that rather than provide, maintain and interpret a definition of LEA, ICANN should instead make a reference to a list, compilation of lists or some other collection defined and maintained by some other authority or authorities that specialize in that subject matter.	6/29/2015 7:41 AM

12	There should be no back door requirements to disclose information to any outside party. It should be wholly up to the provider of the service to follow the law as written when disclosing a users information. It should not be based on accreditation standards.	6/29/2015 7:38 AM
13	Don't dignify the assertion that corporations and other commercial organizations are people.	6/28/2015 8:34 PM
14	Go fuck yourself.	6/28/2015 6:40 PM
15	I especially disagree with the following: 1) Mandatory disclosure to law enforcement: I can only see this being abused. Most privacy services will be run by people that understand when a request is pertinent to a dangerous situation and when it is simply abusive and refuse to service the request. This is a feature, not a bug. If the LEA has a court order, then an impartial judge has decided that the officer isn't being abusive. 2) I disagree with ICANN dictating policy based on the content of the website in question. While I understand that for a long time, .com and .org were separate based on whether the organization registering them was a non-profit, that barrier has long fallen. The beauty of the internet is how people can use it without being stuffed into little boxes set created by someone else. 3) This policy severely compromises the ability of anyone who needs privacy or simply wants privacy to speak their mind. Government dissidents, members of LGBT communities overseas, anyone speaking truth to power or refusing to hide will be uncovered worldwide unless they happen to be a member of a corporation that has front office. The impact is disproportionately on individuals rather than companies.	6/28/2015 1:58 PM
16	With regards to private and public domain registration services. With the rise of digital organizations that are dedicated to causing havoc and mischief, a system that allows almost any individual with a nicely formatted letter, and or convincingly spoofed email, to reveal critically private information for individuals without a legal department would be devastating to home businesses and those that use the domain name system in a more professional than private manner.	6/28/2015 11:12 AM
17	If you handle registrant privacy, freedom, and information like a police state, you lose any moral ground. People will not trust you, and you will force behavior that will make new industries and services based on avoiding illegal and unethical practices by your company and those you work with/for. Your reputation is on the line. If people do not want to be tracked or evaluated by unelected private companies, they have every moral and ethical right to do so. The free market will remain free. Freedom and privacy will win. The police state will be navigated around at all costs. You are either for freedom and privacy or against it. there is not middle ground.	6/28/2015 7:49 AM
18	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:14 AM
19	A privacy provider should be allowed to refuse disclosure except when required by compulsory legal process (warrant, subpoena, court order, or other binding legal process it is required to comply with by the jurisdiction in which it operates.) It should be allowed to refuse any requests by law enforcement to not notify the customer of the disclosure whenever those requests are not legally obligatory. Members of the public deserve the full protection of their privacy available under the law and it is wrong for ICANN to try to mandate less privacy protections than the law itself provides.	6/28/2015 3:45 AM
20	I don't believe that you should have to disclose your personal identity to the whole world just to get a domain name for your blog or other personal website. And I don't believe that there should be a means of forcing the disclosure of personal identity without a court process. Or that whois records should include personally identifiable information. Or that domain registrars should be required to obtain personally identifying information from customers. If someone wants to buy a domain with bitcoin, and not identify themselves beyond an email like "someguy@example.com" it should more than sufficient. Frankly, I don't think Whois makes any sense. There should be some kind of DNS record for domain contact that just lists an email address and the rest of Whois ought to be just completely killed off.	6/28/2015 3:18 AM
21	Law enforcement requests should come with judicial warrants.	6/28/2015 3:11 AM
22	KEEP WHOIS PRIVACY SERVICES ALIVE. Do NOT kill online privacy! Respect being anonymous!	6/27/2015 9:51 PM
23	Disagree with quasi-governments being considered law enforcement authority.	6/27/2015 7:10 PM
24	I oppose the current proposals to change the privacy disclosure to what ICANN is is proposing. If we are paying for privacy then that is what we should get, privacy period.	6/27/2015 5:48 PM
25	ICANN itself is hypocritical on the definitions: Nor does ICANN not follow it's own rules on WHOIS entires. Person seems to have changed meaning so it doesn't mean person anymore - it can be 'domain administrator' ICANS own whois (on http://whois.icann.org/en/lookup?name=icann.org) Name: Domain Administrator Organization: ICANN Mailing Address: 12025 Waterfront Drive, Los Angeles California 90094-2536 US Phone: +1.4242171313 from https://www.icann.org/en/system/files/files/approved-with-specs-27jun13-en.pdf p6 Registration Directory Whois Specification Registry Registrant ID: 5372808-ERL3 Registrant Name: EXAMPLE REGISTRANT4 Registrant Organization: EXAMPLE ORGANIZATION Registrant Street: 123 EXAMPLE STREET Registrant City: ANYTOWN Registrant State/Province: AP5 Registrant Postal Code: A1A1A16 Registrant Country: AA Registrant Phone: +1.5555551212 Registrant Phone Ext: 12347 Registrant Fax: +1.5555551213 Registrant Fax Ext: 4321 Registrant Email: EMAIL@EXAMPLE.TLD Registry Admin ID: 5372809-ERL8 1 Data element may be deleted, provided that if the data element is used, it must appear at this location. 2 Note: all applicable statuses must be displayed in the Whois output. 3 May be left blank if not available from Registry. 4 For the Registrant, Admin and Tech contact fields requiring a “Name” or “Organization”, the output must include either the name or organization (or both, if available). Note point #4 well - ICANN's entry for registrant, admin and technical contact is set to "Domain Administrator" That is is neither a person nor an organization (or both) - and certainly is not the contact for all three. So ICANN want to inflict rules upon the rest of us that they don't even do themseleves.	6/27/2015 12:56 PM
26	I disagree with the “Law enforcement authority” (because the definition is too broad, including "quasi–governmental authorities"), and I agree with all other terms definition.	6/26/2015 12:54 PM
27	I am contented with the WG dealing with some of the chartered questions. But I disagree with their assessment and proposed resolution involving, "provider obligations in relation to "relay" and "reveal" procedures to handle requests for the disclosure of a privacy/proxy customer's identity and contact details." There should be no instances except under a sanctioned court order that anyone's private information is made public to any form. It violates due process, is blatant privacy infringement, and endangers millions of domain registrars and domain owners by enabling personal information to be available not only unnecessarily but also irrelevantly pertaining to their website or business. It is both directly and indirectly harmful and dangerous.	6/26/2015 12:05 PM
28	The internet has become too much of an important utility for the world. You cannot start now to only care about the interests of a few anti piracy groups. There are way too many other groups that are also not even pirates who need to have privacy. Please for the love of god leave it to the individual countries and local laws to deal with this stuff. Your fatcat, anti piracy totalitarians are not the only ones on the block with an interest. It shouldnt be your job. Please just stay out of it and remain neutral.	6/26/2015 12:50 AM
29	You've made this public comment form too complicated and neglected to show the sections you are referring to as part of the question.	6/25/2015 3:35 PM

30	What kind of survey does NOT allow me to DISAGREE I do not think ICANN should change ANYTHING, except: 1. To insist that GoDaddy provide authorized 3rd party WHOIS services with all WHOIS information rather than a link to their site. For example in the link below WHO.IS are unable to publish the complete information and the user is FORCED to go to GoDaddy. http://www.who.is/whois/oxcars.com I also think that ALL WHOIS providers should protect the data from bots by masking the email address with a long graphic, it is not sufficient to put a capcha as there are automated capacha systems What is wrong is that some of the services, specifically Domains by Proxy, Melbourne IT and the one in Panama, do NOT properly respond when you tell them that the domain has been used for spamming. I think they should simply cease providing the privacy service if Spamcop and Spamhaus havce sufficient human reports of spam (not automated or ticks, a proper copy of header and email reported to said companies).	6/25/2015 2:58 PM
31	Protect our privacy. The burden for small business owners to provide their home address to the public is crazy! This proposal is narrow minded, and does not take into consideration the small players.	6/24/2015 10:10 AM
32	Disagree with disclosure of contact information. Identity theft is rampant and by disclosing contact information will only add to the problem.	6/24/2015 9:50 AM
33	Disagree with: A) ICANN should publish and maintain a publicly accessible list of all accredited P/P service providers, with all appropriate contact information. Registrars should provide a web link to P/P services run by them or their Affiliates, and P/P service providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program. No. ICANN should not publish such a list. 'Commercial activities' is too broad, to vague, and to static. My own domains have in the past, and in the future may continue to switch between commercial and non-commercial. B) Should registrants of domain names associated with commercial activities and which are used for online financial transactions be prohibited from using, or continuing to use, P/P services? If so, why, and if not, why not? No. Consumers are able to determine which domains do provide this information, and choose who to conduct business with. ICANN should be a 'Good Housekeeping Seal' not a police force.	6/22/2015 12:05 PM
34	Private proxy registration makes it exceedingly difficult, time-consuming, and clost-prohibitive to pursue a copyright infringement claim. BUT -- for individual private "bloggers" with a "personal" website, eliminating private registration exposes millions of part-time hobbyist individuals to invasion of privacy and has a chilling effect on their online publication goals and pursuits.	6/21/2015 7:16 PM

Q5 Do you agree with the WG's recommendation that privacy and proxy services should be treated the same way for the purpose of the accreditation process? (Section 1.3.1 Recommendation 2, and Section 7.1, Category A)

Answered: 131 Skipped: 221



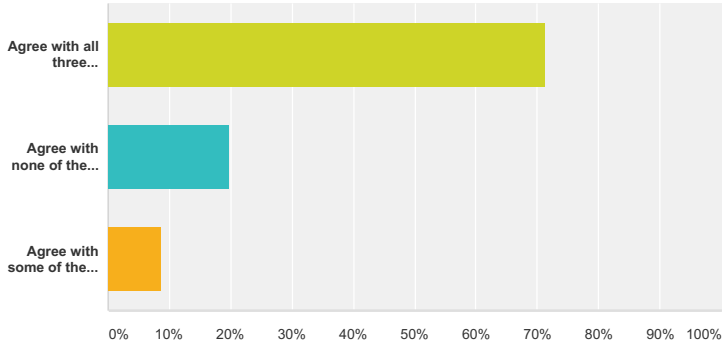
Answer Choices	Responses	
Yes	**40.46%**	53
No	**59.54%**	78
Total		**131**

#	Additional Comments	Date
1	accreditation process provides a guarantee to registrants that registrars are following correct processes and are responsible to the services they are providing. P/P services has similar relevance than other services in the Domain Name space and as such, similar guarantee, provided by the accreditation process shall be in place.	7/6/2015 10:33 AM
2	Keep the Whois privacy please	7/5/2015 3:38 PM
3	With one delimiter: Since ICANN's authority is by appointment from the Federal Government, it could be viewed as a Government agency and might be subject to PII requirements under the Privacy Act. As an individual, I have some concern that the Privacy Act was included as part of the discussion (anywhere in the document).	7/5/2015 2:30 AM
4	I disagree with this statement on a technicality: Neither term has been defined at this point in the document.	7/5/2015 1:46 AM
5	Yes. There are many legitimate reasons to need privacy and proxy services, such as operating home-based businesses or publishing politically contentious material, and this should not be used as a means to discriminate.	7/2/2015 4:55 PM
6	Accreditation in and of itself is a nonstarter. The process should be killed.	7/2/2015 9:25 AM
7	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
8	A proxy is a 3rd identifiable party. A privacy is a non existent party that provides a similar service. But not equal. There are legal differences in liability for example.	7/1/2015 8:24 AM
9	Putting too much demand onto domain registrants will cause bloat, cost, ... Publication of contact data is required by certain countries (Germany) and should not be demanded by ICANN for all countires. Again: privacy is an important good. Protection against harassment by government, extremists, terrorists, and spammers is an overriding concern.	7/1/2015 4:48 AM
10	I do not believe that imposing these requirements where it should be the responsibility of the domain registrars is in the interest of the majority who may be affected should these recommendations come to pass, and this may create more problems where there weren't any previously.	6/30/2015 11:10 PM
11	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:42 AM
12	With reservations: this should be approached on a recommendation-by-recommendation basis, not imposed as policy, as the contractual implications are different.	6/29/2015 4:12 PM
13	No accreditation should be required.	6/29/2015 12:10 AM
14	They provide different services for different purposes, and deserve to be treated separately.	6/28/2015 8:34 PM
15	This is going to end badly for you.	6/28/2015 6:40 PM
16	My privacy and of my clients is not guaranteed nor safe at all under ICANN rules.	6/28/2015 10:32 AM
17	Hell no!	6/28/2015 7:49 AM
18	Don't know	6/28/2015 3:45 AM
19	I don't think it should be ICANN's business what someone is using a domain for and I don't think ICANN should be in the business of "accrediting" a domain. The only question should be "is it already in use?" If it's not, then it shouldn't matter who's using it. Likewise, I don't think privacy and proxy services should have to be accredited. (Though if ICANN insists on trying to do such things it's not clear to me that there's a difference between a "privacy" and "proxy" service.)	6/28/2015 3:18 AM

20	Reducing privacy on the open internet will reduce the individual content being produced and distributed. This limit of speech is unacceptable and will drive people to the dark net.	6/28/2015 3:11 AM
21	No if you accredit it you will want to publish it. I do not want any of my details published. I am willing to publish a contact email address that will be monitored - and if it receives much spam then we know that ICANN was responsible for it.	6/27/2015 12:56 PM
22	You've made this public comment form too complicated and neglected to show the sections you are referring to as part of the question. No idea how to answer this.	6/25/2015 3:35 PM
23	What is critical here is that proxy services do not become a service for spammers. To this end, they should be required to provide owner information to Spamhaus and/or Spamcop in the event that there are more than 10 EXPLICIT user reports of spam, i.e that a human reported the item as Spam via the said services.	6/25/2015 2:58 PM
24	Hypothetical example: Website A has posted without permission content owned by the owner/manager of Website B. The Website B owner should be able to contact the owner of Website A without too much fuss. Registration services (private and proxy) should be required to contact the owner of Website A within a short period, at no charge, with the complaint from Website B, and should be required to provide a response from A to B within a short period (say 5 business days). If Website A does not respond, then registrar provides contact info directly to Bebsite B owner.	6/21/2015 7:16 PM

Q6 Do you agree with the WG's recommendation that: (1) the status of a registrant as a commercial organization, non-commercial organization, or individual should not be the driving factor in whether proxy/privacy services are available to the registrant; (2) privacy and proxy services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals; and (3) privacy and proxy registrations should not be limited to private individuals who use their domains for non-commercial purposes?(Section 1.3.1 Recommendation 3, Section 7.1 Category C)

Answered: 136 Skipped: 216



Answer Choices	Responses	
Agree with all three statements	**71.32%**	97
Agree with none of the statements	**19.85%**	27
Agree with some of the statements (please indicate in the box below the reasons for your answer)	**8.82%**	12
Total		**136**

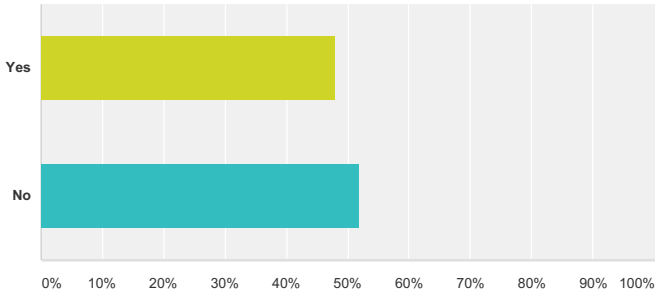
#	Additional Comments	Date
1	P/P should be banned	7/7/2015 7:16 PM
2	the status of a registrant as a commercial organization, non-commercial organization, or individual should be the driving factor in whether proxy/privacy services are available to the registrant	7/6/2015 10:39 AM
3	there is no reason to discriminate the statues of registrant. whatever they are, that shall have identical rights. P/P services is a right shall be available to any registrant.	7/6/2015 10:33 AM
4	Does my site constitute commercial purposes? No. You tell me! A blog that has ads, does that count? What about I sell physical goods over the phone and ship them to buyers and use a website strictly to deliver invoices and allow payment online? Does that count?	7/6/2015 9:54 AM
5	I value my privacy. 'Commercial' definition way too vague.	7/6/2015 7:27 AM
6	Keep the Whois privacy please	7/5/2015 3:38 PM
7	In some cases, it may be advantageous for the registrar to require a "public" interface with an organization (e.g., Public Affairs Officer or similar). Such could be required without exposing individuals' PII (e.g., use of a role or title, with an email address, phone number, or physical mailing address).	7/5/2015 2:30 AM
8	I disagree that an individual should be treated the same as a commercial or non-commercial organisation. The reason for this is that any staff member or representative of an organisation is able to go home at night and be safe. An individual or sole-trader only has their home address to give; and this opens them up immediately to serious personal risk and harrassment outside the nine to five business hours, as their telephone number will be published. If someone has a problem with a service, then they should go through the propper channels. ie. legal or oversight body. To do otherwise is to expose a family home to harassment and possible physical abuse. ie. things like hate speach should be brought before the courts rather than putting bricks through windows and petrol through letterboxes.	7/5/2015 2:28 AM
9	Domain name registrants place great trust in ICANN and its accredited providers. With respect to the members of the ICANN WG, I implore you to please not abuse this trust with the weasel-words and commerce-trumps-personal-privacy attitude of corporate and intellectual property interests.	7/4/2015 1:16 AM

10	Yes. Both private individuals and commercial organizations need privacy to allow for free speech, ability to conduct business, and ability to be safe from harassment and abuse. All parties should be entitled to the use of privacy services, but a particular consideration is that the line between private activity and commercial activity online is often blurry: for example, small home-based businesses or individual artists and writers may be considered "commercial" but have economic and privacy concerns similar to individuals. Meanwhile, many "noncommercial" activities, such as large charities, are run by nonprofits with resources and legal infrastructure comparable to large corporations, and the impact of their activity online is also no different.	7/2/2015 4:55 PM
11	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
12	disagree strongly with 1 - agree with 2, no opinion on 3	7/1/2015 9:10 PM
13	I think I agree unless there is something I don't understand. Privacy is of the utmost importance to me as an individual owner and business owner of domain names.	7/1/2015 6:57 PM
14	It is important to uphold all possible privacy protections that are currently made available to users, small and large, by the privacy and proxy service organizations. Without this, people would receive a lot more spam and would also be subject to the whims and fancies of anyone who finds a site objectionable.	6/30/2015 10:42 AM
15	1 and 2	6/30/2015 7:03 AM
16	Disagree with 1. Agree with 2 and 3. Privacy and proxy services should remain available to all under all conditions.	6/29/2015 12:10 AM
17	Privacy and proxy services should be available to domain registrants regardless of the nature and use of their domains. There are several reasons for this, of which the most obvious is that one person might control a domain which is used commercially and another which is used privately; it is ridiculous to suppose that privacy could be kept on one but not the other.	6/28/2015 8:34 PM
18	Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good.	6/28/2015 8:30 PM
19	If you try to force your will on the people, the people will respond with violence.	6/28/2015 6:40 PM
20	Privacy is essential in the decentralized miasma that is the Internet. Limiting who can utilize these services would devastate the state of e-commerce and other legal online venues.	6/28/2015 11:12 AM
21	Hell no!	6/28/2015 7:49 AM
22	Privacy should be the default. Not the pay-to-play opt in option.	6/28/2015 3:18 AM
23	(3) privacy and proxy registrations should not be limited to private individuals who use their domains for non-commercial purposes	6/28/2015 2:56 AM
24	I do not agree with the above statements due to the notes that accompany them on the actual document which are not provided here.	6/27/2015 7:10 PM
25	ICANN itself does not publish it's own people's names in it's own whois entry! http://whois.icann.org/en/lookup?name=icann.org So why should anyone else? Furthermore - my Limited Company (1 person) is correctly registered where I live and operate - even here, the government's own company registrar does not list my companies contact details for anyone to browse - it does not even publish contact details. Merely the registration number, and that my firms registration is still live and when the registration was first made. So if that is good enough for the government it should be good enough to merely hold a domain name - which is a very small subset of running a company	6/27/2015 12:56 PM
26	It's not fair to individuals, bloggers and small businesses that have their home address listed for their domain. Large corporations and bigger companies with brick and mortar addresses have the luxury of not having their personal information listed. Security and safety: Let's say I'm a blogger and I make money from my site. I'm guessing this would mean commercial. But I happen to blog about anti muslim type stuff. If my address were revealed this would put my life, my wife and kids life and even my dogs life in harms way, not to mention my property. According to the law, I have a right to feel safe and secure in my own home without distress. I'm not a lawyer but this new proposal seems like it would put certain peoples safety in harms way. And to be clear I don't blog about anti muslim stuff, it was just an example. Plus, we pay for this service. So the executives at ICANN came up with the brilliant idea of "hey, let's cut this so our revenues decrease." Any other corporation in the world would fire the people who came up with this idea. Jus saying.	6/27/2015 12:23 PM
27	I think that ICANN is the wrong level to deal with the issues: it should be a matter for national law, particularly as that allows differing definitions of commercial and differing levels of required disclosure appropriate local business practices. In almost all cases it will be possible to enforce this at national level.	6/27/2015 5:16 AM
28	Privacy and proxy registrations should be available to the registrant regardless of their use or status. It should not be compartmentalized dependent on use and given exceptions under specific circumstances.	6/26/2015 12:05 PM
29	I feel that the "Privacy and Proxy Services" as currently available should not be permitted. These faciliities where apparently created as a new mechanism for registrars to charge for services, and NOT to protect privacy. If the registrars wanted to provide privacy, they wouldn't be charging for this. Disallow the services in full.	6/25/2015 4:42 PM
30	This is no different than our right to list or not list a phone number and/or address in a phone book. This is private information that is available to every single person who has access to the internet. You cannot allow the desires and money of a few organizations with a very narrow view of the world to dictate the privacy for billions of people. These same companies have a legal process they can go through to get their desired information. Just because that is time consuming and costly doesn't mean you can take away the right to privacy for all other organizations, companies and individuals.	6/25/2015 3:35 PM

31	In simple terms I think the WHOIS privacy data should stay how it is now, i.e. published unless WHOIS privacy is privided by the Domain Registrar. The changes you are proposing will increase spam, remove privacy, expose commercially sensitive information and potentially wreck genuine businesses. 1. YES and it should not even be recorded whether it is an individual or organisation because this is commercially sensitive information, otherwise you help spammers who can garner that data and sent targetted spam. 2. YES, this is critical to avoid spam, retain privacy and protect commercially sensitive information 3. Yes privacy and proxy registrations should NOT be limited to private individuals who use their domains for non-commercial purposes? Once your details are out there they are sold and shared on black hat forums. Publishing the name of a domain owner without WHOIS privacy will result in a massive increase in SPAM, you will be helping the spammers. As a result of this domain owners will get more spam. This is commercially sensitive information, sites like webboar re-publish this information, consider Amber Jalink, a Canadian woman who helps local businesses, this link identifies the customers whose domains she manages http://www.webboar.com/whois-name/YW1iZXIgamFsaW5rIA== They already did this in Canada which is why her commercially sensitive information (the names of her customers) is now freely available on the above link. If you want to know the owner of an office building you have to pay for each entry in the register and the information is copyright so cannot be re-published and you don't then get the name and address of every other building they own. Well that is what happens if you publish the owner of a domain. It also affects the standing of the domain owners from Google who has already shown itself as abusive as far as data collection is concerned (Google Streetview cars breaking past home routers, stealing documents from PC's and indexing that information, plus publishing the details of routers to remove privacy with Apps like Waze.) The real villains here are the spammers, the solution to spammers is for the FTC to FOLLOW THE MONEY, every spam email has a link, that link can be traced with sites like http://tools.pingdom.com/ the link then shows the affiliate reference. What the FTC need to do is simply bring in an obligation of companies like Leadpages, Clickbank, JVZoo, WarriorForum and anyone else who pays out to provide the financial information of who they are paying to the likes of Spamhaus and Spamcop who can then provide it with evidence to the FTC for prosecution.	6/25/2015 2:58 PM
32	The consequences of publicly showing private information of small internet business are very dangerous. Competitors are capable of anything to take down a successful entrepreneur. This information will be use for abuse and actionable harm. There must be a way to protect small business owners who work at home. Not having access to privacy/ Proxy service would be devastating. Not a good idea. This measure would put their safety and their family' safety in danger.	6/24/2015 1:49 PM
33	Any person (includes natural and legal persons, as well as organizations and entities) registering a domain name that will be utilized to market products or merchandise to be sold to the general public for profit should not be permitted to utilize proxy/privacy services, nor should any person registering a domain name utilized for transactional purposes (a website where payment processing occurs via credit card or any other accepted form of payment)	6/24/2015 1:24 PM
34	Don't agree with disclosure of private individual's information. Therefore, you cannot treat them the same as an organization.	6/24/2015 9:50 AM
35	Additional provision: Any registrant with more than 3 complaints about copyright infringement (or other illegal actions on their website) should be considered/reviewed for loss of proxy/private registration privileges. After review by a qualified panel, this consideration could be extended by such panel to include 3 complaints in 10 years.	6/21/2015 7:16 PM

Q7 Do you agree with the WG's recommendation that domain names registered using a privacy or proxy service should be labeled as such in Whois? (Section 1.3.1 Recommendation 4, Section 7.1 Category B-1)

Answered: 133 Skipped: 219



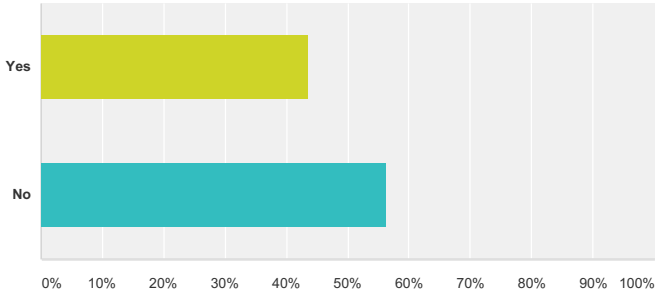
Answer Choices	Responses	
Yes	**48.12%**	64
No	**51.88%**	69
Total		**133**

#	Additional Comments	Date
1	I see nothing wrong with that recommendation. Inf act most of the bigger proxy services seem to have the word "proxy" (or "privacy") somewhere in there name already. So why not making such a label mandatory?	7/7/2015 6:44 AM
2	We disagree with the WG's recommendation. Privacy and proxy services are designed to ensure a level of privacy that benefits the end user, and a designation such as this removes that benefit.	7/6/2015 11:43 AM
3	must be clear to registrant and other as Law Enforcement Agent that the registrant has opted to be unders P/P services, and for such this shall be stated at Whois platform.	7/6/2015 10:33 AM
4	No point.	7/6/2015 7:27 AM
5	Keep the Whois privacy please	7/5/2015 3:38 PM
6	This is not a change from today, where anyone with a pulse can tell.	7/5/2015 1:46 AM
7	Provided no personally-identifiable (or personally-correlatable) information is exposed, I would agree. If two domains registered privately to the same individual would have the same identifier simply because it's the same individual, I'd say No.	7/4/2015 1:16 AM
8	There is no reason to make this discrimination. Marking this in WHOIS would give a signal to those looking for contact information that the registrant feels they need extra privacy--this may increase the likelihood that potential harassers and abusers will look for the information that is being hidden, and to use the publication of that information as an attack.	7/2/2015 4:55 PM
9	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
10	I believe that when one wants to start a website, there should be no need to give up private information at all, but it should especially not be available to the general public.	7/1/2015 7:12 PM
11	?? do not understand.	7/1/2015 6:57 PM
12	An extra label is not necessary, as long as contact information is correct.	7/1/2015 8:24 AM
13	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:42 AM
14	This is clearly an additional burden on everyone involved in WHOIS maintenance, including registrars and registrants, and should therefore not be included unless clearly necessary for the good functioning of the service. In fact, the opposite is true: the WHOIS system provides contact information, not legal ownership information, and thus the legal relationship of the provided contact to the domain registrant is irrelevant.	6/29/2015 4:12 PM
15	This would create an atmosphere of contempt for those wishing to remain anonymous online. It is a constitutional right to be anonymous when one wants to. These services should appear identical to any other non private service. More importantly many healthcare organizations use these services to transmit protected health information. Any attempt to violate this security could be seen as a violation of HIPAA under the security and privacy rules.	6/29/2015 7:38 AM
16	No strong opinion, but this seems appropriate.	6/28/2015 8:34 PM
17	Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good.	6/28/2015 8:30 PM
18	Shaming people who want privacy is immoral.	6/28/2015 6:40 PM

19	not really in favor, neither against.	6/28/2015 10:32 AM
20	The only advantage I see is determining whether a given email address is reachable, but labeling it has many more repercussions. Anything handling domains might discriminate on this field, e.g. search engines may rank anonymous domains lower and SSL/TLS certificate authorities might reject these domains. It probably ends up in discrimination of domains somewhere. Crooks can use fake info because they are willing to break the law to achieve it; everyone else who wishes their personally identifiable information to be private (only available to the registrar itself, which authorities can reach) gets discriminated by such a policy.	6/28/2015 8:43 AM
21	Hell no!	6/28/2015 7:49 AM
22	I've already stated my position that Whois in its current incarnation should not exist. All it does is create risk for those who need privacy and enable bad state actors like China and Turkey. All that should be required for getting a domain is a minimal method of contact (an email or similar) and all Whois should disclose is that that email.	6/28/2015 3:18 AM
23	I do not think privacy services should be regulated. There is already a market for these services and market forces will drive the best to the top and the users of those services to advertise their use themselves. Furthermore most normal internet users don't know how to use Whois so it is worthless to list there anyway.	6/28/2015 3:11 AM
24	Do not understand the need to label domain names as registered via privacy or proxy services.	6/27/2015 7:10 PM
25	I prefer that very limited information is published in whois. Limited to a contact email is quite sufficient.	6/27/2015 12:56 PM
26	Absolutely not. WHOIS information is made public or private when the domain is registered, it should not be modified at free will, it's unfair and unjust.	6/26/2015 12:05 PM
27	They already are. There is no confusion and these companies that have spent a ton of money to get this common practice eliminated, should be told to turn around and attempt to pay for influence elsewhere.	6/25/2015 3:35 PM
28	No need, it is pretty obvious if it says Privacy Protected or Domains by Proxy	6/25/2015 2:58 PM
29	I believe, labeling private or proxy registrations to clearly show they are being kept private is fine. However, revealing the company providing that is providing the service is the first step to ending that privacy. In the interests of privacy, I therefore strongly recommend the proxy not be named.	6/25/2015 2:55 PM
30	Not sure I understand this one ... if I look up a domain with Whois I can see if it's private (??)	6/21/2015 7:16 PM

Q8 Do you agree with the WG's recommendation that: (1) privacy/proxy customer data is to be validated and verified in a manner consistent with the requirements outlined in the WHOIS Accuracy Specification of the 2013 RAA; and (2) in the cases where a privacy/proxy service provider is Affiliated with a registrar (as defined by the 2013 RAA), and validation and verification of the customer data has been carried out by the registrar, re-verification by the privacy/proxy service provider of the same, identical, information should not be required?(Section 1.3.1 Recommendation 5, Section 7.1 Category B-2)

Answered: 133 Skipped: 219



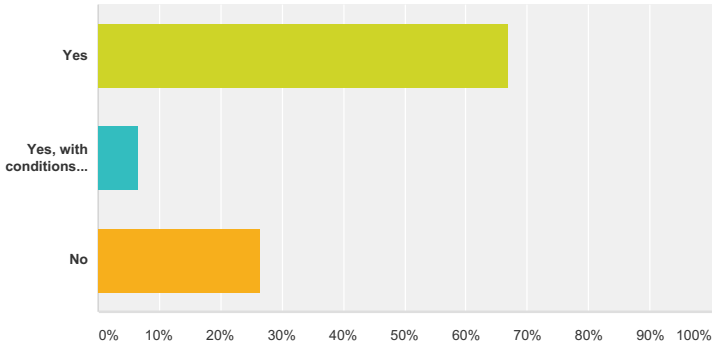
Answer Choices	Responses	
Yes	**43.61%**	58
No	**56.39%**	75
Total		**133**

#	Additional Comments	Date
1	A corrupt registrar will just run a corrupt P/P service.	7/7/2015 7:16 PM
2	both statement follow a correct logic	7/6/2015 10:33 AM
3	The WHOIS Accuracy Program is useless (criminals will still use fake data) and harmful (it makes registrants vulnerable to phishing attacks).	7/5/2015 5:33 PM
4	This proposal only makes sense if there is a very high level of certainty that the original data were accurate and there has been no material change of circumstances since.	7/5/2015 12:20 PM
5	With at least one of the registrars that I've employed, re-verification has been a nuisance.	7/5/2015 2:30 AM
6	I cannot trust or evaluate this because it incorporates excessive language by reference,	7/5/2015 1:46 AM
7	The WHOIS accuracy specification is fundamentally flawed.	7/2/2015 9:25 AM
8	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
9	Please keep my information private and unavailable to anyone that I have not authorized to have it!!	7/1/2015 6:57 PM
10	From the Netherlands and 10 Dutch ICANN accredited registrars, we have several objections to the WHOIS Accuracy Specification of the 2013 RAA. We do agree that re-verification should not be required on identical data.	7/1/2015 8:24 AM
11	Spam issues can cause failure to re-verify. Spam needs to be solved. Actually, it is easier to verify anonymous data than public email data. I think Godaddy should be prohibited from demanding privacy protection to be removed before changing domain registrars. Never should privacy be lifted, this should be illegal. I did have a good reachable private email address, and during domain registrar transfer this email became known and spammed. This issues MUST be solved. Court orders may be an exception. Destroying a bona fide honest email address caused extreme hardship and made normal contact impossible. It also makes me weary to provide good spam free email contact to the Anonymizer service Godaddy (and maybe others) does this to prevent registrar changes. They hold their domain holders hostage.	7/1/2015 4:48 AM

12	Re: Recommendation 1: Third-party handling and verification of customer data defeats the entire purpose of the privacy/proxy service, which I believe should be a relationship only between the service provider and the customer, and I'm certain there are many others who agree with this sentiment. From my understanding, the current low standards for disclosure will do more harm than good to individuals, may very well open them up to harm and harassment from "doxxers" and other unscrupulous people who may want to silence their critics physically or otherwise. The current language of this document places the metaphorical keys in the hands of "Law enforcement authority" as liberally defined by the GNSO Initial Report document in Section 1.3.1 Recommendation 1, which more or less the door for privileged special interest organizations to encroach on the individual right to privacy.	6/30/2015 11:10 PM
13	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:42 AM
14	8(1): I believe that the WHOIS Accuracy Specification is fundamentally misguided, and should be demoted to a recommended practice rather than a requirement. For example, email is not a guaranteed delivery mechanism, so it is inappropriate to depend on email as a primary contact, and perhaps even inappropriate to mandate in contact information. The current Specification assumes otherwise for all of these. 8(2): No objection.	6/29/2015 4:12 PM
15	Requiring the adoption of a whois verfication and sharing standard like this would do little to hamper those who intend not to provide legitimate or meaningful information to the whois system with intent of malice, especially outside North America and Europe. Those seeking to to acquire a domain registration anonymously for legitimate purposes such as companies looking to preemptively prevent domain squatting without making their association to a domain visible to their competition (a company doesn't want it's competitors to know that a proxy service acting on it's behalf purchased myexamplemarketingcampaign.com or mypotentialnewwidgetname.com) will be driven to 3rd parties (already a common practice, as seen with the release of .xxx TLDs) creating needless hassle/friction/cost. The additional cost/hassle would disproportionately impact individuals with legitimate motives for desiring anonymity (owning something like mybeerblog.something isn't something most people would want showing up on a pre-employment background check).	6/29/2015 7:41 AM
16	To validate privacy customer data would negate the entire purpose of the customer using the privacy service. This would destroy an entire industry. It would also open up secure data such as protected health information in transmission and could cause violations of the HIPAA privacy rule.	6/29/2015 7:38 AM
17	No strong opinion. This is acceptable.	6/28/2015 8:34 PM
18	Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good.	6/28/2015 8:30 PM
19	You don't get to decide.	6/28/2015 6:40 PM
20	With regard to (1), no. Whois Accuracy as specified by 2013 RAA does not need to be applied to P/P providers.	6/28/2015 4:17 PM
21	Hell no!	6/28/2015 7:49 AM
22	I disagree with (1) but agree with (2).	6/28/2015 6:14 AM
23	WHOIS Accuracy Specification is overly onerous.	6/28/2015 3:45 AM
24	Point two I suppose I agree with given that point one is required, but as previously stated I don't think date should be validated or verified. The identity of a domain's owner should not be part of the domain system. Anything else is likely to put freedom of speech at risk by forcing those who wish to express themselves anonymously to go through a gatekeeper who can censor their speech.	6/28/2015 3:18 AM
25	This defeats the purpose of having the privacy provider.	6/28/2015 3:11 AM
26	There is no need to validate users if they already have an ongoing commercial relationship. There is no need to have accurate information in whois.	6/27/2015 12:56 PM
27	Whether or not customer data is verified, and the manner in which it is verified should be left to the discretion of the privacy/proxy service.	6/25/2015 7:05 PM
28	Not only is this overly burdensome which will force an increase in already high registry costs, but it's anti capitalism. I don't have to give my personal data and have it verified when I subscribe to online services or at restaurants or brick and morter stores. That process is wholly unfair, unless the registrant is claiming to be a registered business or non-profit. In those cases automated online lookups could be done.	6/25/2015 3:35 PM
29	I believe the 2nd condition is true however, in the interests of privacy and the smooth running of the internet I don't believe ICANN should begin policing. If perhaps I misunderstood some parts of the WHOIS Accuracy Program Specification of the RAA 2013 and policing isn't the intention. My intent is to say that privacy is a human right that should not be infringed in the interests a few companies.	6/25/2015 2:55 PM
30	Based on the ability to contact the registrant as currently required concerning contact details being maintained.	6/23/2015 11:44 AM

Q9 Do you agree with the WG's recommendation that: (1) all rights, responsibilities and obligations of registrants, privacy/proxy service customers and service providers need to be clearly communicated in the privacy/proxy registration agreement, including a provider's obligations in managing those rights and responsibilities and any specific requirements applying to transfers and renewals of a domain name; and (2) all privacy/proxy service providers must disclose to their customers the conditions under which the service may be terminated in the event of a transfer of the domain name, and how requests for transfers of a domain name are handled?(Section 1.3.1 Recommendation 6, Section 7.1 Category B-3)

Answered: 121 Skipped: 231



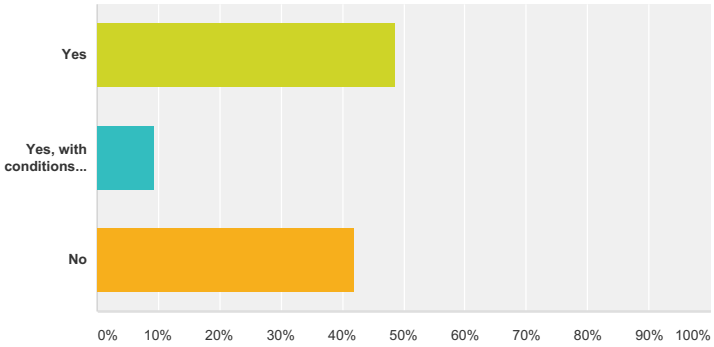
Answer Choices	Responses	
Yes	**66.94%**	81
Yes, with conditions (please specify what those conditions are in the box below)	**6.61%**	8
No	**26.45%**	32
Total		**121**

#	Additional Comments	Date
1	P/P services are additional services to whom decided to make such choice. hence, all obligations and responsibilities and rights for both sides shall be clearly stated at the signed agreement. Basic services supported by RAA will continue to be valid and the interface between Registrar and P/P Service Provider shall also be clear into the P/P agreement with registrant. Disclosure, Publication, termination, transfer or renew shall also be include in such agreement.	7/6/2015 10:51 AM
2	It's no	7/6/2015 7:28 AM
3	Domain registrars have done bad job of disclosing restrictions on transfer of private domains. Either, rules should be amended to allow transfer of private domains, or registrars should be mandated to disclose upfront that domains may not be transferred without having privacy turned off in large print, not hidden in the find print of the end user agreement.	7/6/2015 12:04 AM
4	Since ICANN is a Government-appointed entity, I would suspect most that most, if not all, provisions of the Privacy Act would apply. (The Privacy Act is not even referenced in the Report.) It's always been a point of concern that many registrars treat privacy as an "opt in" measure and leverage it as a vehicle for profit.	7/5/2015 2:37 AM
5	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
6	In the case of a transfer, the service cannot be guaranteed or forced. If a reseller does not offer the service, a client transferring to that reseller in the market cannot force the reseller via any ICANN policy or contract.	7/1/2015 8:33 AM
7	Absolutely, termination of privacy can be life threatening or cause hardship.	7/1/2015 4:53 AM
8	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:44 AM

9	Since a providers disclosure of customer information may violate the privacy and security rule under HIPAA. It would be a gross violation of federal law to enforce service provider to disclose customers. This could lead to hacking attacks or other security violations.	6/29/2015 7:41 AM
10	Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good.	6/28/2015 8:30 PM
11	I disagree with this part the most. As an individual, I simply don't want my personal information to be readily available to the Internet at large, and I don't want privacy companies to have to disclose that information so easily. Nor do I want the additional bureaucratic overhead to result in additional costs for me.	6/28/2015 5:57 PM
12	not something that should be under icann regulations	6/28/2015 10:37 AM
13	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:50 AM
14	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:16 AM
15	As previously stated I don't believe identity should have to be disclosed in order to obtain a domain, or that a registrar or privacy/proxy service should be required to know their customer's identity, or have to reveal what they know of their customer's identity, particularly without informing their customer or a court order.	6/28/2015 3:21 AM
16	This shouldn't be regulated. The best providers will be transparent in their terms and services and gain the most users.	6/28/2015 3:17 AM
17	I do not entirely agree with everything. A good compromise would be to apply this to privacy services provided by registrars (most of them) but do not attempt to prevent other parties from providing such services standalone.	6/27/2015 5:20 AM
18	Yes, they absolutely have to be clearly communicated, nothing should be done behind closed doors, from what I am understanding this to say.	6/26/2015 12:09 PM
19	Um, obvious. Come on... if it's not clear and in the contract, it doesn't exist, period!	6/25/2015 3:41 PM

Q10 Do you agree with the WG's recommendation that accredited P/P service providers must include on their websites, and in all Publication and Disclosure-related policies and documents, a link to either a standardized request form or an equivalent list of specific criteria that the provider requires in order to determine whether or not to comply with third party requests, such as for the Disclosure or Publication of customer identity or contact details?(Section 1.3.1 Recommendation 7, Section 7.1 Category F)

Answered: 117 Skipped: 235



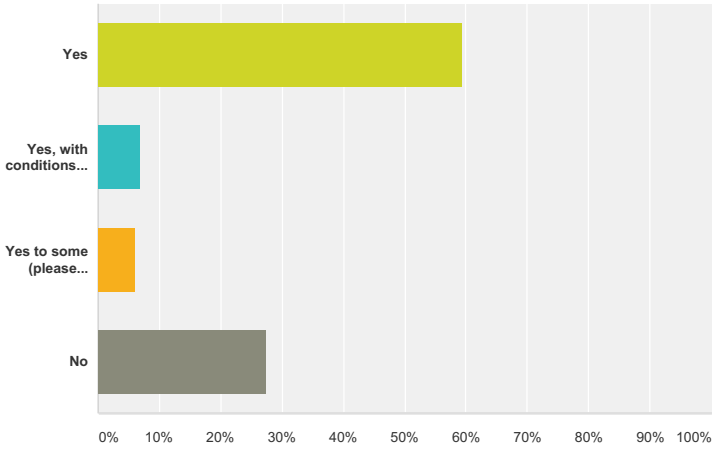
Answer Choices	Responses	
Yes	**48.72%**	57
Yes, with conditions (please specify what those conditions are in the box below)	**9.40%**	11
No	**41.88%**	49
Total		**117**

#	Additional Comments	Date
1	But of course the P/P providers will jsut ignore requests.	7/7/2015 7:19 PM
2	If the request for disclosure of any personal data, identity or cantact details does not come with a valid and legal court order, any such request must be forwarded to the registrant to enable them to object. Since a court order cannot be sent through any online request form, no such request must be complied with without first notifying the registrant and allowing them to object. And no such request must be granted without following some very strict and clear rules which the registrant must have agreed with at some point (usually during the registration of the domain).	7/7/2015 6:58 AM
3	transparence is key. make it available to customer at their website or at other way where registrant will access to make its option is fundamental. I would not enphazise "all publication". being complete under the link provided at the P/P Services Provider, look suffice for me.	7/6/2015 10:51 AM
4	Private should mean PRIVATE - not "Private until further notice"	7/6/2015 10:41 AM
5	There is no need for more burdenous regulation. This is what the court system is designed for.	7/6/2015 4:19 AM
6	It's probably a good idea to include a limitation of "in accordance with the registrar's host/parent country".	7/5/2015 2:37 AM
7	Commercial organisations that run from listed buildings should actually, in my personal opinion, not be granted the right to be protected. This service is currently being abused by spammers operating as, "marketing companies," who are then impossible to trace in order to report to authorities. Rule of thumb - persons name, allow the option to be protected. Business name, not protected.	7/5/2015 2:31 AM
8	The accreditation program is a fundamental issue. It should not exist!	7/2/2015 9:35 AM
9	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
10	The decision should be mine alone, as the information is mine alone.	7/1/2015 7:01 PM
11	Clients of accredited P/P service providers need to be protected in the event of frivolous litigation requests to P/P service providers, directed at the P/P service provider's client(s).	7/1/2015 6:44 PM
12	Where the only parties using said form are authorized by local authorities to do so. Quasi-governmental or similar is too vague, not in line with privacy law, and unacceptable.	7/1/2015 8:33 AM
13	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:44 AM

14	Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good.	6/28/2015 8:30 PM
15	Yes, but in addition to a standard process for requesting disclosure/publication, there also needs to be a standard process for opposing disclosure/publication.	6/28/2015 4:24 PM
16	If the recommendation as a whole passes, yes, but I do not think it should pass.	6/28/2015 2:06 PM
17	the former only if it clearly lists which items are required (i.e. the latter)	6/28/2015 12:31 PM
18	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:50 AM
19	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:16 AM
20	As previously stated I don't believe identity should have to be disclosed in order to obtain a domain, or that a registrar or privacy/proxy service should be required to know their customer's identity, or have to reveal what they know of their customer's identity, particularly without informing their customer or a court order.	6/28/2015 3:21 AM
21	This should not be regulated. A law enforcement entity will know how to get in touch and the requirements to request private information (valid court order)	6/28/2015 3:17 AM
22	Privacy or proxy services should not be required to provide personal info	6/27/2015 7:21 PM
23	I have no objection to law enforcement seeking such information - I have no choice anyway. All others can contact me through my websites email or my whois entry email. There is no reason whatsoever that anyone should be given my name, home phone number and home address.	6/27/2015 1:01 PM
24	They should also be emailing and contacting current customers in the circumstances this occurs. It is misleading to just put a link in a standardized document or form on their website.	6/26/2015 12:09 PM
25	Publication and disclosure requests will be abused by third-parties.	6/26/2015 4:02 AM
26	I believe local country laws may be held higher than these policies when appropriate.	6/25/2015 3:03 PM
27	This will be abused, the only people who should be able to to request disclosure should be: FTC Spamhaus Spamcop Court Order	6/25/2015 2:58 PM

Q11 Do you agree that the following additional provisions regarding Disclosure and Publication should be included in the Terms of Service: (1) clarification of when there is a reference to Publication requests (and their consequences) and when to Disclosure requests (and their consequences); (2) explanation of the meaning and consequences of Publication; (3) the specific grounds upon which a customer's details may be Disclosed or Published or service suspended or terminated; and (4) clarification as to whether or not a customer: (i) will be notified when a provider receives a Publication or Disclosure request from a third party; and (ii) in the case of Publication, whether the customer may opt to cancel its domain registration prior to and in lieu of Publication or Disclosure? (Section 1.3.1 Recommendation 8, Section 7.1 Category F)

Answered: 116 Skipped: 236



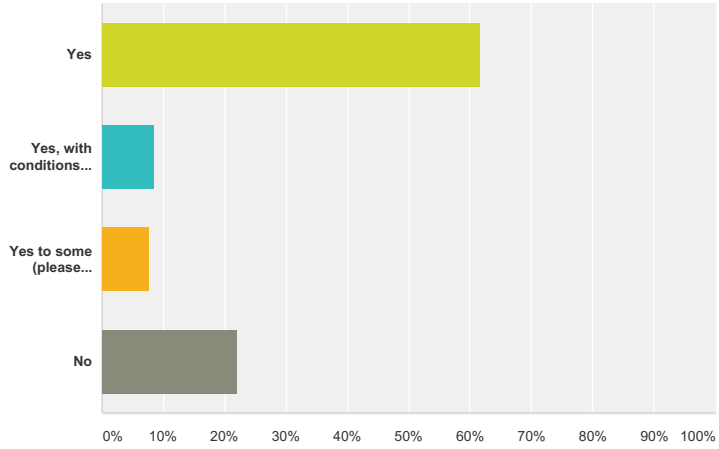
Answer Choices	Responses	
Yes	**59.48%**	69
Yes, with conditions (please specify what those conditions are in the box below)	**6.90%**	8
Yes to some (please indicate which you agree or disagree with, and why, in the box below)	**6.03%**	7
No	**27.59%**	32
Total		**116**

#	Additional Comments	Date
1	4ii should not be allowed.	7/7/2015 7:19 PM
2	this, in my view shall be clearly stated - all those - at the link provided by P/P provider as stated at question 1o above.	7/6/2015 10:51 AM
3	I would much rather that providers notify customers/registrants of *ALL* Publication or Disclosure requests, making clarification as to whether a customer will be notified irrelevant.	7/2/2015 6:56 PM
4	Terms of Service are already impenetrable. If you are insistent on an "accurate" WHOIS database, then the only thing you should do is verify that the contact information a P/P provider gives is accurate. Other than that, stay the hell out of the industry. You have no role to play there.	7/2/2015 9:35 AM
5	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM

6	They should not be giving out my information in any case unless I have authorized it or they have a legitimate subpoena from law enforcement.	7/1/2015 7:01 PM
7	For (4)(ii), I am concerned about frivolous litigious attacks from disconnected legal entities representing IP owners, and individuals needing to cancel their domain registration prior to and in lieu of Publication or Disclosure, because they are fearful of or cannot afford litigious engagement. I see this process being abused by IP rights holders looking to inappropriately expand their brand presence via domain registration.	7/1/2015 6:44 PM
8	If the Registrar's criteria has been met, the Disclosure and/or Publication of the WHOIS data to a non-law enforcement third-party should be limited to the equivalent of a Public Records search. For example, in the United States you can search the public business records of the California Secretary of State. A search for Google Inc. discloses the entity name and mailing address. But it does not expose the private email address or phone numbers of the business owner or it's employees. In addition to the basic contact information the public business records search includes the "Agent for Service of Process" which is the legal representative of the entity. I assert the ICANN P/P Service Regulations should adopt a similar policy directing Registrar's to only disclose basic contact information and "Agent for Service of Process" contact information to a non-law enforcement third-party.	7/1/2015 5:45 PM
9	Not until these policies have been improved and approved.	7/1/2015 8:33 AM
10	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:44 AM
11	I disagree with 4.i, a customer should always be notified. Recent news have shown that law enforcement entities tend to misuse the powers they are granted, or not even that, in some cases. There should be very strict rules around not notifying a customer. 4.ii should also be an option for a customer. In general, it must remain possible (and encouraged) for privacy and proxy providers to provide the strongest guarantees they can make. The process currently works, and an accreditation process that would harm existing providers (and their customers) is unacceptable.	6/29/2015 1:14 PM
12	Privacy and proxy registrations should be eliminated. They are abused to an extent that they no longer serve a public good.	6/28/2015 8:30 PM
13	Just fuck off.	6/28/2015 4:45 PM
14	(2), (3), (4) seem reasonable. (1) seems like unnecessary busywork.	6/28/2015 4:24 PM
15	Disclosure and delay for responsive lititgation must be mandatory in all circumstances. Disclosure should be prohibited except when legally ordered.	6/28/2015 1:49 PM
16	customers should always receive notification unless prohibited by law.	6/28/2015 12:31 PM
17	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:50 AM
18	Due process per the law of the domain owner's country should be required before revealing ANY information, including entity type.	6/28/2015 4:16 AM
19	As previously stated I don't believe identity should have to be disclosed in order to obtain a domain, or that a registrar or privacy/proxy service should be required to know their customer's identity, or have to reveal what they know of their customer's identity, particularly without informing their customer or a court order.	6/28/2015 3:21 AM
20	These are good recommendations but shouldn't be mandatory and privacy services should adopt them voluntarily.	6/28/2015 3:17 AM
21	Do not agree with the reasons for or the persons able to request personal information from privacy or procy services	6/27/2015 7:21 PM
22	I have no objection to law enforcement seeking such information - I have no choice anyway. There is no reason whatsoever that any servie provider should disclose my name, home phone number and home address. They may pass along email communications that I may chose to answer.	6/27/2015 1:01 PM
23	As above - not all privacy providers need by accredited, only those combining registrar and privacy services.	6/27/2015 5:20 AM
24	Yes, also contacing the customer, again, is important.	6/26/2015 12:09 PM
25	Customers must have full transparency on the conditions under which their information may be published or disclosed. There should be almost no such conditions.	6/26/2015 4:02 AM
26	These are the ICANN's recommended best practices for P/P providers. Again I don't feel it's ICANN's place to police these policies.	6/25/2015 3:03 PM
27	I also think that disclosure should only be made to valid requestors and law enforcement agencies or consumer protection groups via some form of secured email communication system and not in the whois database itself.	6/22/2015 12:14 PM
28	Especially (3) and (4)	6/21/2015 7:18 PM
29	Customer MUST be notified when provider receives a publication or disclosure request from a third paty	6/20/2015 10:08 PM

Q12 Do you agree that the following should be recommended as "best practices" for P/P service providers: (1) they should facilitate and not obstruct the transfer, renewal or restoration of a domain name by their customers, including without limitation a renewal during a Redemption Grace Period under the Expired Registration Recovery Policy and transfers to another registrar; (2) they should use commercially reasonable efforts to avoid the need to disclose underlying customer data in the process of renewing, transferring or restoring a domain name; and (3) they should include in their terms of service a link or other direction to the ICANN website (or other ICANN-approved online location) where a person may look up the authoritative definitions and meanings of specific terms such as Disclosure or Publication?(Section 1.3.1 Recommendation 9, Section 7.1 Category B-3)

Answered: 118 Skipped: 234



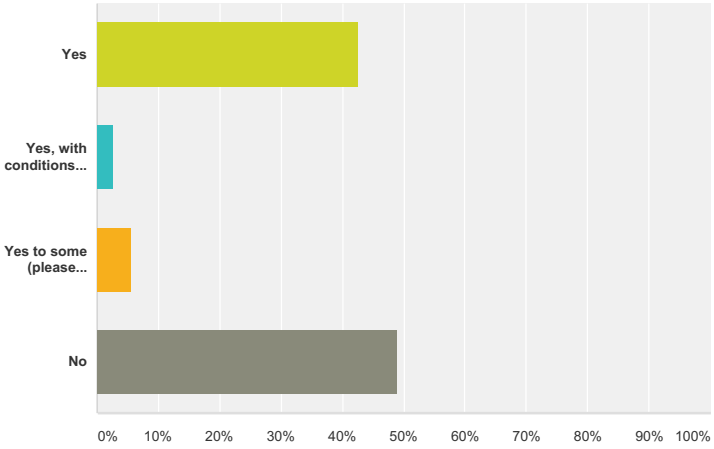
Answer Choices	Responses	
Yes	**61.86%**	73
Yes, with conditions (please specify those conditions in the box below)	**8.47%**	10
Yes to some (please indicate which you agree or disagree with, and why, in the box below)	**7.63%**	9
No	**22.03%**	26
Total		**118**

#	Additional Comments	Date
1	(2) is in contradiction to (1)	7/7/2015 7:19 PM
2	For 12.3, where the working group definitions are used.	7/6/2015 11:51 AM
3	As I have state, in my view conditions under RAA, and best practices followed by accredited registrars shall remain valid for those registrants that have opted to have P/P services. As such, P/P services provider shall offer conditions stated in 1 and 2, allowing registrants to understand what they as entitle to and which are their rights and obligations.	7/6/2015 10:51 AM
4	1. "or other ICANN-approved online location" puts an undue burden on the P/P provider to know where your link is at all times, even after you move it. 2. The authoritative definitions must form part of a document such as you provide and must not be subject to arbitrary future change, which is easy to do with a link-in-motion.	7/5/2015 1:53 AM

5	Agree to 1 and 2. Disagree with 3: the authoritative definitions and meanings should be codified upon accreditation. Putting them on a separate Web site means that they can be changed without approval of the registrar.	7/4/2015 1:19 AM
6	Get the hell out of the P/P business. Beyond ensuring they themselves provide accurate contact information, there is nothing more I as an individual want you to do about P/P services!	7/2/2015 9:35 AM
7	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
8	My information should be protected at all times!!	7/1/2015 7:01 PM
9	Privacy can be an obstruction for transfer if either party does not offer the service. The P/P service provider should not decide or make efforts on whether said privacy is to be upheld or not. If a legitimate and legal need to disclosure is submitted, it must be executed. The distinction between Disclosure and Publication is ripe for abuse by those parties requesting Disclosure in bulk. Parties should not generally be allowed, unless they are local authority binded by law.	7/1/2015 8:33 AM
10	absolutely. Privacy protection must be mandatory until the end of transfer to another registrar. Registrar's requirement to remove privacy (Godaddy) is extreme hardship, dangerous, and defeats the entire purpose of privacy.	7/1/2015 4:53 AM
11	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:44 AM
12	We need a higher standard than "commercially reasonable." Your profit is not worth someone's privacy. Explanatory language should be in terms that are accessible to anyone the policy is going to affect, including those who may not be highly literate in English or any language.	6/28/2015 8:40 PM
13	(1) and (2) seem like clear wins. (3) is unnecessary given Section 1.3.1 Recommendation 8, Section 7.1 Category F, subpoint 2	6/28/2015 4:24 PM
14	I don't understand why a P/P provider would intentionally obstruct these procedures when ordered by their customer. If this means that ordinarily, the customer would have to notify the P/P provider before initiating the action, and this item would mean disclosure of information not ordinarily transferred, I object.	6/28/2015 2:06 PM
15	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:50 AM
16	I	6/28/2015 7:50 AM
17	Due process per the law of the domain owner's country should be required before revealing ANY information.	6/28/2015 4:16 AM
18	As previously stated I don't believe identity should have to be disclosed in order to obtain a domain, or that a registrar or privacy/proxy service should be required to know their customer's identity, or have to reveal what they know of their customer's identity, particularly without informing their customer or a court order.	6/28/2015 3:21 AM
19	Advertising ICANN shouldn't be a best practice	6/28/2015 3:17 AM
20	(3) they should include in their terms of service a link or other direction to the ICANN website (or other ICANN-approved online location) where a person may look up the authoritative definitions and meanings of specific terms such as Disclosure or Publication?	6/28/2015 3:04 AM
21	Unsure	6/27/2015 7:21 PM
22	3) I think Google will assist more than ICANN will.	6/27/2015 1:01 PM
23	I don't see (3) as needed. I agree with (1), but not with (2), because a P/P service should NEVER disclose the data, not to make only "commercially reasonable efforts".	6/26/2015 12:57 PM
24	I don't like the word, "commercially reasonable", disclosure should be made aware to the customer at all times unless it is a legal court order or warrant.	6/26/2015 12:09 PM
25	These and all rules, laws, regulations, clauses, etc must be written so an average person can 100% understand them. No legalese, no jargon meant to fool readers and no loopholes for big companies to gain access to data without prior notification and an appeal process before any personal data would be shared with anyone, regardless of how much money they spend trying to buy these rules that they want.	6/25/2015 3:41 PM
26	To this end, WHOIS privacy should extend when the domain has expired and until released. Many registrars remove the service in the grace period and even redirect the domain to a page where the registrar makes money displaying ads.	6/25/2015 2:58 PM
27	If the privacy service is apart of a registrar then it should be made clear that by transferring away from that registrar privacy service will be deactivated and contact information will be made public. The losing registrar should not be obligated to keep the contact data private. If a third-party privacy service is used then the privacy should remain in place.	6/22/2015 12:14 PM

Q13 Do you agree with the WG's recommendation that: (1) ICANN should publish and maintain a publicly accessible list of all accredited P/P service providers, with all appropriate contact information; (2) registrars should provide a web link to P/P services run by them or their Affiliates; and (3) P/P service providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program? (Section 1.3.1 Recommendation 10, Section 7.1 Category D-1)

Answered: 108 Skipped: 244



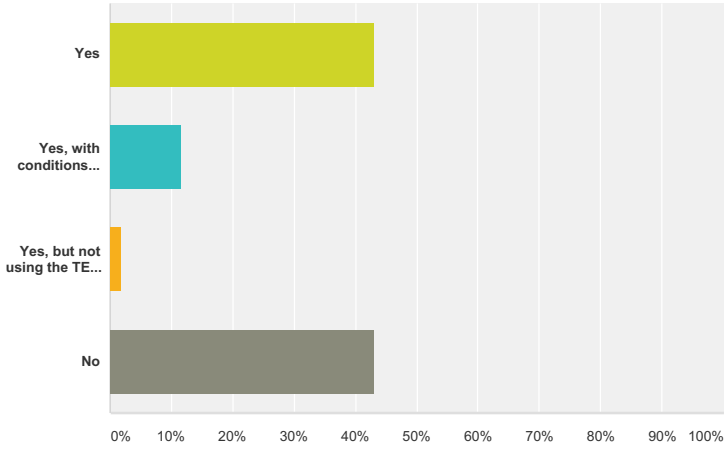
Answer Choices	Responses	
Yes	**42.59%**	46
Yes, with conditions (please specify what those conditions are in the box below)	**2.78%**	3
Yes to some (please indicate which you agree or disagree with, and why, in the box below)	**5.56%**	6
No	**49.07%**	53
Total		**108**

#	Additional Comments	Date
1	Plus require P/P actully respond to requests.	7/7/2015 7:22 PM
2	Agree to: 1. ICANN should publish and maintain a publicly accessible list of all accredited P/P service providers, with all appropriate contact information; This should be at registrars' discretion: 2. registrars should provide a web link to P/P services run by them or their Affiliates This should not be a requirement for accreditation: 3. P/P service providers should declare their Affiliation with a registrar (if any) as a requirement of the accreditation program?	7/6/2015 12:06 PM
3	Relevant for the registrant to know beforehand which P/ P are available, their affiliation with which registrar wherever logical places registrants will look fro information - ICANN, Registrars or P?P service providers.	7/6/2015 11:04 AM
4	"Appropriate contact information" is not defined and subject to litigation. The term "appropriate" needs to be replaced with specific requirements.	7/5/2015 2:04 AM
5	No to 1. Yes to 2 and 3. Providers should be accredited and their privacy/proxy affiliation disclosed. This accreditation should not be able to be contingent, however, upon the behavior of the P/P service and P/P services should not require any sort of accreditation.	7/4/2015 1:25 AM
6	To hell with the accreditation program in its entirety, thank you very much. We don't need it; besides which it is an offense against the privacy of us, "the people". You should be moving in the opposite direction - towards lessening the amount of personal information required and collected (directly or through registrars / providers) from individual registrants / customers.	7/2/2015 7:16 PM
7	No, no, no! Get out of the P/P business. I don't want accreditation. I don't even want a public WHOIS database. But even if the database isn't going anywhere, all you should be doing with P/P providers is making sure the contact information they provide is accurate. Leave the rest to the market. I see zero benefit to me as an individual to you guys meddling.	7/2/2015 9:42 AM
8	This will cripple independent P/P services. It effectively extends your monopoly over domain registration.	7/2/2015 8:54 AM
9	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM

10	Disagree with (2). There are way too many affiliates to provide links to. They change too often. It's unlikely to provide a complete or clarifying overview.	7/1/2015 8:41 AM
11	I believe that accreditation of these service providers is unnecessary. It may only serve to benefit special interests who are otherwise obstructed by current proxy/privacy service providers.	6/30/2015 11:16 PM
12	There is no need to have a list of accredited and controlled list of such providers which would undermine people's privacy. Just let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:47 AM
13	This assumes that all privacy or proxy service providers are advertising their services to the general public. For persons needing to contact a specific provider, the contact information is already in WHOIS. This proposal requires all providers to be listed publicly, and thus enables malicious third parties to determine conclusively whether a given site is or is not using a provider, eroding that site's security. (For example, such a third party could send false emails to the WHOIS email contact, including the provider as an intermediary if and only if the site uses a provider.) No objection if all lists and links are voluntary, since providers will then be able to decide and respond to this issue for themselves.	6/29/2015 5:00 PM
14	centrally located information has inherent risk for breaches and privacy violations. This would create a target rich with information for hackers.	6/29/2015 7:42 AM
15	No accreditation should be required.	6/29/2015 12:15 AM
16	It is not and should not be ICANN's responsibility to manage P/P services. If you wish to create an independent, voluntary accreditation program with clear and reasonable criteria--reasonable from a person's perspective, not a corporation's perspective--I would support that. But the system described here is dangerous and worrying. Independent P/P services are much more meaningful and valuable for privacy than anything tied to a registrar, or a single accrediting agency, could possibly be.	6/28/2015 8:54 PM
17	I disagree with any text relating to an accreditation program. I do not want to see an accreditation program come into existence.	6/28/2015 5:59 PM
18	(1) and (2) are unnecessary; privacy/proxy services are already easy for consumers to find. I suspect that (3) happens in most cases already, but it's not a bad idea.	6/28/2015 4:34 PM
19	No to an accreditation program. A centralized accreditation process will ensure that over time privacy will be weakened. In this case specifically, it is known that the intention is to weaken privacy.	6/28/2015 2:10 PM
20	ICANN should not define, track, or control privacy companies.	6/28/2015 1:51 PM
21	this is not in icann 's domain is it? What's next, only icann accredited content on a site?	6/28/2015 10:46 AM
22	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:51 AM
23	Due process per the law of the domain owner's country should be required before revealing any information. The identity of the proxy agency should also be protected under the same rules.	6/28/2015 4:17 AM
24	ICANN should not be in the business of accrediting P/P service providers.	6/28/2015 3:23 AM
25	They should not be regulated	6/28/2015 3:20 AM
26	Unsure	6/27/2015 7:30 PM
27	As long as it is not infringing upon personal privacy, a list of accredited PP services and affiliates seems acceptable.	6/26/2015 12:14 PM
28	I believe ICANN should publish a list of P/P providers that want to be listed and adhere to the rules and guidelines established - maintenance of that list should be minimal. I don't believe it's important that P/P providers declare an affiliation as a requirement for accreditation.	6/25/2015 3:13 PM
29	Accredited P/P providers should be updated at least twice annually.	6/21/2015 7:21 PM
30	ICANN should publish and maintain a publicly accessible list of all UNaccredited P/P service providers who are no longer accredited and the date when they lost their accreditation. We want to know who the bad actors are too!	6/20/2015 10:10 PM

Q14 Do you agree that providing a "designated" rather than a "dedicated" point of contact will be sufficient for abuse reporting purposes, since the primary concern is to have one contact point that third parties can go to and expect a response from? Do you also agree that the designated point of contact should be capable and authorized to investigate and handle abuse reports and information requests received (a standard similar to that currently required for a Transfer Emergency Action Contact under the Inter Registrar Transfer Policy)?(Section 1.3.1 Recommendations 11 & 14, Section 7.1 Category D-2)

Answered: 102 Skipped: 250



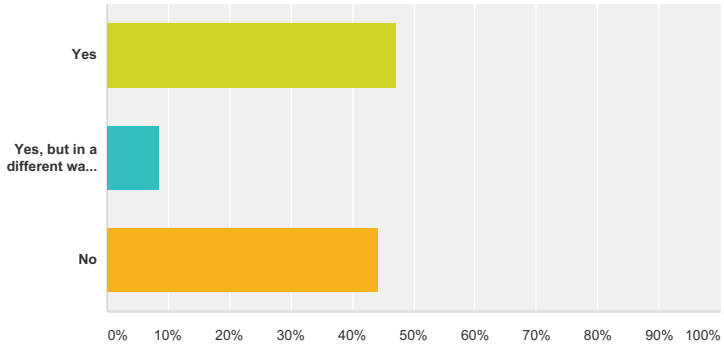
Answer Choices	Responses	
Yes	43.14%	44
Yes, with conditions (please specify what those conditions are in the box below)	11.76%	12
Yes, but not using the TEAC standard from the IRTP (please include alternative suggestions in the box below)	1.96%	2
No	43.14%	44
Total		102

#	Additional Comments	Date
1	And a time limit to respond needs to be set.	7/7/2015 7:22 PM
2	We agree that a "designated" point of contact is sufficient, provided this role is not limited to a single person (but rather is one others can operationally fulfill).	7/6/2015 12:06 PM
3	for me there is no need of a "dedicated contact" to provide a good service. must be clear who is the designated contact and that such contact will be responsive in a timely manner. TEAC standard in my view is suffice to support registrants.	7/6/2015 11:04 AM
4	How does this affect the accreditation process? I'm wary of the combined authority to "investigate and handle" ("handle" being a very vague term). Would rather see a separation of duties, possibly involving third parties.	7/5/2015 2:53 AM
5	This language is unclear; recommendations 10 and 14 appear to be separated deliberately to create ambiguity; and recommendation 14 includes too much content incorporated by reference.	7/5/2015 2:04 AM
6	To hell with the accreditation program in its entirety, thank you very much. We don't need it; besides which it is an offense against the privacy of us, "the people". You should be moving in the opposite direction - towards lessening the amount of personal information required and collected (directly or through registrars / providers) from individual registrants / customers.	7/2/2015 7:16 PM
7	I do not understand what the heck this recommendation even means.	7/2/2015 9:42 AM
8	Horrible idea all around.	7/2/2015 8:54 AM

9	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
10	If the Registrar's criteria has been met, the Disclosure and/or Publication of the WHOIS data to a non-law enforcement third-party should be limited to the equivalent of a Public Records search. For example, in the United States you can search the public business records of the California Secretary of State. A search for Google Inc. discloses the entity name and mailing address. But it does not expose the private email address or phone numbers of the business owner or it's employees. In addition to the basic contact information the public business records search includes the "Agent for Service of Process" which is the legal representative of the entity. I assert the ICANN P/P Service Regulations should adopt a similar policy directing Registrar's to only disclose basic contact information and "Agent for Service of Process" contact information to non-law enforcement third-parties.	7/1/2015 5:51 PM
11	Not above and beyond the normal abuse channel. There is no additional ground for it.	7/1/2015 8:41 AM
12	It should be the sole responsibility of the service provider to maintain contactability.	6/30/2015 11:16 PM
13	The services work as they should currently. It isn't broken so changing it can only make the situation worse.	6/30/2015 9:22 PM
14	Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:47 AM
15	Reservation: I have not reviewed the IRTP, and have no opinion on the second point.	6/29/2015 5:00 PM
16	A P/P service should be able to operate independently of a registrar and thus not be required to be able to take any action with respect to the domain it protects.	6/28/2015 8:54 PM
17	It doesn't fucking matter. You shitheads ignore us anyway.	6/28/2015 6:43 PM
18	In the case of an individual, the designated contact will often be themselves. If the mail can reach them without piercing their privacy shield, it might be ok.	6/28/2015 2:10 PM
19	I believe that only the original domain registrant should be able to authorise disclosure of information and should handle abuse complaints, not a third party.	6/28/2015 7:53 AM
20	I agree that ICANN should be a designated point of contact for abuse reporting and investigation, but I do not think ICANN should have the power to dictate to registrars when and when not data should be released.	6/28/2015 6:23 AM
21	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
22	Designated point of contact may simply be an email address monitored by the company.	6/28/2015 3:20 AM
23	Do not agree with who is able to request info	6/27/2015 7:30 PM
24	Yes I am happy to process abuse reports (I have never received any in 15 years of domain ownership) that are received by email. If someone calls me up on the phone in the middle of the night or shows up at my doorstep they will get abuse from me. Sure if my site is hacked and re-purposed for illegal activity I want to know about it. If someone show up at or call my home when I am at work and my kid is there, well, I would be very angry. So - there is no need ever to publish addresses or phone numbers - or real names - ICANN doesn't do the latter.	6/27/2015 1:10 PM
25	Designated versus dedicated sounds more appropriate.	6/26/2015 12:14 PM
26	I find that many abuse contacts do not take abuse reports seriously at all. They never report back what happened or what action they took.	6/25/2015 2:58 PM
27	Designated point of contact should be regularly reviewed for responsiveness and lose accreditation upon demonstrated lack of responsiveness.	6/21/2015 7:21 PM

Q15 Do you agree with the WG's recommendation that P/P service providers should be fully contactable, through the publication of contact details on their websites in a manner modelled after Section 2.3 of the 2013 RAA Specification on Privacy and Proxy Registrations? (Section 1.3.1 Recommendation 12, Section 7.1 Category D-3)

Answered: 106 Skipped: 246



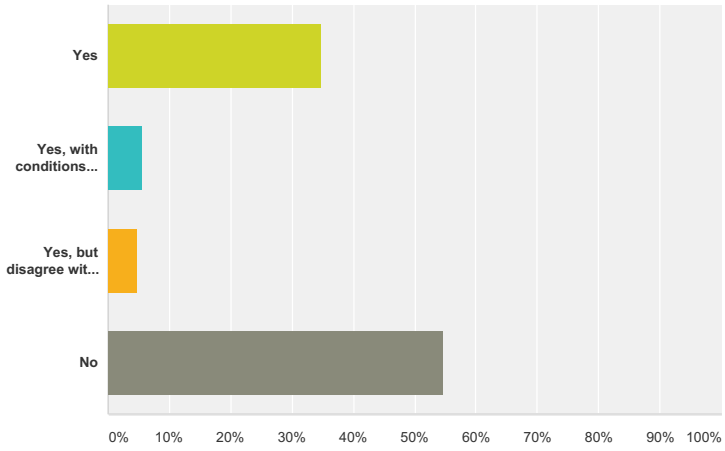
Answer Choices	Responses	
Yes	**47.17%**	50
Yes, but in a different way from what the WG recommends (please provide further details in the box below)	**8.49%**	9
No	**44.34%**	47
Total		**106**

#	Additional Comments	Date
1	And they need to be required to respond in a short period of time.	7/7/2015 7:22 PM
2	of course thinking in a worldwide way there is no better alternative than publicise the full contact, including full address and telephone alternative.	7/6/2015 11:04 AM
3	"Fully contactable" remains undefined (Section 2.3 of the 2013 RAA is a single sentence with sufficient "wiggle room" for minor shenanigans (i.e., the "and/or" piece)).	7/5/2015 2:53 AM
4	This information should be published, but you incorporate by reference a document that makes no reference to this subject. Perhaps you meant that they should use similar standards as registrars?	7/5/2015 2:04 AM
5	To hell with the accreditation program in its entirety, thank you very much. We don't need it; besides which it is an offense against the privacy of us, "the people". You should be moving in the opposite direction - towards lessening the amount of personal information required and collected (directly or through registrars / providers) from individual registrants / customers.	7/2/2015 7:16 PM
6	I have no problem with P/P providers being required to provide accurate contact information, but that's the extent of it.	7/2/2015 9:42 AM
7	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
8	All communication should be subject to review by the registrar offering and the person using the service, as well as subject to approval for any Disclosure or Publication, where not legally binding or forced to do so.	7/1/2015 8:41 AM
9	It should be the sole responsibility of the service provider to maintain contactability.	6/30/2015 11:16 PM
10	Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:47 AM
11	I believe that WHOIS information is generally sufficient for this purpose.	6/29/2015 5:00 PM
12	I support this as a recommendation but not a requirement, as I would for any other commercial business.	6/28/2015 8:54 PM
13	It's unnecessary. The details provided by P/P services in whois databases are more convenient for people who want to contact the registrant anyway.	6/28/2015 4:34 PM
14	Everyone should be permitted to use the web anonymously, especialy companies providing anonymity services.	6/28/2015 1:51 PM
15	I have not read the section in question, so cannot comment to its suitability.	6/28/2015 7:53 AM
16	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:51 AM
17	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
18	Unsure	6/27/2015 7:30 PM

19	by email is fine	6/27/2015 1:10 PM
20	They should be contactable, but not in a way that could facilitate harassment.	6/26/2015 12:14 PM
21	It's up to consumers whether they want to do business with a company they have no way to communicate with. Not up to the likes of the MPAA to decide how businesses provide communication options with consumers.	6/25/2015 3:46 PM
22	This is very important as many times I have been unable to contact a domain owner because the privacy service is completely uncontactable.	6/22/2015 12:20 PM

Q16 Do you agree that a list of the forms of malicious conduct to be covered by a privacy/proxy service provider's designated published point of contact should be included? Do you also agree that these requirements should allow for enough flexibility to accommodate new types of malicious conduct, and that Section 3 of the Public Interest Commitments (PIC) Specification in the New gTLD Registry Agreement or Safeguard 2, Annex 1, of the GAC's Beijing Communique could serve as starting points for developing such a list? (Section 1.3.1 Recommendation 13, Section 7.1 Category D-4)

Answered: 106 Skipped: 246



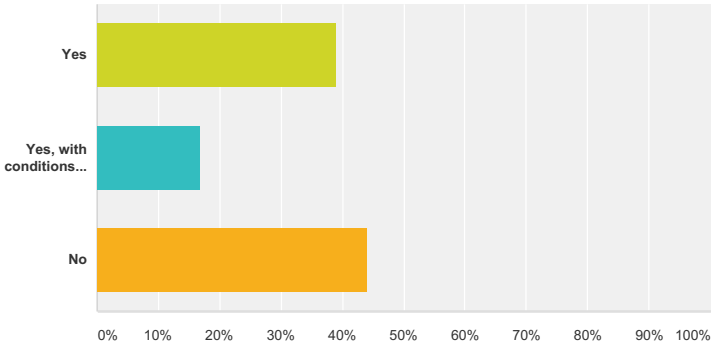
Answer Choices	Responses	
Yes	**34.91%**	37
Yes, with conditions (please specify what those conditions are in the box below)	**5.66%**	6
Yes, but disagree with using either the PIC Specification and/or GAC Safeguard 2, Annex 1 (please provide further details below)	**4.72%**	5
No	**54.72%**	58
Total		**106**

#	Additional Comments	Date
1	I agree that list of the forms of malicious conduct to be covered by a privacy/proxy service provider's point of contact should be included. I disagree that these requirements should be flexible because I believe the WG has not demonstrated historical precedent to justify that these requirements need to be flexible. I disagree with using either the PIC Specification and/or GAC Safeguard 2, Annex 1. More secure software (and anti-malware software) can protect against malware, education can help protect against phishing, etc.	7/8/2015 1:44 AM
2	We disagree that the list of forms of malicious conduct should be limited or defined by third parties. The registry operator's acceptable use policy should be the primary authority for a P/P service provider's actions (such a list may very well be more inclusive). We agree that requirements should be flexible enough to allow additions or deletions as appropriate; we disagree with using Section 3 of the PIC specification and/or GAC Safeguard 2, Annex 1 as a starting point.	7/6/2015 12:06 PM
3	We disagree that the list of forms of malicious conduct should be limited or defined by third parties. The registry operator's acceptable use policy should be the primary authority for a P/P service provider's actions (such a list may very well be more inclusive). We agree that requirements should be flexible enough to allow additions or deletions as appropriate; we disagree with using Section 3 of the PIC specification as a starting point.	7/6/2015 12:06 PM
4	it is clear. no need additional explanation.	7/6/2015 11:04 AM
5	Would recommend identifying host-country limitations as what one country considers illegal may be part of another country's charter (e.g., freedom of speech issues). In some (hopefully rare) cases, involvement the State Department (or other host country equivalent) may be required.	7/5/2015 2:53 AM
6	There should be a documented list, but you cannot incorporate draft recommendations by reference to accomplish this. Requirements must be clear and must be specified at the time of execution of this document. It is reasonable to anticipate future forms of malicious conduct, but a blanket statement such as "any future form of malicious conduct" would outrageous, unenforceable, and a PR nightmare.	7/5/2015 2:04 AM

7	If you can eliminate domain name kiting and domain name speculation, please go ahead with this.	7/4/2015 1:25 AM
8	Privacy providers, proxy providers, and even registrars have no business nosing about in the conduct of customers. That is (already) the responsibility of the hosting service. Do you all hope to become some new self-appointed Internet-police ? Kindly fuck off with that.	7/2/2015 7:16 PM
9	I fail to see the purpose of such a list. If you have valid contact information, that should be the extent of it. If they don't respond, you disable their domains, as you can already do.	7/2/2015 9:42 AM
10	ICANN shouldn't be involved in this aspect AT ALL.	7/2/2015 8:54 AM
11	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:18 AM
12	I believe these kinds of disclosures should be guidelines only, because it is too difficult to make them extensible to cover new types of malicious conduct.	7/1/2015 6:46 PM
13	Malicious conduct should not be covered this way. New forms are found every day, while what may be malicious in one jurisdiction is not malicious in another jurisdiction. Compare US and EU law on privacy, for example. The US privacy law can be called malicious in our view.	7/1/2015 8:41 AM
14	It should be the responsibility of service providers to remove illegal or otherwise malicious content hosted by their service.	6/30/2015 11:16 PM
15	ICANN should not be involved.	6/30/2015 9:22 PM
16	Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:47 AM
17	I object to any open-ended malicious conduct standard being imposed, since such standards are more open to abuse. If changes need to be made as technology changes, they can be adopted through the usual process.	6/29/2015 5:00 PM
18	This should not be applicable: ICANN should not be reviewing or evaluating the content of websites, nor should it be the sole authority over people who do.	6/28/2015 8:54 PM
19	This sounds like bullshit. Who do you think we are?	6/28/2015 6:43 PM
20	Safeguard 2, Annex 1, of the GAC's Beijing Communique is a good starting point, but the list should not be flexible: there should be a specific list of narrow categories of behavior that is prohibited by registrants. The list should not expand to become a vehicle to regulate all prohibited kinds of conduct.	6/28/2015 4:34 PM
21	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:51 AM
22	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
23	Privacy providers should not be required to reveal customer identity except when legally required to do so by the law of the jurisdiction in which they operate. People should not have weaker privacy protections online than they enjoy offline	6/28/2015 3:47 AM
24	Unsure	6/27/2015 7:30 PM
25	I do not feel ICANN should not be creating or in any way participating in defining malicious conduct. This goes to ICANN policing internet behavior and that should be handled by laws and courts.	6/25/2015 3:13 PM

Q17 Do you agree with the WG's recommendation that a standardized form should be developed for the purpose of reporting abuse and submitting requests (including requests for Disclosure of customer information), to also include space for free form text? Do you also agree that privacy/proxy service providers should have the ability to "categorize" reports received, in order to facilitate responsiveness?(Section 1.3.1 Recommendation 15, Section 7.1 Category D-4)

Answered: 100 Skipped: 252



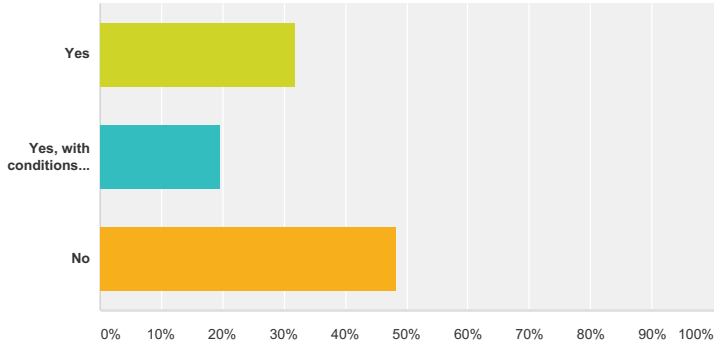
Answer Choices	Responses	
Yes	**39.00%**	39
Yes, with conditions (please specify what those conditions are in the box below)	**17.00%**	17
No	**44.00%**	44
Total		**100**

#	Additional Comments	Date
1	If response is not FIFO they will just ignore the reports they do not want to deal with.	7/7/2015 7:25 PM
2	We disagree that a standardized submission form should be created; each P/P provider should be permitted the latitude to use a form suitable for their own specific services. We disagree that a freeform text option be included. We agree that P/P providers should have the ability to categorize reports if they so choose; however, they should not be required to do so.	7/6/2015 12:40 PM
3	We disagree that a standardized submission form should be created; each P/P provider should be permitted the latitude to use a form suitable for their own specific services. We disagree that a freeform text option be included. We agree that P/P providers should have the ability to categorize reports if they so choose; however, they should not be required to do so.	7/6/2015 12:40 PM
4	templates are really a facilitator to both sides and shall be included, but not with too many specificities that will make it difficult to registrant to report . general categories plus a space to detail it would be suffice. However let me remember that languages availability is essencial. Templates shall be the same to all P/P services and shall come into at least the same languages ICANN is providing to its website. being the same document, costs to have it in the languages provided by ICANN can be diluted among P/P providers.	7/6/2015 11:39 AM
5	Standardised forms should allow option options for circumstances that we haven't dreamed would happen yet. I've hit form submissinos where I couldn't actually submit my complaints because the form was too rigid.	7/5/2015 2:34 AM
6	Putting "conditions" in quotes, and not defining any, suggests that you don't know what they might be. By writing this recommendation in the passive voice, it seems that you are delegating this standardization to the P/P organizations. If you intend to develop this form, you must say so explicitly.	7/5/2015 2:20 AM
7	Standardized forms are nice, if you must, but no category, nor any submission, should ever trigger any automated or automatic action against the customer / against the customer's services.	7/2/2015 7:28 PM
8	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
9	Privacy/proxy service providers should have the ability to "categorize" reports received, but should not be required to.	7/1/2015 6:53 PM
10	Not beyond the normal abuse form already present.	7/1/2015 8:50 AM
11	It should be the sole responsibility of the service provider to handle these requests, but if a separate form is created elsewhere to make it easier for people to file abuse reports, this is acceptable.	6/30/2015 11:19 PM

12	Just let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:48 AM
13	I do not believe a standard form is necessary, but one may be tried on a voluntary basis. No objection to categorizing reports.	6/29/2015 5:22 PM
14	No opinion.	6/28/2015 8:57 PM
15	Now you're just making shit up.	6/28/2015 6:44 PM
16	The only process for violating privacy should be the existing legal processes.	6/28/2015 1:53 PM
17	if the text is required to be sent together with the rest of the request to the customer	6/28/2015 12:34 PM
18	Disclosure should not be without the knowledge of the original registrant.	6/28/2015 7:56 AM
19	This one sounds legit.	6/28/2015 7:52 AM
20	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
21	Do not agree with persons able to make requests	6/27/2015 7:35 PM
22	I don't think enough reports are received to warrant special categories. I have not received one report in 15 years and with about 10 domains.	6/27/2015 1:22 PM
23	As long as it does not facilitate harassment, again.	6/26/2015 12:17 PM
24	This standard could be offered for use and P/P providers may even be required to accept them to become accredited. However, I believe the level of responsiveness is beyond the purview of ICANN.	6/25/2015 3:27 PM
25	But requests for Disclosure should be restricted to FTC, spamcop and Spamhaus unless there is a Court Order.	6/25/2015 2:58 PM
26	A very high priortiy should be focused on third parties' ability to report copyright infringement, malicious or libelous content, "revenge porn" and other damaging content -- all of which should be prioritized for immediate (or very quick) takedown.	6/21/2015 7:27 PM

Q18 Do you agree with the WG's recommendation concerning the relaying of electronic communications? Namely, that: (1) All communications required by the RAA and ICANN Consensus Policies must be forwarded; and (2) For all other electronic communications, P/P service providers may elect one of the following two options:i. Option #1: Forward all electronic requests received (including those received via emails and via web forms), but the provider may implement commercially reasonable safeguards (including CAPTCHA) to filter out spam and other forms of abusive communications, orii. Option #2: Forward all electronic requests received (including those received via emails and web forms) received from law enforcement authorities and third parties containing allegations of domain name abuse (i.e. illegal activities)? Do you also agree that P/P service providers must publish and maintain a mechanism (e.g. designated email point of contact) for Requesters to contact to follow up on, or escalate, their original requests? (Section 1.3.1 Recommendation 16, Section 7.1 Category E)

Answered: 97 Skipped: 255



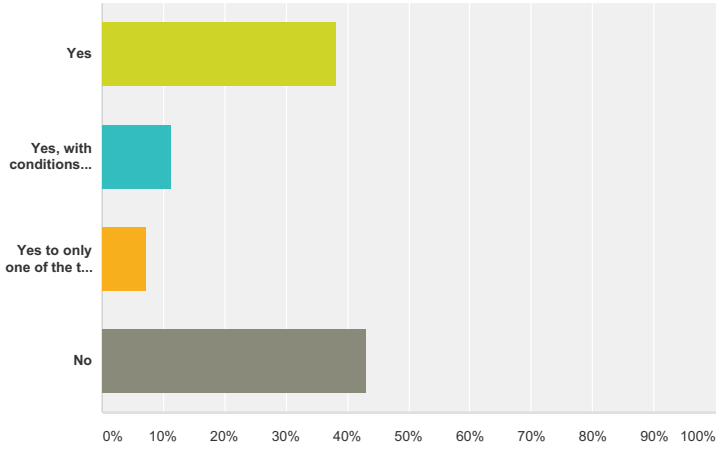
Answer Choices	Responses	
Yes	**31.96%**	31
Yes, with conditions (please specify what those conditions are in the box below)	**19.59%**	19
No	**48.45%**	47
Total		**97**

#	Additional Comments	Date
1	The WG should clarify the escalation mechanism. I believe the requester, not the customer, should bear any escalation fee.	7/8/2015 2:03 AM
2	SPAM filtering can not be allowed, spam complaints, containing spam being reported, will get filtered.	7/7/2015 7:25 PM
3	Yes: (1) All communications required by the RAA and ICANN Consensus Policies must be forwarded; and No: (2) For all other electronic communications, P/P service providers may elect one of the following two options: P/P providers and customers should have the option to elect which information should be forwarded; such scenarios should not be limited to these two options. Yes: Do you also agree that P/P service providers must publish and maintain a mechanism (e.g. designated email point of contact) for Requesters to contact to follow up on, or escalate, their original requests?	7/6/2015 12:40 PM
4	P/P providers and customers should have the option to elect which information should be forwarded; such scenarios should not be limited to these two options.	7/6/2015 12:40 PM

5	there is no full security that using option #1 will guarantee there will not be abusive communication and this may be clearly stated in its agreements - reasonable safeguards shall be enough to the registrant.	7/6/2015 11:39 AM
6	In option #2: Only mail received from law enforcement authorites should be forwarded. No third parties.	7/5/2015 6:12 PM
7	Option #1 is preposterously broad and should be eliminated. Option #2, in speaking of third parties alleging any form of illegal activity, ignores the concept of due process. All I would have to do is file a form that says "he put a music file on his site" and I could pierce the P/P protection. The P/P provider must have the authority (under penalty of law, if abused) to protect common domain owners from vast third-party bots with canned "illegal activity" language.	7/5/2015 2:20 AM
8	Agreed on 1. Agreed on 2 if and ONLY if requests are made by a human (electronically, by voice, or by phone) who can clearly describe their need to communicate. Automated correspondence such as machine-generated notifications should be discarded. Disagreed on escalation mechanisms.	7/4/2015 1:33 AM
9	Seriously? You want to leave the courts out of this process? Are you on crack?	7/2/2015 8:59 AM
10	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
11	I do not want spam in any case.	7/1/2015 7:05 PM
12	For Option #2, law enforcement authorities and third parties act on allegations of domain name abuse, whether justified or not, and forcing forwarding of electronic requests could create an avenue for harassment of individual clients of P/P service providers.	7/1/2015 6:53 PM
13	Option #2 with the exclusion of 3rd parties, and the right for registrars to filter commercial offers to the end user and person using the service. Allegations of illegal activities must follow the normal abuse procedure.	7/1/2015 8:50 AM
14	It should be the sole responsibility of the service provider to maintain contactability and no one else should be imposing this.	6/30/2015 11:19 PM
15	This would destroy a legitimate safeguard that protects small business.	6/30/2015 9:30 PM
16	We do not need a controlled list of privacy/proxy service providers at all. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:48 AM
17	I believe the general concept is reasonable here, but would benefit from refinement. OK as recommendation to providers; not yet OK as mandate for providers.	6/29/2015 5:22 PM
18	What communications should be relayed and how is between the P/P service and the user of that service. I do not support any measures imposing restrictions on this.	6/28/2015 8:57 PM
19	Fuck you.	6/28/2015 6:44 PM
20	Option #1 and #2 are too limiting. P/P service providers should be given the flexibility to decide which level of filtering they wish to offer their customers. For example, a P/P service provider may block allegations of abuse that are not substantiated.	6/28/2015 11:46 AM
21	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:52 AM
22	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
23	P/P service providers shouldn't exist, but if they do, it shouldn't be up to them to participate in escalation.	6/28/2015 2:52 AM
24	Do not agree with law enforcement authority as defined	6/27/2015 7:35 PM
25	I have no objection to recieving any requests from law enforcement about allegations. But this is interesting - what if my site is hacked and is now hosting say illegal material - I see this and delete the content refresh the server etc. Then am I going to be prosecuted for destroying evidence? Because - in the UK at least possession of 'child porn' is a strict liability offence. So if I observe files on there that shouldn't be there (content unknown) I am legally safe if I delete them without knowing their contents. If I find out or know what is in the files then this would potentially be evidence against me. Even the US government has been well and truly hacked so this is not outside the bounds of possibility.	6/27/2015 1:22 PM
26	For (2), P/P need to be compelled to use a safeguard against spam, not to be just an option.	6/26/2015 1:04 PM
27	Agree only with recommendation 1. Customers should have full transparency on third party requests for their identity or other information.	6/26/2015 4:08 AM
28	Except the requirement that service providers have followup capability. Again, that should be up to the service provider.	6/25/2015 3:54 PM
29	Forwarding of electronic communications is important but privacy is more important. This must be considered when creating these policies else the internet becomes like George Orwell's novel 1984.	6/25/2015 3:27 PM
30	I completely disagree with Option #2 The very LAST thing you should be doing is giving the domain owner details of the person accusing the abuse. To a spammer a domain is disposable, what they LOVE to know is that an email is active, this increases the price they can sell the email for. The obvious middle ground here is Spamcop and Spamhaus When you report spam to Spamcop they resolve links determine who the spammer is. What is BAD is that some companies (even big companies like GoDaddy) ignore the abuse reports so all spamcop can do is record the information for stats.	6/25/2015 2:58 PM
31	The user of the privacy service should be able to indicate how they want communications and which communications (excluding RAA and ICANN communications). In addition, any captcha system should be required to be accessible to anyone regardless of ability to include the use of audio captcha and math captcha. the W3 web accessibility ggroup could advise further on this point.	6/22/2015 12:40 PM

Q19 Do you agree with the WG's recommendation that: (1) all third party electronic requests alleging abuse by a P/P service customer will be promptly forwarded to the customer; and (2) a Requester will be promptly notified of a persistent failure of delivery that a P/P service provider becomes aware of? [In answering this question, please feel free to provide additional guidance to the WG as to what would constitute a "persistent delivery failure" beyond what is stated in the Initial Report](Section 1.3.1 Recommendation 17, Section 7.1 Category E)

Answered: 97 Skipped: 255



Answer Choices	Responses	
Yes	**38.14%**	37
Yes, with conditions (please specify what those conditions are in the box below)	**11.34%**	11
Yes to only one of the two recommendations (please specify which, and why, in the box below)	**7.22%**	7
No	**43.30%**	42
Total		**97**

#	Additional Comments	Date
1	The WG should clarify what a persistent delivery failure is.	7/8/2015 2:03 AM
2	I'd have to see some consensus on numbers of attempts and "a reasonable period of time" as mentioned, in order get an idea of how open to abuse it would be.	7/6/2015 7:02 PM
3	We disagree with these recommendations, as they are too broad and allow for abuse of the proposed system. The community has seen that, while P/P services may provide shelter for a certain number of registrants that abuse the domain name system, there also is proven abusive behavior on the part of self-designated (but not authoritative) "policing" entities. Instead, legitimate requests alleging abuse (as determined by P/P provider) may be forwarded.	7/6/2015 12:40 PM
4	We disagree with these recommendations, as they are too broad and allow for abuse of the proposed system. The community has seen that, while P/P services may provide shelter for a certain number of registrants that abuse the domain name system, there also is proven abusive behavior on the part of self-designated (but not authoritative) "policing" entities.	7/6/2015 12:40 PM
5	the report states a reasonable definition of what represents Persistent delivery failure.	7/6/2015 11:39 AM
6	(1) Third party requests should be forwarded only if the customer has elected to have all requests forwarded.	7/5/2015 6:12 PM
7	Whatever definition is finally evolved it should not, in effect, provide a loophole which would allow malefactors materially to extend the period of their inappropriate activity. If all parts of the chain are made aware of the criticality of these processes then they will know the importance of responding promptly to them and the potential consequnces of not so doing.	7/5/2015 12:33 PM
8	1. Disagree; see above. "Third-party allegation" is an unacceptably low bar and must be recast. 2. Agree; a properly vetted complaint should have an escalation path if delivery fails.	7/5/2015 2:20 AM

9	Agreed to 1 provided these requests are made on a case-by-case basis by a human. Automated notifications of abuse should be discarded. Disagreed on 2: if someone chooses to ignore communication they should be free to choose to do so. If the registration holder is in violation of the law, traditional means of enforcement should be used, modeled after United States due process and the concept of "innocent until proven guilty." When someone breaks laws they can be subject to arrest or a lawsuit, same as with other venues for committing crime.	7/4/2015 1:33 AM
10	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
11	I think this opens up the opportunity for frivolous harassment of P/P service provider Clients.	7/1/2015 6:53 PM
12	If included, this is not a privacy service anymore. Anybody alleging abuse is way too broad and intrusive. The feedback of delivery failure goes to the registrar or P/P service provider. They will find alternative means. It is not the right of the Requester to know so, nor should it be.	7/1/2015 8:50 AM
13	1 is OK. 2 is unclear what counts as failure, and hence is prone to abuse.	6/30/2015 9:30 PM
14	We do not need over reaches like what's being proposed. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:48 AM
15	OK as recommendation to providers, not OK as mandate to providers. Providers must have discretion to refuse requests, for example if the request facility itself is being abused.	6/29/2015 5:22 PM
16	As above. The nature of relay service is between the P/P provider and its user, and it's for them to determine the conditions of that service.	6/28/2015 8:57 PM
17	Your days are numbered.	6/28/2015 6:44 PM
18	I only agree with part 1.	6/28/2015 6:01 PM
19	Persistent delivery failure should not happen after only one method of communication fails. P/P providers should attempt to contact the registrant using at least two methods of communication, and they should allow the registrant a reasonably amount of time to reply. (Unless, for example, the email bounces or their phone line is disconnected.)	6/28/2015 4:45 PM
20	If they're not getting through right now, the P/P provider is either incompetent or it's because they are screening vexatious emails that are known to be from bad actors. (1) would provide a hijack that forces emails to be delivered.	6/28/2015 2:17 PM
21	Agree with #1. #2, I would want a a long enough time definition of "persistent" to be sure it's not a transient failure of an email server.	6/28/2015 12:58 PM
22	"Persistent delivery failure" would include e.g. multiple emails bouncing, in which case telephoning or writing to the registrant would be appropriate.	6/28/2015 7:56 AM
23	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:52 AM
24	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
25	Unsure	6/27/2015 7:35 PM
26	I would be concerned about veracious abuse allegations being reported over and over. For example Microsoft sent legal threats to MikeRoweSoft - belonging to Mike Rowe... that should be dismissed.	6/27/2015 1:22 PM
27	Yes, very promptly forwarded to the customer.	6/26/2015 12:17 PM
28	Only the first recommendation.	6/26/2015 4:08 AM
29	Promptly should be 30 to 60 days after initial attempt. You must provide adequate time and air on the side of fairness. Anything shorter could be the result of holidays, vacations, illness, etc.	6/25/2015 3:54 PM
30	Forwarding of electronic communications is important but privacy is more important. This must be considered when creating these policies else the internet becomes like George Orwell's novel 1984.	6/25/2015 3:27 PM
31	A persistant failure of delivery could be a bounced email for over 72 days, because if the email is on a domain that has expired then the user might recover the domain within that period. After that is goes to auction.	6/25/2015 2:58 PM
32	Persistent failure to me would be a failure of the message to be delivered after five attempts with one attempt made every 24 hours. At that point the privacy provider should initiate the verification procedures. I also think that the requestor should be notified after the fifth failure that the registrant cannot be contacted and then be given the protected whois information so that they can follow up via postal mail or other contact methods.	6/22/2015 12:40 PM

Q20 The WG has not yet reached consensus on mandatory next steps for a privacy/proxy service provider regarding the escalation of relay requests. What should be the minimum mandatory requirements for escalation of relay requests in the event of a persistent delivery failure of an electronic communication? What is your view of the current language under consideration by the WG?(Section 1.3.2, Section 7.1 Category E)

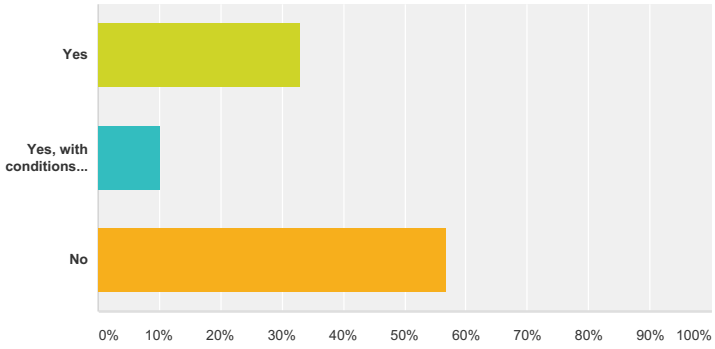
Answered: 48 Skipped: 304

#	Responses	Date
1	I believe the requester, not the customer, should bear any escalation fee.	7/8/2015 2:03 AM
2	pompt domain cancelation should be the punishment.	7/7/2015 7:25 PM
3	It's Fine	7/7/2015 9:27 AM
4	The language seems appropriate, as long as providers exercise their right to limit requests of this nature - repeated malicious requests in order to incur recovery costs on the customer seems a plausible abuse vector, in light of the many spurious uses of DMCA takedown requests and similar systems.	7/6/2015 7:02 PM
5	There should not be a minimum mandatory requirement for escalation of relay requests.	7/6/2015 12:40 PM
6	There should not be a minimum mandatory requirement.	7/6/2015 12:40 PM
7	The provider must upon request forward a further form of notice to its customer. A provider should have the discretion to select the most appropriate means of forwarding such a request.	7/6/2015 12:12 PM
8	my belief is that after a request , the provider SHOULD forward a further form of notice to its customer. I am in favor to charge a reasonable fee. normally fees discourage abusive actions.	7/6/2015 11:39 AM
9	Do nothing in the event of delivery failure.	7/6/2015 3:26 AM
10	The P/P service provider _should_ request the registrant verify his or her contact information. The cost of forwarding materials to the customer (the registrant of the domain) should be borne by the requester (the party wishing to contact the customer), not the customer or the P/P service provider.	7/6/2015 12:12 AM
11	I agree	7/5/2015 8:31 PM
12	I'm not comfortable that "reasonable fee" is defined by one party and imposed on another. Recommend that "reasonable fee" be defined in the site's terms of service and specific limitations be included.	7/5/2015 2:57 AM
13	Subject to the legitimacy requirements I reiterate here, the existing language is reasonable with the prepending of a forward to postmaster@domain, whose existence is required by RFC.	7/5/2015 2:20 AM
14	No escalation. If a registration holder ignores the communication, a public court-ordered subpoena may be served.	7/4/2015 1:33 AM
15	As stated already, we have no need and no want for this bullshit accreditation system. The WG ought consider finding something else - preferably of actual value to society - to do with their time.	7/2/2015 7:28 PM
16	I fail to see the problem. If the P/P or real holder choose not to reply, you already have tools in place to disable domain names. What more do you want?	7/2/2015 9:46 AM
17	It's already too invasive. This needs to be dropped.	7/2/2015 8:59 AM
18	Minimum mandatory requirements regarding the escalation of relay requests should be probable cause from a law enforcement agency.	7/1/2015 6:53 PM
19	5 attempts over a period of 15 business days should be used as a minimum threshold before determining a delivery failure. I agree with the language in Section 7.1 Category E.	7/1/2015 6:24 PM
20	Relay requests should not follow different rules or paths compared to regular information requests as part of investigating abuse and/or illegal behaviour.	7/1/2015 8:50 AM
21	None	6/30/2015 10:48 AM
22	If there is no consensus on minimum mandatory requirements, then no minimum mandatory requirements should be imposed at this time.	6/29/2015 5:22 PM
23	No minimum mandatory requirements.	6/29/2015 12:17 AM
24	As above, this is between the P/P service provider and the user. There should be no mandatory requirements about relay service.	6/28/2015 8:57 PM
25	Serivce provider to act as an intermediary when source email IP's or domains are RBL'd causing delivery failures. For example, I blackhole all mail from IP space in CN, KR, and other countries because of spam and hacking.	6/28/2015 8:36 PM
26	5	6/28/2015 3:06 PM
27	There should be no ecalation of requests beyond existing legal channels.	6/28/2015 1:53 PM
28	you are trespassing legal territory here	6/28/2015 10:50 AM
29	full disclosure	6/28/2015 9:23 AM

30	No comment	6/28/2015 7:56 AM
31	N/A	6/28/2015 7:52 AM
32	A court order should be the minimum mandatory requirement for escalation of relay request in the event of persistent delivery failure of communication or perpetual unavailability of the client/end-user.	6/28/2015 5:14 AM
33	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
34	I don't agree that mandatory requirements for escalation are necessary	6/28/2015 3:24 AM
35	Privacy / Proxy Service Providers should not need to answer abuse emails or otherwise this alone will cause the internet to break down to a he said she said.	6/28/2015 3:09 AM
36	Unsure	6/27/2015 7:35 PM
37	I am sure that ICANN does not care less for registrants privacy	6/27/2015 1:22 PM
38	not sure	6/27/2015 12:23 PM
39	It is sometimes difficult to contact providers and receive timely responses. There should be a high mandatory minimum behind persistent delivery failures, maybe 5 or more attempts.	6/26/2015 12:17 PM
40	The requester has the option to send a physical letter which would be forwarded to the registrant by the service provider via certified mail.	6/25/2015 3:54 PM
41	I feel one attempt to relay a message is sufficient and not always possible or required. The sovereign laws of a country are more important than a companies interests.	6/25/2015 3:27 PM
42	Do not assume you are dealing with domain professionals. The other day I was helping a dentist, he had a guy who was managing his domains and thought he had done it, then could not get hold of him for months.	6/25/2015 2:58 PM
43	minimum mandatory requirements for escalation of relay requests should be 100	6/25/2015 1:20 PM
44	The language looks fine to me; I prefer 'should' over 'must', approve of limits on requests, and am ambivalent on cost recovery.	6/24/2015 7:54 PM
45	Privacy/proxy service providers should have, in addition to an email address, other validated contact information for its customers, such as a telephone number. Failure to obtain contact with a customer after a period of 15 days through any means by a privacy/proxy service provider, should trigger escalation of a relay request.	6/24/2015 1:31 PM
46	I agree with the term "must" in the language under consideration. Furthermore, if a persistent failure has taken place I agree that the p/p should send further communications at the request of the requester and that the customer, not the requester pay the cost. Once the persistent failure has taken place the p/p should have 30 days to send further contact requests and conduct domain contact verification. During this escalated contact period the requester should be able to work directly with someone at the p/p to facilitate the request process. I think some form of fee is also appropriate for failing to respond to the p/p during the escalated period.	6/22/2015 12:40 PM
47	5 calendar days for first response, 2 calendar days on second request. It's easy enough to fix/delete/edit website content. It's also easy and fast to put a site back online. If there's no initial response and then no secondary response, take the site down.	6/21/2015 7:27 PM
48	There should be no requirements	6/20/2015 2:17 PM

Q21 Do you agree with the WG's recommendation that when a P/P service provider becomes aware of a persistent delivery failure to a customer, that will trigger the provider's obligation to perform a verification/re-verification (as applicable) of the customer's email address(es), in accordance with the WG's recommendation that customer data be validated and verified in a manner consistent with the WHOIS Accuracy Specification of the 2013 RAA? (Section 1.3.1 Recommendation 17, Section 7.1 Category E)

Answered: 97 Skipped: 255



Answer Choices	Responses	
Yes	**32.99%**	32
Yes, with conditions (please specify what those conditions are in the box below)	**10.31%**	10
No	**56.70%**	55
Total		**97**

#	Additional Comments	Date
1	A P/P service provider and a customer can communicate with each other via means other than those specified in the Initial Report, so the WG should not mandate any particular form of contact information. For example, a customer can log into a Web site of the P/P service provider to receive or send messages.	7/8/2015 2:03 AM
2	We disagree with this recommendation. It is the obligation of the registrar to validate a Whois record according to the terms of the 2013 RAA. The recommendation, as worded, opens the door to constant re-verification of a record based on failure of delivery that could be caused by multiple reasons (not related to an inaccurate Whois record).	7/6/2015 12:40 PM
3	We disagree with this recommendation. It is the obligation of the registrar to validate a Whois record according to the terms of the 2013 RAA. The recommendation, as worded, opens the door to constant re-verification of a record based on failure of delivery that could be caused by multiple reasons (not related to an inaccurate Whois record).	7/6/2015 12:40 PM
4	sure, re-verification shall be a normal process when facing persistent delivery failure.	7/6/2015 11:39 AM
5	Subject to my prior conditions of legitimacy and attempt to reach postmaster@domain, the language seems reasonable.	7/5/2015 2:20 AM
6	Provided the re-verification takes place no more than once during each year (term) of domain name registration, this makes sense. Otherwise these requests could become a denial-of-service in an attempt to garner a response.	7/4/2015 1:33 AM
7	Stay out of the P/P business. Believe me, once my domain gets disabled, you *will* hear from me.	7/2/2015 9:46 AM
8	Whois is a useless database that only serves to aid stalkers and those with malicious intent in discovering the personal data of a domain name registrant.	7/2/2015 8:59 AM
9	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
10	dont know	7/1/2015 7:05 PM
11	Only due to delivery of authorized parties, not 3rd parties alleging abuse. Otherwise, this recommendation is open for abuse by 3rd parties suspecting a temporary e-mail failure and seizing the opportunity to disable the domain name. Efforts for P/P service provider within commercial reason.	7/1/2015 8:50 AM

12	Spam issues are a serious problem as described before. My registrant emails were all destroyed when I transferred away from Godaddy and godaddy lifted my privacy. Failure to respond is not lack of good will. Spam issues must be tackled and solved. Response forms may be one solution, instead of publishing emails.	7/1/2015 4:57 AM
13	This should be solely the responsibility of the provider.	6/30/2015 11:19 PM
14	As failure is not defined, this is prone to abuse. Needs clarification.	6/30/2015 9:30 PM
15	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:48 AM
16	Email is not a guaranteed delivery mechanism! Allowing third parties to trigger verification and potentially cause suspension of registration is a denial-of-service mechanism with nontrivial chance of success. The continued operation of a website should not depend on the whims of the email provider's spam filter.	6/29/2015 5:22 PM
17	Non-applicable, as above.	6/28/2015 8:57 PM
18	Service provider to contact registrant for explanation prior to reverification.	6/28/2015 8:36 PM
19	It's not clear what benefit this would provide.	6/28/2015 4:45 PM
20	This would risk the privacy and safety of those who need it most, and provide an excuse for stealing domains.	6/28/2015 1:53 PM
21	Not all domains have email.	6/28/2015 9:23 AM
22	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:52 AM
23	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
24	P/Ps should not be forced to police their customers on behalf of others.	6/28/2015 3:24 AM
25	ffs calm down with the millions of questions	6/27/2015 9:53 PM
26	Unsure	6/27/2015 7:35 PM
27	How many of these are we talking about?	6/27/2015 1:22 PM
28	If the appropriate amount of attempts occurred.	6/26/2015 12:17 PM
29	Absolutely not. It's up to the consumer to make sure they update their records, if necessary.	6/25/2015 3:54 PM
30	I think full contact verification should take place not just of the email address.	6/22/2015 12:40 PM
31	email and/or phone.	6/21/2015 7:27 PM

Q22 What are your views on the WG's recommended illustrative Disclosure Framework (Annex E of the Initial Report) for IP rights-holders? Note that the proposal contains some alternative language formulations not yet finalized by the WG.(Section 1.3.1 Recommendation 19, Section 7.1 Category F and Annex E)

Answered: 53 Skipped: 299

#	Responses	Date
1	I.B.iv. The WG should clarify what a "streamlined process" would be. III.A. Customers should have at least 60 calendar days to respond. III.D. Privacy/proxy services should be able to refuse disclosure solely for lack of (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; P/P service providers should be able to refuse to disclose solely based on the fact that the request is founded on alleged intellectual property infringement in content on a website associated with the domain name.	7/8/2015 2:33 AM
2	'cost recovery' from complainants? really??? Another way tof a bad P/P to delay, deny, and profit.	7/7/2015 7:31 PM
3	Any are fine.	7/7/2015 9:32 AM
4	Preference for the wording: [a reasonable basis for believing (i) that it is not infringing the Requester's claimed intellectual property rights, and/or (ii) that its use of the claimed intellectual property is defensible], as long as appropriate follow-up guidelines are established for preventing abuse by customers "playing dumb".	7/6/2015 7:32 PM
5	This recommendation is very troubling (particularly, D. Disclosure cannot be refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; nor can refusal to disclose be solely based on the fact that the request is founded on alleged intellectual property infringement in content on a website associated with the domain name). As has been the case in prior attempts, this is an attempt by rights holders to compel providers to either hand over client information without due process and/or to adjudicate their clients' usage of potentially trademarked or copyrighted terms. We disagree with such efforts and again state that due process is central to any effort to compel registrant or provider behavior.	7/6/2015 12:57 PM
6	This recommendation is very troubling. As has been the case in prior attempts, this is an attempt by rights holders to compel providers to either hand over client information without due process and/or to adjudicate their clients' usage of potentially trademarked or copyrighted terms. We disagree with such efforts and again state that due process is central to any effort to compel registrant or provider behavior.	7/6/2015 12:57 PM
7	Disclosure to be made only upon a court order.	7/6/2015 12:20 PM
8	item b- I am in favor of the word: "encouraged but not required to" item c : "sufficient" is a better word than the 2 other alternatives	7/6/2015 11:56 AM
9	Unacceptable in any form. IP rights are no justification for any changes to the whois system and rules that would affect privacy and freedom of domain holders.	7/6/2015 3:29 AM
10	The report did not make a compelling case that IP holders should have their claims handled in higher-priority manner than other claimants (libel litigants, journalists, etc.). IP holders should use the same, standard mechanism for private domain registrant contacts. Service provider should be encouraged, but not required to, manage access to the Request submission process (Annex E, I. , B.)	7/6/2015 12:27 AM
11	I agree	7/5/2015 8:37 PM
12	IP rights-holders are not LEA, and therefore should not be able to request publication or disclosure. Intellectual property is very complex and it is not the provider's role to judge such cases.	7/5/2015 6:32 PM
13	Would recommend inclusion of temporal data (e.g., when domain was acquired, when trademark was granted). Have seen at least one attempt to seize a long-standing domain via use of a recently appointed trademark.	7/5/2015 3:07 AM
14	In Annex E, Sections A and B seem defensible. I am completely opposed to section C, allegation of trademark violation on web site; a statement such as "Mickey Mouse is a filthy rat" would qualify under this section. In the circumstance of section C, personal information should be disclosed only under court order or as part of a legal proceeding.	7/5/2015 2:36 AM
15	I do not believe that any disclosure conditions, beyond those involving traditional venues (courts of law, courts of tort) should be included for intellectual property concerns.	7/4/2015 1:38 AM
16	ARGH! It is NOT your job to chase down supposed IP infringement! So frustrating! ICANN is not a law-enforcing body, and the recommendations you're making do NOTHING for individuals like myself.	7/2/2015 9:48 AM
17	Honestly, you need to drop this completely.	7/2/2015 9:05 AM
18	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
19	If the Registrar's criteria has been met, the Disclosure and/or Publication of the WHOIS data to a non-law enforcement third-party should be limited to the equivalent of a Public Records search. For example, in the United States you can search the public business records of the California Secretary of State. A search for Google Inc. discloses the entity name and mailing address. But it does not expose the private email address or phone numbers of the business owner or it's employees. In addition to the basic contact information the public business records search includes the "Agent for Service of Process" which is the legal representative of the entity. I assert the ICANN P/P Service Regulations should adopt a similar policy directing Registrar's to only disclose basic contact information and "Agent for Service of Process" contact information to non-law enforcement third-party.	7/1/2015 8:27 PM
20	I think the language is too loose, and opens individuals up to frivolous litigation from IP rights owners and third-party agencies whose contracted relationship is to expand IP brand presence.	7/1/2015 6:58 PM

21	This disclosure framework destroys any privacy the person using the service may have had. When refusing the request to disclose. This is ludicrous.	7/1/2015 8:55 AM
22	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:49 AM
23	It allows too much leeway for rights-holders, who already have a lot of opportunities for misusing the rights they are already granted. In particular, laying the burden of proof on the accused is not acceptable, and will likely be abused as the DMCA is.	6/29/2015 1:24 PM
24	These types of communication should not have any special treatment over other types. Existing legal procedures do not require assistance from what should be a neutral service provider.	6/28/2015 9:02 PM
25	Existing legal systems handle these issues just fine.	6/28/2015 6:03 PM
26	It provides no way of "blacklisting" IP holders that use the process abusively. (For example, AF HOLDINGS, LLC, v. DOES 1 – 1058) There should be a global blacklist of "vexatious litigants" maintained by ICANN, and a P/P provider responding to a request from one of these organizations would not be required to disclose any information about their customers.	6/28/2015 5:17 PM
27	Fuc{ off	6/28/2015 4:48 PM
28	This attempts to set up large companies as the owners of the internet with a kangaroo court for destroying any internet services and individuals they do not care for.	6/28/2015 1:57 PM
29	I think all of the ideas are terrible given access via court order is already in existence and there is no need to make it easier.	6/28/2015 1:21 PM
30	A valid court order should be required for disclosure.	6/28/2015 12:40 PM
31	The recommendation imposes too much burden on the service provider to determine if the request is with or without merits. Such determination should not be the role of the service provider, and should be left to the judicial process.	6/28/2015 11:56 AM
32	No comment	6/28/2015 7:56 AM
33	They are too invasive and make you look like you are beholden to the police state	6/28/2015 7:53 AM
34	Bullshit.	6/28/2015 5:15 AM
35	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
36	"Rights holders" should be required to use legal processes (i.e. file a lawsuit, seek a court order) if they believe their rights are being violated. There should not be any additional rules beyond what the law already provides.	6/28/2015 3:50 AM
37	It's impossible for a domain name itself to infringe IP rights since even copyrighted or trademarked words and phrases may legitimately be used for criticism, complaint, parody, and other legitimate purposes. If someone hates Ford cars, they should be able to use fordcarsblow.com. If someone things Star Wars is dumb, they should be able to use theforceisafarce.com. If someone hates GW Bush, they should be able to use gwbush.com if it was unregistered when they registered it. Therefore there should not be any process to disclose registrants or suspend domains at the behest of IP rights holders - any IP issue would be an issue of CONTENT, not the domain name itself, and should be taken up with site's host or owner, not with ICANN or the person or entity who registered the domain name. ICANN should not be concerned with content and not participate in issues having to do with content rather than domain names themselves.	6/28/2015 3:33 AM
38	Disagree	6/28/2015 3:25 AM
39	?	6/27/2015 9:53 PM
40	Can not agree if the terms have yet to be defined	6/27/2015 7:37 PM
41	As long as it costs some money to the one who wants to know the details.	6/27/2015 1:25 PM
42	not sure	6/27/2015 12:23 PM
43	A steaming pile of cow excrement.	6/26/2015 11:50 PM
44	IP rights-holders should have no interaction with the domain system, including P/P. The only way that this interaction must happen is through the justice system, not directly.	6/26/2015 1:10 PM
45	Anything that compromises privacy should be avoided.	6/26/2015 12:20 PM
46	No disclosure or publication.	6/26/2015 4:09 AM
47	I think that this is a very tricky area to navigate. The safeguards that have been put in are reasonable. Copyright can be very difficult to ascertain legally from the copyright owner perspective but making it onerous for the copyright owner is justified in avoiding abouse of this system.	6/25/2015 6:50 PM
48	No opinion, you didn't provide the text to be reviewed.	6/25/2015 3:57 PM
49	It is never acceptable to disclose a persons information absent a court order specifically requiring that action. To do anything else erodes the fabric of the internet.	6/25/2015 3:34 PM
50	I strongly agree with the requirement that the sworn statement provide a basis for believing that the alleged infringement is indefensible, rather than simply alleging infringement. Section (III) clause D should be struck. A P/P provider should be free to only disclose customer details when served with valid legal process from a court with jurisdiction.	6/24/2015 8:10 PM
51	None	6/22/2015 12:50 PM
52	.	6/21/2015 7:28 PM
53	I disagree with any disclosure to copyright holders.	6/20/2015 2:20 PM

Q23 The WG's illustrative Disclosure Framework currently applies only to IP (i.e. trademark or copyright) rights-holders. Please provide your views on the applicability of a similar framework or policy to other types of requesters. In particular, please provide your views on the following specific questions:(1) Should it be mandatory for accredited P/P service providers to comply with express requests from LEA in the provider's jurisdiction not to notify a customer? (2) Should there be mandatory Publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity? (3) What (if any) should the remedies be for unwarranted Publication?(4) Should a similar framework and/or considerations apply to requests made by third parties other than LEA and intellectual property rights-holders?(Section 1.3.2, Section 7.1 Category F)

Answered: 67 Skipped: 285

#	Responses	Date
1	(1) No, P/P service providers should be able to notify their customers. (2) No, P/P service providers should be able to protect the privacy of their customers. (4) P/P service providers should be able to notify their customers and protect them from other third parties as well.	7/8/2015 2:33 AM
2	(1) Which LEA in which venue? Impossible to regulate. (2) yes (3) none (4) abusers should not be protected in any way.	7/7/2015 7:31 PM
3	(1) YES, with a caveat. Providers should be required to comply with LEA requests not to notify a customer only in cases in which the LEA request for information has already been deemed valid. (2) YES. Publication of domain abusers' WHOIS information is critical for proactive anti-abuse. Without it, a registrant can engage in blatant domain name abuse (such as phishing, malware hosting, command and control of botnets, and high volume SPAM) but hide behind the protection of a P/P service. Withholding publication in the face of such behavior would not only defeat the purpose of anti-abuse criteria; it would enable and further embolden cybercriminals. Furthermore, withholding publication when such violations occur would be a disservice to those seeking P/P services for legitimate reasons, victims from around the globe harmed by cybercriminals, and the integrity of the entire DNS system. P/P services are just that, services that provide WHOIS privacy and/or proxy protection for a customer pursuant to terms of use. Removing publication consequences for those who engage in domain name abuse (such as phishing, malware hosting, command and control of botnets, and high volume SPAM) will cause great harm to the DNS. A recent ICANN-sponsored study concluded that privacy and proxy services are one method used by cybercriminals in their perpetration of domain name abuse (http://gnso.icann.org/en/issues/whois/pp-abuse-study-20sep13-en.pdf). Merely taking down a domain name but allowing for P/P protection to remain or only disclosing such information to a complaining party will enable cybercriminals to be repeat offenders. Accordingly, this will stifle proactive anti-abuse efforts by preventing a registrar or another P/P service from knowing that a domain name abuser is registering with them. WHOIS privacy is offered as a service subject to a P/P's terms of service. The obligation of a P/P provider to provide WHOIS privacy is therefore extinguished upon the breach of such terms. Accordingly, a registrant engaged in phishing, malware hosting, botnet command and control, malware, or high volume spam on a domain name protected by P/P should lose their WHOIS privacy protection. It should be noted that the termination of P/P service is wholly distinct from the due process rights afforded to one accused of a crime by a sovereign government. (3) It depends upon whether or not such publication was due to negligence, harmless error, or malicious motivation. At their core, P/P services are provided by contract. Accordingly, contract law remedies should be available for a registrant if a P/P provider does in fact breach the contract and cause harm. Incentives for P/P operators to exercise caution when publishing WHOIS information should be implemented through the ICANN accreditation and compliance process. If and when unwarranted publication occurs then complaints should be lodged with ICANN. ICANN itself can threaten to withdraw accreditation if a P/P provider conducts unwarranted publication due to negligence or malicious intent and there is demonstrable harm on behalf of the aggrieved party. Proper auditing and publication of errors made by P/P providers will enhance the ability of registrants to choose a P/P provider with a strong reputation for fulfilling their P/P contract services. A P/P system without remedies for unwarranted publication could enable P/P providers to cave to pressure and publish WHOIS information for reasons unrelated to domain name abuse and/or a breach of terms of service. This would harm accountability efforts and call into question the purpose of an accreditation regime. (4) Yes, interested and aggrieved third parties do not always fall into the category of LEA or intellectual property rights holders. Domain name abuse affects the entire Internet ecosystem. As a result, many NGOs and public benefit entities seek to stop cybercriminals and should be able to seek publication of WHOIS information for registrants that breach the terms of P/P services.	7/7/2015 5:58 PM
4	Yes to 1, 2 & 4 Unwarranted Publication ignoring take down notice should lose their right to operate the site.	7/7/2015 9:32 AM
5	(1) Hard to choose between (a) risking a criminal being notified and thus evading an investigation, and (b) potential abuse by law enforcement agency. In the current political climate, and considering that ICANN oversees the world, not just a few nations, I would tend towards non-mandatory. (2) Yes, provided an unambiguous description of all such activities/violations were made prominently available to the customer.	7/6/2015 7:32 PM

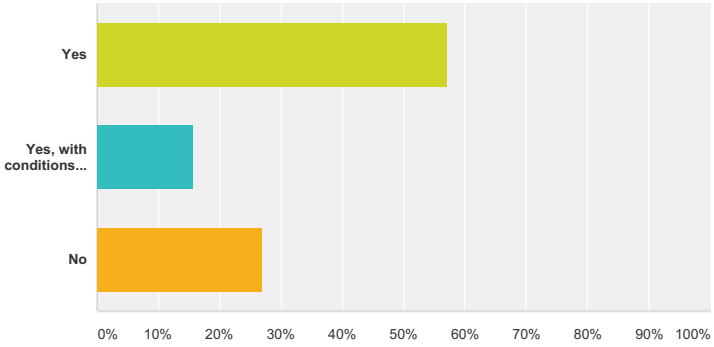
6	We believe providers should be subject to laws in their jurisdictions and that no ICANN policy should attempt to create new rights or responsibilities not enshrined in law. We believe no framework or consideration is necessary for LEA, intellectual property rights holders or other third parties.	7/6/2015 12:57 PM
7	We believe providers should be subject to laws in their jurisdictions and that no ICANN policy should attempt to create new rights or responsibilities not enshrined in law. We believe no framework or consideration is necessary for LEA, intellectual property rights holders or other third parties.	7/6/2015 12:57 PM
8	Disclosure should be made only upon a court order.	7/6/2015 12:20 PM
9	1) yes 2) publication is always problematic, my position would be no. 3)unhappily I do not have one yet. 4) I prefer a no.	7/6/2015 11:56 AM
10	1-4 are unacceptable in any form. IP rights and law enforcement concerns are no justification for any changes to the whois system and rules that would affect privacy and freedom of domain holders.	7/6/2015 3:29 AM
11	It should not be mandatory for accredited P/P service providers to comply with express requests from LEA in the provider's jurisdiction not to notify a customer.	7/6/2015 1:02 AM
12	The registrant should be able to ask the court of his or her residence to block disclosure or publication of his or her identifying information. The registrant of the domain should be able to request identifying information about the requester.	7/6/2015 12:27 AM
13	1. If required by law, LEA requests MUST be obeyed. If just a casual request, no. 2. No 3. Substantial compensation, regardless of actual damage caused. 4. No. It should only apply to LEA. If an IP rights holder wants to make a claim, it should be done through a LEA. Otherwise, any person can make a claim and gain access to information that had been made private.	7/5/2015 8:37 PM
14	(1) Providers should act according to their jurisdiction's law, which may forbid them to notify the customer. (2) No. If the activity is really illegal, then the customer has probably provided fake contact details, or the details of an innocent person. (3) Only publish details when requested by a LEA. Once published there is no remedy. (4) Only LEA should be able to request publication or disclosure.	7/5/2015 6:32 PM
15	(1) yes (2) yes (4) Seems like a good idea	7/5/2015 12:41 PM
16	Concerning "remedies", host country laws should be senior and, in multi-national concerns, it's probably appropriate that the State Department (or host-country equivalent) by notified/involved.	7/5/2015 3:07 AM
17	1. It is never defensible not to notify a customer. This power has been asserted only under the PATRIOT Act, intended to fight terrorism, not IP misuse, and even there such withholding has come under intense pressure. 2. Mandatory publication is never justified. If a Chinese hacker whacks my WordPress site and puts a virus on it, do you intend to give me a scarlet letter? 3. Unfortunately, in unwarranted Publication, the damage is done. This should have two aspects: (a) because personal information has been compromised, the victim must be entitled to a one-year fraud and identity protection service, paid for by ICANN or the P/P, depending on whose policies caused the exposure; and (b) because it is a single disclosure, not a class, standard legal recourse should be available. Such recourse could be costly if overbroad policies are found to merit punitive damages.	7/5/2015 2:36 AM
18	1. If the P/P service provider receives a National Security Letter or other binding request with a silencing order, then non-notified requests make sense since otherwise they would be in violation of the law. For standard law enforcement requests, by contrast, actively notifying the customer should be mandatory regardless of whether any information was disclosed. 2. No mandatory publication should be required since malware/viruses change so often; false positives pose a threat; and people like security researchers might face issues if their actions are construed to violate a too-ambiguous law.	7/4/2015 1:38 AM
19	(1) Accredited P/P service providers *MUST*, in all cases - even against express requests from LEA - notify the customer. We the people are sick enough of that kind of secrecy / lack of transparency, and we're growing ever more intolerant of it. (2) No. No Publication should ever occur without the express consent of the customer. If you or anyone has a problem with illegal or potentially illegal activity, refer the issue to an actual legal authority. Nevermind these shenanigans of playing "Internet-police" for domains (names, content, etc.). (3) There is no remedy for unwarranted Publication. There is no "undo" for breach of privacy. Except for ceasing all Publication, entirely. For everyone. Forever. Christ, this isn't even that difficult a concept. (4) Look : Fuck these corporate interests. What a tremendous waste of time and energy to be contriving these systems of agreements and mandates. Work instead towards lessening the amount of personal information collected and the world'll be better off for it.	7/2/2015 7:45 PM
20	Kill it. This is so inappropriate.	7/2/2015 9:48 AM
21	Dear God... You want to continue expanding the rights of Law Enforcement over the rights of individuals? Seriously? P/P Providers, when held to certain regulations, are perfectly able to handle all requests for disclosure/publication, and to set their own standards. What you're proposing is an expansion of the ability of any individual who has an issue with an individual domain registrant, for whatever reason, to obtain the personal information needed to do that person real harm.	7/2/2015 9:05 AM
22	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
23	The WG's illustrative Disclosure Framework should not try to anticipate other types of requests. The WG's was formed to recommend a balanced between the requester with a valid DCMA complaint and the user of a P/P service expectation of privacy. 1) No 2) No 3) A refund of the P/P service fee. 4) Not at this time, because other requests imply other complaints beyond the scope of LEA and DCMA issues.	7/1/2015 8:27 PM
24	I believe there are legal avenues available for genuine infractions of trademark and copyright, and the proposed changes overstep and do not add to those avenues. Given that, I do not recommend effort be expended for similar frameworks.	7/1/2015 6:58 PM
25	(1) only if mandated by law. (2) only if mandated by law. (3) punishment of the requester by law. (4) no separate framework should be supported for IP rights-holders. No separate framework than that existent for LEA is necessary or warranted.	7/1/2015 8:55 AM
26	The current laws provide the necessary due process that protects individuals and businesses. Removing these protections, as will be done under these guidelines, would presume individuals and small businesses guilty without even giving them a chance to respond. Hence this disclosure framework is unsatisfactory.	6/30/2015 9:33 PM
27	In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:49 AM

28	1. ICANN must not mandate this! If LEA in provider jurisdiction have actual authority to do this, the provider is already subject to local laws. If LEA have no such authority, ICANN is aiding in what could potentially be an illegal act. 2. No. Publication cannot be undone, and much illegal activity could be the result of third-party attacks on a site. If a malicious third party can trigger Publication by attacking a site, then their attacks are only magnified in strength. 3. This may in general be left to contract between the registrant and provider. ICANN's only clear option here is to remove accreditation for repeated violations. 4. No. Publication cannot be undone, and the rationale in point 2 also applies here. Legitimate third-party requests always have the option of filing a complaint with local LEA, should the conduct actually be actionable.	6/29/2015 5:41 PM
29	(1) No, as already mentioned this should almost never happen, especially not if it is only requested. As recent news have shown such powers will be abused by law enforcement. (2) No. (4) No. Neither LEAs or rights-holders or anyone else should get this power, and especially not if they are not by-law allowed to enforce the privacy of their requests. Privacy is a fundamental right, no entity of any sort should be granted loopholes to get around protections that are already granted by law.	6/29/2015 1:24 PM
30	American citizens have the right to face their accusers. It is a violation of basic civil liberties to withhold an accusation made by another.	6/29/2015 7:44 AM
31	1. No. If not legally required, the P/P service should not compelled to comply with law enforcement requests. 2. No. 3. None. 4. Absolutely not.	6/29/2015 12:19 AM
32	Any requirement of mandatory, involuntary publication would threaten privacy for all domain owners, at a time when people are already under threat against their lives for something as trivial as posting opinions about video games. To make it this much easier to harrass and threaten people online would be unconscionable. Privacy, once lost, cannot be recovered, and the special needs of media companies do not deserve to be privileged over the rights of individuals. It is appalling that these measures are even being considered.	6/28/2015 9:02 PM
33	I disagree across the board. Existing legal systems handle these issues just fine.	6/28/2015 6:03 PM
34	(1) No, unless the request is legally binding. Existing subpoenas already provide a way to suppress their disclosure; a second method is unnecessary. (2) Yes, but there should be a dispute period where the Registrant can oppose Publication, and P/P providers should not be required to monitor their customer's websites. (3) There is no possible remedy. You cannot "unpublish" the information. Therefore, unwarranted Publication needs to not happen in the first place. We can move towards this by requiring that all Publications be able to be opposed, and requiring that Registrants be allowed to present their case in front of a neutral mediator. Further, when a P/P Publishes, it should reference a specific clause within their terms of service, and those terms should not have a catch-all like 'the provider may Publish the Registrants information if it deems it necessary.' The requirements should be consistently and neutrally enforced, and not on the basis of the speech contained within a site. Alternately, all of the purposes fulfilled by Publication are already fulfilled by Disclosure, so this really has very little point. (4) All requests should have the possibility of appeal by the Registrant. Sooner or later, you're going to have someone who will lie to a P/P provider to unmask the owner of the domain.	6/28/2015 5:17 PM
35	Fuc{ off	6/28/2015 4:48 PM
36	(1) No. LEA without a court order has only the power to ask.	6/28/2015 2:19 PM
37	1. No, service providers must alert customers under all circumtances. 2. No, there should be no vague excuses available to destroy privacy. 3. If any users privacy is violated, the organization who attempted it and ICANN should be held jointly liable for consequences and also subject to large mandatory fines. 4. No. There should be no framework for violating users' privacy.	6/28/2015 1:57 PM
38	I think all of the ideas are terrible given access via court order is already in existence and there is no need to make it easier.	6/28/2015 1:21 PM
39	(1) No. it is important that citizens are free to express opinions contrary to the government online without fear of secret repercussion. (2) No. Otherwise, file sharing (e.g. "GitHub"-like sites) and similar sites would be unable to operate. Furthermore, illegal activity in *what jurisdiction* and determined by whome? (3) Some process should be established at the end of which should be revocation of certification status. (4) Yes.	6/28/2015 12:40 PM
40	1. No 2. No 4. Absolutely not	6/28/2015 12:00 PM
41	All requests for customers data, and requests to not notify the customer, should be decided by the judicial process. To comply with such requests without judicial oversight will permit an abuse of the customer's privacy. Such framework should not be apply to any requests, including those by IP rights holders and LEA.	6/28/2015 11:56 AM
42	no, leave it as is it is fine	6/28/2015 9:24 AM
43	No comment	6/28/2015 7:56 AM
44	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:53 AM
45	(1) - no (2) - no (3) - standard legal process: warrant by justice system, police investigation (3) - no	6/28/2015 6:19 AM
46	Seriously.. How much did you guys get paid ? RIAA and MPAA must have some really deep pockets and well endowed sausages.	6/28/2015 5:15 AM
47	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:17 AM
48	"Should it be mandatory for accredited P/P service providers to comply with express requests from LEA in the provider's jurisdiction not to notify a customer? " => No. Only if the law requires it. Why should providers be required to do more than the law requires? If Law Enforcement doesn't like this, they should talk to the relevant legislatures, not ICANN. 2) There should not be any publication except where legally required.	6/28/2015 3:50 AM
49	There should not be a disclosure framework. Personal information should not be required to obtain a domain. Disclosure of personal information should mean that whoever registered the domain has all litigation costs covered by ICANN and that ICANN should bear all costs derived from the disclosure of personal information.	6/28/2015 3:33 AM
50	P/Ps should not be regulated. Current legal remedies are sufficient for policing illegal activity.	6/28/2015 3:25 AM
51	Do not agree with lea as defined	6/27/2015 7:37 PM
52	It turns out my own domain name is some copyrighted name from years ago. I registered my domain it in good faith and am in a different industry altogether. But domains were meant to be company names not product trademarks. Let trademark holders have ".trademark"	6/27/2015 1:25 PM
53	not sure	6/27/2015 12:23 PM
54	1. No. 2. No. 3. Suck it up and enjoy the free publicity. 4. No.	6/26/2015 11:50 PM

55	As stated above, IP rights-holders should have no interaction with the domain system, including P/P. The only way that this interaction must happen is through the justice system, not directly. Also, P/P should not be forced to comply with requests from LEA not to notify a customer irrespective of the jurisdiction; there should be NO special treatment regarding publication for certain types of activity (they must be treated like any other type of sites). In general, no third party should have any power over the domain system, unless decided by a court of law.	6/26/2015 1:10 PM
56	Customer should always be notified, no mandatory publications whatsoever, no unwarranted anything, and again anything compromises privacy needs to be vehemently avoided.	6/26/2015 12:20 PM
57	No disclosure or publication.	6/26/2015 4:09 AM
58	23 (1) notification to the customer of p/p services should always occur. This is called transparency and we need more of this in the world not less. 23 (2) no 23 (3) for the p/p there should be some sort of punishment. Not sure how to implement it though 23(4) there should be strict requirements over any request process. What if the P/P customer is requiring to protect themselves for political reasons.	6/25/2015 6:50 PM
59	Use the courts. There should never be an automatic release of private data. The requestor must gain a courts order and the registrant must be notified ahead of time so they can appeal and/or appear in court.	6/25/2015 3:57 PM
60	There is no remedy for unwarranted publication. Once the information is out it is no longer controllable. Therefore, the only circumstances where information should be released is under a court order. Notifying or not notifying a customer should also be based on local laws - not broad policies.	6/25/2015 3:34 PM
61	Again this is tricky, a user has their site hacked and malware is put there, a spammer then sends an email that infects a user. The domain owner has no idea. What should happen is that the registrar should change the name servers to protect the public from the malware, the hosting company should be informed and the owner should be told that their site has had name servers changed due to malware. The domain owner should then use FTP to remove malware and restore the name servers. If there are 2 additional reports of malware after that incident the domain owner would not be able to restore name servers without an appeal process with a risk that the domain is confiscated and released to market.	6/25/2015 2:58 PM
62	1. It should not be mandatory to comply with such requests. Any obligation not to notify a customer should come solely from the the laws of the provider's jurisdiction, not from ICANN requirements. 2. No. There should be no mandatory publication for any offenses. Disclosure can be made to appropriate law enforcement agencies or plaintiffs through the ordinary disclosure channels. 4. No. Third parties can use existing legal process to obtain disclosure.	6/24/2015 8:10 PM
63	Yes, it should be mandatory for accredited P/P service providers to comply with requests by law enforcement that the customer not be notified.Yes, publication should be mandatory for any violation of terms of service relating to any illegal activity. No specific remedies for unwarranted publication are necessary. Unwarranted publication would be a matter between the customer and the privacy/proxy service provider. Yes, the same framework and considerations should apply to all reports of abuse.	6/24/2015 1:34 PM
64	1) That kind of depends on the rights that the customer is provided in their geographical location by their countries laws.	6/23/2015 11:53 AM
65	(1) Should it be mandatory for accredited P/P service providers to comply with express requests from LEA in the provider's jurisdiction not to notify a customer? The accredited P/P providers should only keep an LEA request confidential in matters of national security or with a court order. P/P providers must work for their customers and demand the highest legal proof for keeping an LEA request confidential. The default should be to notify the customer of any requests. (2) Should there be mandatory Publication for certain types of activity e.g. malware/viruses or violation of terms of service relating to illegal activity? In cases of malware and viruses this is the responsibility of the web host, and since a P/P is not a host terms of service issues would also fall to the host or the registrar. Publication in these cases is not warranted. (3) What (if any) should the remedies be for unwarranted Publication? A complaint procedure should be established via the ICANN accrediting process. The fee for pursuing a complaint should be either nothing or a very low amount. If an ICANN investigation finds that publication was unwarranted the p/p should face a fine. If the p/p has more than 25 unwarranted publications in the span of 10 years they should lose their accreditation. (4) Should a similar framework and/or considerations apply to requests made by third parties other than LEA and intellectual property rights-holders? No	6/22/2015 12:50 PM
66	.	6/21/2015 7:28 PM
67	1: They should notify the customer 2: No 3: None the provider will lose business 4: I disagree with any disclosure to copyright holders	6/20/2015 2:20 PM

Q24 Do you agree that privacy/proxy service customers should be notified prior to de-accreditation of a P/P service provider, to enable them to make alternative arrangements? If so, should this be when Compliance sends breach notices to the provider, as customers would then be put on notice (as is done for registrar de-accreditation)?(Section 1.3.1 Recommendation 20, Section 7.1 Category G)

Answered: 89 Skipped: 263



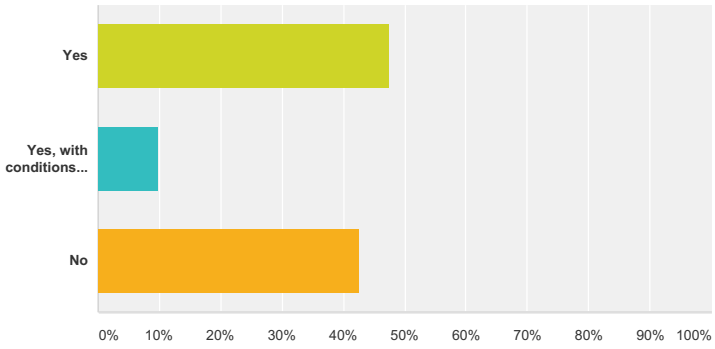
Answer Choices	Responses	
Yes	**57.30%**	51
Yes, with conditions (please specify what those conditions are in the box below)	**15.73%**	14
No	**26.97%**	24
Total		**89**

#	Additional Comments	Date
1	Yes provided the reasonable timeline for cure of the breach has been accommodated and is passed.	7/6/2015 1:04 PM
2	This is ominous. Of course I would want to know of a P/P provider had its accreditation revoked, but it is unclear to me the circumstances under which ICANN would take such a brazen step.	7/5/2015 2:44 AM
3	Yes, this should be when the breach notices are submitted. I continue to disagree with the idea of accrediting P/P services.	7/4/2015 1:41 AM
4	Kill the accreditation process. Kill it with fire.	7/2/2015 9:51 AM
5	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
6	notification should come from the P/P provider itself as soon as possible.	7/1/2015 7:09 PM
7	Accreditation or de-accreditation should not negatively impact the service or the privacy of the customer information, and at no point should it be disclosed or subject to threat of disclosure by any third-party organization.	6/30/2015 11:26 PM
8	We do not need accreditation for these providers in the first place. Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:50 AM
9	Individual registrants must be able to reasonably maintain their privacy regardless of the actions of the provider. If de-accreditation poses any risk of Publication or Disclosure, the registrant must be provided adequate recourse for maintaining privacy, since Publication and Disclosure cannot be undone.	6/29/2015 5:51 PM
10	Yes, but accrediation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue.	6/29/2015 1:25 PM
11	No accreditation should be required.	6/29/2015 12:21 AM
12	Should not be applicable; if the recommendations of the working group were unwisely adopted, then yes.	6/28/2015 9:05 PM
13	No. That's a risk of hiding behind p/p.	6/28/2015 8:38 PM
14	I do not want to see an accreditation process come into existence.	6/28/2015 6:05 PM
15	Customers should only be notified if there is a deaccreditation. Sending an email on notice of breach is a forceful move that's intended to put pressure on the P/P provider. The P/P provider is looking out for the interests of the customers in this case, not ICANN.	6/28/2015 2:25 PM

16	There should be no accreditation of privacy service providers.	6/28/2015 1:58 PM
17	is not your business.	6/28/2015 10:54 AM
18	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:55 AM
19	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:20 AM
20	I don't agree with the whole framework but the taking of property (de-accreditation) requires a high burden and sufficient transparency for the customers.	6/28/2015 3:29 AM
21	This requires accreditation, which is a steaming pile of cow excrement in itself.	6/26/2015 11:52 PM
22	Notification is extremely important.	6/26/2015 12:21 PM
23	Clearly, consumers must be given the option to find another p/p provider.	6/25/2015 3:59 PM
24	A domain name owner should be notified at the time ICANN has determined to de-accredit a p/p. In addition, ICANN should provide up to three p/p providers for the customer to choose from and require that the p/p losing accreditation must post this information on its home page as well as on the ICANN website.	6/22/2015 12:58 PM
25	I do not think that P/P service providers need accreditation.	6/20/2015 2:22 PM

Q25 Do you agree that other P/P service providers should also be notified, to enable interested providers to indicate if they wish to become the gaining P/P provider (as is done for registrar de-accreditation)? If so, should all notification(s) be published on the ICANN website (as is done for registrar de-accreditation)?(Section 1.3.1 Recommendation 20, Section 7.1 Category G)

Answered: 82 Skipped: 270



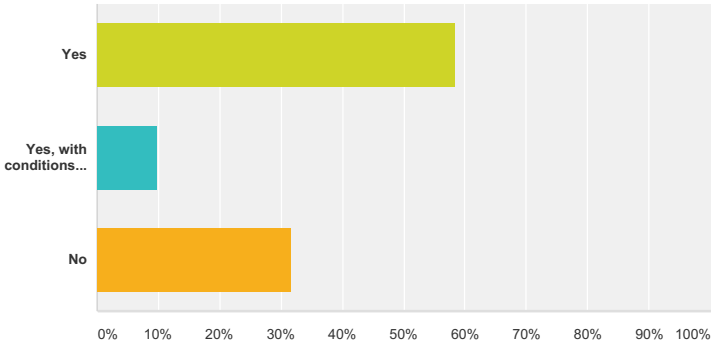
Answer Choices	Responses	
Yes	**47.56%**	39
Yes, with conditions (please specify what those conditions are in the box below)	**9.76%**	8
No	**42.68%**	35
Total		**82**

#	Additional Comments	Date
1	I think this is reasonable but it remains unclear how this could happen.	7/5/2015 2:44 AM
2	Yes, agreed, and these notifications should be published. I continue to disagree with the idea of accrediting P/P services.	7/4/2015 1:41 AM
3	Kill the accreditation process. Kill it with fire.	7/2/2015 9:51 AM
4	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
5	that would entail releasing customers' information.	7/1/2015 7:09 PM
6	I believe this would provide a "chilling effect" to the industry and to this particular vertical market.	7/1/2015 7:02 PM
7	ICANN should be less involved, so the second clause should be amended.	6/30/2015 9:35 PM
8	We do not need accreditation for these providers in the first place. Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:50 AM
9	Impending de-accreditation should not impinge on the registrant's privacy, including by providing third parties with mailing lists. Third-party solicitation should probably not be encouraged.	6/29/2015 5:51 PM
10	Yes, but accrediation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue.	6/29/2015 1:25 PM
11	No accreditation should be required.	6/29/2015 12:21 AM
12	I do not want to see an accreditation process come into existence.	6/28/2015 6:05 PM
13	This makes it too easy for a problematic accredited P/P provider to insert itself everywhere. The customer should be notified and have to research it.	6/28/2015 2:25 PM
14	There should be no accreditation of privacy service providers.	6/28/2015 1:58 PM
15	This question implies I agree with accreditation of P/P. I can't answer this because this is not and should not be in your domain.	6/28/2015 10:54 AM
16	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:55 AM
17	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:20 AM
18	Perhaps the initial registrant could at registration list a preferred provider so as not to receive 35 spam emails in the event of de-accreditation.	6/21/2015 7:31 PM

19	I do not think that P/P service providers need accreditation.	6/20/2015 2:22 PM

Q26 Do you agree that a de-accredited P/P service provider should have the opportunity to find a gaining provider to work with (as sometimes occurs with registrar de-accreditation)? (Section 1.3.1 Recommendation 20, Section 7.1 Category G)

Answered: 82 Skipped: 270



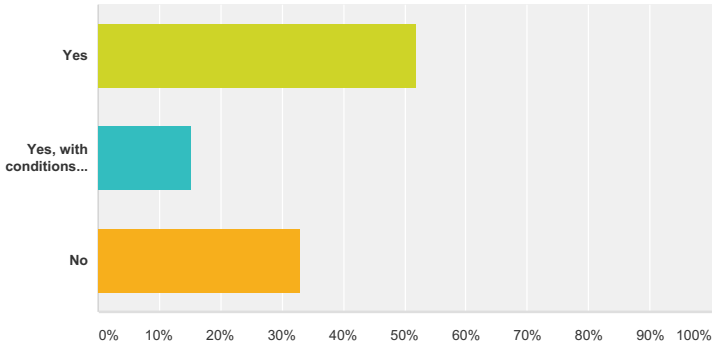
Answer Choices	Responses	
Yes	**58.54%**	48
Yes, with conditions (please specify what those conditions are in the box below)	**9.76%**	8
No	**31.71%**	26
Total		**82**

#	Additional Comments	Date
1	Much depends on the circumstances leading up to de-accreditation. It may be more appropriate that the de-accredited service provider be given a list of options rather than allowing it to "find" another service provider with motivations similar to its own.	7/5/2015 3:11 AM
2	I think this is reasonable but it remains unclear how this could happen.	7/5/2015 2:44 AM
3	Yes, agreed. I continue to disagree with the idea of accrediting P/P services.	7/4/2015 1:41 AM
4	Kill the accreditation process. Kill it with fire.	7/2/2015 9:51 AM
5	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
6	If this were enforced, there needs to be some oversight to ensure there is not a usury scenario occuring that is artificially / maliciously forcing accredeted P/P service providers out of business to the benefit of a gaining provider.	7/1/2015 7:02 PM
7	Accreditation or de-accreditation should not negatively impact the service or the privacy of the customer information, and at no point should it be disclosed or subject to threat of disclosure by any third-party organization that the customer does not wish to disclose that information to.	6/30/2015 11:26 PM
8	We do not need accreditation for these providers in the first place. Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:50 AM
9	Yes, but accrediation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue.	6/29/2015 1:25 PM
10	No accreditation should be required.	6/29/2015 12:21 AM
11	Should not be applicable; if the recommendations of the working group were unwisely adopted, then yes.	6/28/2015 9:05 PM
12	I do not want to see an accreditation process come into existence.	6/28/2015 6:05 PM
13	There should be no accreditation of privacy service providers.	6/28/2015 1:58 PM
14	This question implies I agree with accreditation of P/P. I can't answer this because this is not and should not be in your domain.	6/28/2015 10:54 AM
15	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:55 AM
16	Due process per the law of the domain owner's country should be required before revealing information about even the proxy provider!	6/28/2015 4:20 AM
17	ICANN should make the determination of the gaining provider to eliminate the possibility that a de-accredited privacy/proxy provider would select an affiliated entity.	6/24/2015 1:35 PM
18	zero tolerance.	6/21/2015 7:31 PM

19	I do not think that P/P service providers need accreditation.	6/20/2015 2:22 PM

Q27 Do you agree that a "graduated response" approach to de-accreditation should be explored, i.e. a set series of breach notices (e.g. up to three) with escalating sanctions, with the final recourse being de-accreditation?(Section 1.3.1 Recommendation 20, Section 7.1 Category G)

Answered: 79 Skipped: 273

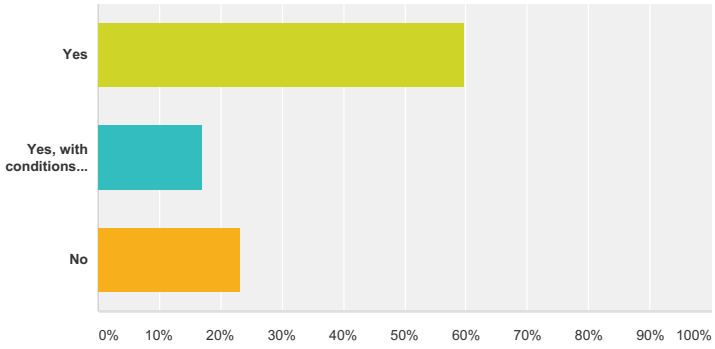


Answer Choices	Responses	
Yes	**51.90%**	41
Yes, with conditions (please specify what those conditions are in the box below)	**15.19%**	12
No	**32.91%**	26
Total		**79**

#	Additional Comments	Date
1	The WG should explore allowing more than three series of breach notices.	7/8/2015 2:39 AM
2	As long as the process does not linger.	7/7/2015 7:33 PM
3	I think this is reasonable but it remains unclear how this could happen.	7/5/2015 2:44 AM
4	No new territory or conditions for de-accreditation should be defined here. I continue to disagree with the idea of accrediting P/P services.	7/4/2015 1:41 AM
5	Kill the accreditation process. Kill it with fire.	7/2/2015 9:51 AM
6	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
7	That local authority law is not infringed upon by this de-accreditation process.	7/1/2015 8:58 AM
8	We do not need accreditation for these providers in the first place. Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:50 AM
9	Yes, but accrediation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue.	6/29/2015 1:25 PM
10	No accreditation should be required.	6/29/2015 12:21 AM
11	Should not be applicable; if the recommendations of the working group were unwisely adopted, then yes.	6/28/2015 9:05 PM
12	I do not want to see an accreditation process come into existence.	6/28/2015 6:05 PM
13	There should be no accreditation of privacy service providers.	6/28/2015 1:58 PM
14	This question implies I agree with accreditation of P/P. I can't answer this because this is not and should not be in your domain.	6/28/2015 10:54 AM
15	Due process per the law of the domain owner's country should be required before seeking to identify the proxy provider.	6/28/2015 4:20 AM
16	I don't agree with the framework in the first place	6/28/2015 3:29 AM
17	Why up to three? What does baseball have to do with the internet and privacy? 3 strikes and you are ? unaccredited amazing.	6/28/2015 3:21 AM
18	As long as it is a large adequate series of breach notices.	6/26/2015 12:21 PM
19	MAXIMUM three.	6/21/2015 7:31 PM
20	I do not think that P/P service providers need accreditation.	6/20/2015 2:22 PM

Q28 Do you agree that, where feasible, a customer should be able to choose its new P/P service provider in the event of de-accreditation of its existing provider? (Section 1.3.1 Recommendation 20, Section 7.1 Category G)

Answered: 82 Skipped: 270

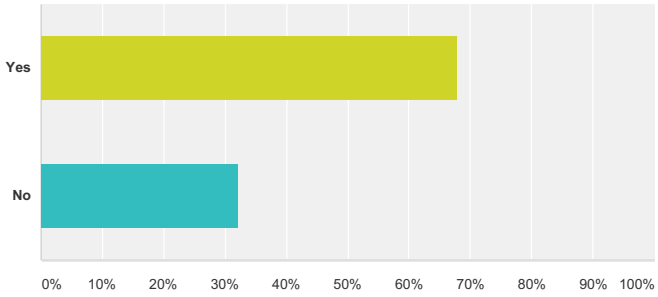


Answer Choices	Responses	
Yes	**59.76%**	49
Yes, with conditions (please specify what those conditions are in the box below)	**17.07%**	14
No	**23.17%**	19
Total		**82**

#	Additional Comments	Date
1	I think this is reasonable but it remains unclear how this could happen.	7/5/2015 2:44 AM
2	I continue to disagree with the idea of accrediting P/P services.	7/4/2015 1:41 AM
3	Kill the accreditation process. Kill it with fire.	7/2/2015 9:51 AM
4	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
5	Though the customer's identity should be protected in the event of switching P/P service provider (per the language elsewhere in the recommendations).	7/1/2015 7:02 PM
6	Within the arrangments made by parties.	7/1/2015 8:58 AM
7	seamless anonymity is absolutely crucial. Anonymity must never be lifted without giving a chance to move over to another anonymitty provider	7/1/2015 5:00 AM
8	We do not need accreditation for these providers in the first place. Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:50 AM
9	Yes, but accrediation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue.	6/29/2015 1:25 PM
10	No accreditation should be required.	6/29/2015 12:21 AM
11	Should not be applicable; if the recommendations of the working group were unwisely adopted, then yes.	6/28/2015 9:05 PM
12	I do not want to see an accreditation process come into existence.	6/28/2015 6:05 PM
13	The customer should also be able to choose a non-accredited provider.	6/28/2015 2:25 PM
14	There should be no accreditation of privacy service providers.	6/28/2015 1:58 PM
15	This question implies I agree with accreditation of P/P. I can't answer this because this is not and should not be in your domain.	6/28/2015 10:54 AM
16	Customers should be given sufficient time to change their privacy provider to ensure that at at no time is private information leaked	6/28/2015 7:58 AM
17	This should be able to be setup prior to even the event of starting use with the first P/P. Thereby allowing the customer to have their information with a P/P service they trust. Not just the next one on the list. And not after their information was turned over automatically to the next P/P service behind the one being unaccredited.	6/28/2015 3:21 AM
18	Not where feasible, but ALWAYS.	6/26/2015 1:11 PM
19	They should be notified.	6/26/2015 12:21 PM
20	YES with no further cost to the user, in the same way that if you transfer a domain with 3 years to run those three years are honored.	6/25/2015 2:58 PM
21	I do not think that P/P service providers need accreditation.	6/20/2015 2:22 PM

Q29 Do you agree that the next review of the IRTP should include an analysis of the impact on P/P service customers, to ensure that adequate safeguards are in place as regards P/P service protection when domain names are transferred pursuant to an IRTP process?(Section 1.3.1 Recommendation 20, Section 7.1 Category G)

Answered: 81 Skipped: 271



Answer Choices	Responses	
Yes	**67.90%**	55
No	**32.10%**	26
Total		**81**

#	Additional Comments	Date
1	No P/P protection should exist at all.	7/7/2015 7:33 PM
2	No. The IRTP is neither defined nor linked here, so it is impossible to agree with this statement.	7/5/2015 2:44 AM
3	I continue to disagree with the idea of accrediting P/P services.	7/4/2015 1:41 AM
4	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
5	Though I question where the cost of the analysis of the impact where will be borne, and whether this will unduly burden P/P service providers (which will be passed on to Clients).	7/1/2015 7:02 PM
6	I believe that the current language of these recommendations is more or less opening a can of worms. Please consider the impact on the customers of these proxy/privacy customers, or at least make these recommendations or guidelines that do not negatively impact their privacy and their ability to express their speech freely on the web.	6/30/2015 11:26 PM
7	We do not need accreditation for these providers in the first place. Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:50 AM
8	The needs of end users do not appear to be a goal of the current recommendations. I would be very interested to review one where they were.	6/28/2015 9:05 PM
9	There should be no accreditation of privacy service providers or mechanism for violating the privacy of users.	6/28/2015 1:58 PM
10	This question implies I agree with accreditation of P/P. I can't answer this because this is not and should not be in your domain.	6/28/2015 10:54 AM
11	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:55 AM
12	Due process per the law of the domain owner's country should be required before revealing information. The WHOIS database is unnecessary in the first place. It should be taken down.	6/28/2015 4:20 AM
13	I do not think that P/P service providers need accreditation.	6/20/2015 2:22 PM

Q30 Please provide any suggestions you may have on a possible compliance framework that may facilitate the effectiveness of the de-accreditation process. (Section 1.3.1 Recommendation 20, Section 7.1 Category G)

Answered: 25 Skipped: 327

#	Responses	Date
1	You lie, you die.	7/7/2015 7:33 PM
2	None	7/7/2015 9:34 AM
3	There should be no de-accreditation process whatsoever.	7/6/2015 3:30 AM
4	De-accreditation of a P/P provider should have a public comment period as it will have far more stakeholders than just ICANN, the provider, the requesters, and the registrants of the requested domains.	7/6/2015 12:30 AM
5	De-accreditation needs to be a consequence of misbehavior, not an arbitrary threat. Currently it appears to be the latter. Whatever framework is defined, it must be as narrow and specific as possible, avoiding the "things we think of later" kind of language seen before,	7/5/2015 2:44 AM
6	Respectfully, I continue to disagree with the idea of accrediting P/P services.	7/4/2015 1:41 AM
7	Abolish accreditation. Else force it upon us and we'll hasten our technological workarounds and moving away from this bullshit, anyway.	7/2/2015 7:50 PM
8	Kill the accreditation process. Kill it with fire.	7/2/2015 9:51 AM
9	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
10	To not use a separate framework for this, or go beyond regular de-accreditation.	7/1/2015 8:58 AM
11	Yes, but accrediation in general is unnecessary at best and harmful at worst. Privacy and proxy providers (and their customers) have spoken at length on the issue.	6/29/2015 1:25 PM
12	No accreditation should be required.	6/29/2015 12:21 AM
13	I do not want to see an accreditation process come into existence.	6/28/2015 6:05 PM
14	There should be no accreditation of privacy service providers.	6/28/2015 1:58 PM
15	Whenever a private company handles an accreditation, that's a bad thing	6/28/2015 7:55 AM
16	Do not force accreditation on providers, in the first place.	6/28/2015 5:17 AM
17	YOU ARE ONLY TROUBLING GOOD-FAITH USERS. THOSE WITH ILL INTENT WILL EASILY CIRCUMVENT THESE RULES!	6/28/2015 4:20 AM
18	If accreditation is required, de-accreditation should only occur because of a failure to keep P/P information private, IE the P/P service disclosing information should be the only reason for de-accreditation, and P/P services should generally be prohibited from disclosing personal information or storing it long term.	6/28/2015 3:36 AM
19	Scrap this whole proposal	6/28/2015 3:29 AM
20	Don't make P/P services jump through these loops. This is an international issue. It should not be something that a USA company can inflict upon a Europe company. This entire Recommendation is just scary for the future of the internet.	6/28/2015 3:21 AM
21	not sure	6/27/2015 12:23 PM
22	Kinda needs accreditation to exist.	6/26/2015 11:52 PM
23	Utilization of iCANN's current compliance program framework is a start; however, greater attention to enforcement, more transparency in the decision-making process and final determinations made by ICANN is needed.	6/24/2015 1:35 PM
24	Could you launch an "initial" compliance framework on "some" sites/providers as a trial?	6/21/2015 7:31 PM
25	I do not think that P/P service providers need accreditation.	6/20/2015 2:22 PM

Q31 Before answering this question, please review the WG's deliberations on the issue of whether registrants of domain names associated with online financial transactions should be permitted to use privacy/proxy services (including the Additional Statements in the Final Report). What is your view on the following questions:(1) Should registrants of domain names associated with commercial activities and which are used for online financial transactions be prohibited from using, or continuing to use, privacy and proxy services? If so, why, and if not, why not?(2) If you agree with this position, do you think it would be useful to adopt a definition of "commercial" or "transactional" to define those domains for which P/P service registrations should be disallowed? If so, what should the definition(s) be?(3) Would it be necessary to make a distinction in the WHOIS data fields to be displayed as a result of distinguishing between domain names used for online financial transactions and domain names that are not?(Section 1.3.3, Section 7.1 Category C)

Answered: 71 Skipped: 281

#	Responses	Date
1	(1) No. Those who want to prohibit usage of privacy and proxy services have not clearly defined what a "commercial entity" is or what "commercial activity" is. The WG should analyze how such a prohibition would harm Customers. (2) I do not agree that ICANN should prohibit registrants of any domains from using, or continuing to use, privacy and proxy services. (3) No.	7/8/2015 2:48 AM
2	(1) no commercial hiding (2) no money, no transaction (3) yes, or just bn ll P/P services	7/7/2015 7:34 PM
3	Commercial/financial transactions should not force people not to use P/P... privacy is more important. I may want to use a website to advertise freelance services or a small business without wanting my private details available in whois. Potential customers/etc should do their own trust judgements on whether to risk transactions based on the identity that can be surmised from the page.	7/7/2015 12:25 PM
4	1) If the site with no transactions supports commercial activity at another site it should be treated the same. 2) Yes - exchange of money or support for a site that does so 3)No	7/7/2015 9:36 AM
5	(1) Registrants should not be prohibited from using P/P services. As to why, I agree strongly with all reservations put forward in Appendix F, section 1.3.3.2 - this is a matter that should fall far outside of ICANN's jurisdiction.	7/6/2015 7:50 PM
6	1. No they should not be prohibited from using P/P services.	7/6/2015 1:05 PM
7	(1) No. Even if it is a commercial site, it may need privacy. Yes, I know that big commercial firms do not need Whois protection. But what about small business owners? Some of them definitely need this protection. For example, if I sell my books from my own website that also hosts my bolg, do I have to disclose my home address? (3) No. There will always be a grey area.	7/6/2015 12:37 PM
8	commerce shall not be able to use P/P services. access to Whois information shall be mandatory to reduce fraud occurrences. 2) the use of the name shall be followed by a clear definition about use of e-commerce in any condition. 3)the whois will be defined for the use of whom has opted to use P/P services, so no need to also identify these registrants.	7/6/2015 12:10 PM
9	All internet users and organizations should have the right to hide their registration information under all circumstances. It is unacceptable that you are considering anything otherwise and we will seek a change in ICANN leadership due to this pandering to IP rights holders.	7/6/2015 3:32 AM
10	All persons and entities ought to be able to register privately or via proxy, irrespective of their status as a commercial entity.	7/6/2015 1:05 AM
11	The definition of commercial activities is far too vague. For example, the clause could potentially be used by oppressive regimes to identify administrators of dissident organizations if the said organizations accepted donations or sold merchandises. Setting a dollar amount limit where the registrant may conduct financial transaction below the set amount with privately registered domain would also open it to abuse since the registrant would have to provide financial details to prove he or she has not gone over the limit. Instead of restricting P/P service, commercial service providers should be encouraged to use Extended Verification SSL certificates and clearly list ways to contact them on their web sites.	7/6/2015 12:39 AM
12	1. P/P services should be available to all. 2. NA 3. No	7/5/2015 8:41 PM

13	No. Phishing victims are not even checking which domain name they are visiting, so it is highly unlikely that they will check the whois. As for consumer rights, businesses already have a legal obligation to publish some data on their web site. A mandatory whois publication would collide with national legislations on several points, as the required data can differ.	7/5/2015 6:50 PM
14	(1) Domain names associated with commercial activities should not be allowed to avail themselves of a P/P service. End users should be able, easily and immediately, to establish as much information as possible about a site with which they engage or with which they may be considering some form of engagement. This might be particularly important to parents who are trying to make a decision about the bona fides of a particular site before they allow or encourage their children to use it. (2) Yes (3) Yes	7/5/2015 12:51 PM
15	I believe the question to be too inexact to be answerable. While "respectable" businesses should be allowed to use p/p services, "shady" businesses may leverage the services for inethical purposes.	7/5/2015 3:14 AM
16	1. My best friend has an Etsy jewelry storefront for which she owns a domain name. It's a side business at most. What business does any non-customer have in knowing where her jewels are? As a result, 2) and 3) are inconsistent with my view above.	7/5/2015 2:47 AM
17	1. Disagreed. Home businesses and contractors would suffer. 2. Agreed. These terms need not be defined now, provided they are clearly described to the domain name holder upon registration. Upon registration, these terms must remain immutable until the next registration cycle. 3. No distinction.	7/4/2015 1:44 AM
18	My husband and I own a small business and work from our home. Because of this, we currently have a domain privacy service. We do make sales through our web site, so it would qualify as "commercial" or "transactional." If we were not allowed to have domain privacy, that would reveal our home address to everyone on the planet, which is obviously highly undesirable. According to the Small Business Administration's Frequenty Asked Questions (https://www.sba.gov/sites/default/files/FAQ_March_2014_0.pdf), "In 2011, there were 28.2 million small businesses", and 52 percent of small businesses are home-based. That means that 14.664 million small businesses in the US would be vulnerable to exposure of their home addresses. I therefore, STRONGLY DISAGREE that such businesses be prohibited from using, or continuing to use, privacy and proxy services.	7/2/2015 1:17 PM
19	There should be no restrictions whatsoever on the use of P/P providers.	7/2/2015 9:52 AM
20	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
21	A way of contacting the business should always be required for those sites used for financial transactions. That does not mean that personal information need be disclosed.	7/1/2015 7:11 PM
22	Domain names associated with commercial activities and which are used for online financial transactions should continue to be allowed to use or continue to use, privacy and proxy services. There are already existing avenues for protecting financial information, avenues for financial redress, and for chargebacks. The removal of privacy protection for these types of entities is not justified.	7/1/2015 7:03 PM
23	Nobody should be prohibited from using privacy. It is an universal right. What happens when a dissident journalist or a women’s shelter are forced to remove privacy because they have a donation button on their websites or when they are simply soliciting support?	7/1/2015 9:00 AM
24	Registrants should be able to and allowed to use privacy and proxy services as their business may be intimately connected with their ability to express themselves freely. Prohibiting them from using these services or otherwise making it easier for special interest parties to gain access to their private information may hamper or end small businesses which exist primarily on the Web.	6/30/2015 11:29 PM
25	The online marketplace is growing quickly. To make a rule that blanket covers all financial transactions is unwarranted as it will block innovation and prevent small businesses from growing.	6/30/2015 9:37 PM
26	Everybody should be allowed to use privacy/proxy services. It is extremely important to retain the current system and protect people's privacy instead of coming up with measures that rob people of their right to free speech and privacy. We do not need accreditation for these providers in the first place. Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:52 AM
27	No, privacy and proxy services should be open to all registrants, regardless of commercial activity. All persons, both natural and legal, engage in commercial and financial transactions! Attempting to define an artificial border between persons allowed privacy, and persons not allowed privacy, according as the degree to which their transactions are visible on the Internet, is an infeasibly broad and vague mandate, and will only get broader in future years as more transactions move toward the Internet. It would also require substantial extra recordkeeping, as part (3) suggests, for everyone involved. Note also that commercial transactions are extensively regulated by local governments, and that LEA generally hold powers to pursue cases that may arise, whether or not a privacy or proxy service is interposed; there is no more need to pre-emptively forbid privacy on the grounds of potential malicious commercial activity than there is, in the non-financial case, to pre-emptively forbid privacy on the grounds that someone could violate copyright.	6/29/2015 6:41 PM
28	(1) They should be able to get the same set of protections that anyone else does. There are many cases in which a business may actually need privacy, for example in the case of home-based businesses. The ICANN should not decide who "deserves" privacy. (2) I do not agree with this position. Privacy needs to be availlable to everyone, by default. Excluding large subsets of people from privacy will likely hurt mostly those who can't afford lawyers and other means of protections, such as smaller businesses and individuals. (3) No.	6/29/2015 1:29 PM
29	1. No. Commercial entities have a right to privacy the same individuals do. Small home based businesses are one example. Moreover, "commercial activities" is too broadly defined. Is an individual with ads on his/her personal blog considered engaging in commercial activities? 2. It should not be necessary since everyone has a right to use a P/P service. 3. No.	6/29/2015 12:24 AM
30	Privacy and proxy registrations should be eliminated in these applications.	6/28/2015 8:38 PM
31	Corporations should be prohibited from using privacy/proxy services.	6/28/2015 6:06 PM
32	(1) I cannot see a compelling reason for this prohibition, and it seems extremely broad. Is a gaming server that accepts donations for hosting commercial under this section? (2) Assuming you're dead-set on having this in the P/P requirements, I suggest you narrow it in a few ways: (a) Explicitly exclude donations from the definition of commercial. (b) Put a floor on the amount of money process to be "used for financial transactions." For example, a website would still be allowed to use a P/P service if they saw less than $10,000 per year in transactions. (c) Exclude non-monetary types of transactions from the definition of transaction. (e.g. database transactions) (3) No.	6/28/2015 5:33 PM
33	No, you have no business in other people's business.	6/28/2015 3:07 PM

34	I don't understand the value of this approach. Websites mutate all the time, this is more red tape to deal with. One day a blog might start selling things on the side for instance. It's not clear what value this designation actually provides.	6/28/2015 2:27 PM
35	1. No, commercial activity is vaguely defined and neccessary for the functioning of many basic speech activities. 2. No, there should be no attempt to define commercial or transactional activity, because the result will be vague, apply to every domain name, and be used as an excuse to destroy privacy. 3. No.	6/28/2015 2:00 PM
36	This is terrible and bad.	6/28/2015 1:22 PM
37	(1) Not in general, and especially not with a clear definition of (2). (2) I do not. (3) No, per (1) and (2).	6/28/2015 12:42 PM
38	1. No, because 'commerial activities' is way too vague. I'm a guy in a basement writing iPhone apps. I don't want my address published.	6/28/2015 12:02 PM
39	They should be allowed to use privacy and proxy services. Many small and home businesses operates online, and deserves privacy protection. Should abuses occurs, if should be left to the legal system to obtain the customer data and pursue the case. While this may create a greater burden on the victim / LEA, it is a reasonable price to pay to protect the innocent users of privacy / proxy services.	6/28/2015 12:01 PM
40	1. Registrants should never be prohibited from using privacy services for any reason. The content of their websites is irrelevant.	6/28/2015 11:47 AM
41	whois is not necessary. Try to get a normal response from Paypal...rest my case.	6/28/2015 10:56 AM
42	1) P/P services should be available to all registrants, without constraint or condition. 2) N/A 3) No	6/28/2015 8:00 AM
43	Hell no! The free market will handle these issues, not the unelected	6/28/2015 7:55 AM
44	(1) - no (2) - no (3) - yes	6/28/2015 6:21 AM
45	No comments - I'm not really interested in the specifics. Please don't make it (ICANN) worse than it already is.	6/28/2015 5:20 AM
46	Due process per the law of the domain owner's country should be required before revealing information.	6/28/2015 4:20 AM
47	People using domains for "commercial"/"financial" activities should have the same opportunities as everyone else. Proposals otherwise are stupid; if I put a paypal donation button on my blog, I would fall under this heading.	6/28/2015 3:52 AM
48	The use of a domain should not be a relevant factor. All domains should be able to take advantage of privacy/proxy services. If anything sites that deal with online financial transactions need to protect their owners more since sites dealing with money are bigger targets for phishing and hacking and any revealed information is revealing a target that a hacker can attempt to compromise.	6/28/2015 3:38 AM
49	P/Ps should be available to all with no Whois disclosure necessary. Consumers have sufficient protection under current law, regulation, and payment processor protection. Consumers are also smart enough to buy from markets that they trust.	6/28/2015 3:31 AM
50	Should registrants of domain names associated with commercial activities and which are used for online financial transactions be prohibited from using, or continuing to use, privacy and proxy services? If so, why, and if not, why not? Sometimes it's nicer to know that no one knows where something is than everyone and you know where something is located.	6/28/2015 3:24 AM
51	NO	6/27/2015 5:51 PM
52	If they choose to hide behind p/p services that is up to them. - There may be valid reasons - like for example animal rights activists attacked the bank holding a particular animal reseach company. It is also up to me wehther I choose to use such a bank/online service.	6/27/2015 1:28 PM
53	It's not fair to individuals, bloggers and small businesses that have their home address listed for their domain. Large corporations and bigger companies with brick and mortar addresses have the luxury of not having their personal information listed. Security and safety: Let's say I'm a blogger and I make money from my site. I'm guessing this would mean commercial. But I happen to blog about anti muslim type stuff. If my address were revealed this would put my life, my wife and kids life and even my dogs life in harms way, not to mention my property. According to the law, I have a right to feel safe and secure in my own home without distress. I'm not a lawyer but this new proposal seems like it would put certain peoples safety in harms way. And to be clear I don't blog about anti muslim stuff, it was just an example. Plus, we pay for this service. So the executives at ICANN came up with the brilliant idea of "hey, let's cut this so our revenues decrease." Any other corporation in the world would fire the people who came up with this idea. Jus saying.	6/27/2015 12:24 PM
54	1/2: No. 3. No.	6/26/2015 11:53 PM
55	For (1): NO, privacy is extremely important for everyone, including registrants of domain names associated with commercial activities, so they MUST BE ALLOWED TO USE A P/P. The only judge of the necessity of disclosure is a court of law, not ICANN or anyone else. For (3): No, no distinction should be made.	6/26/2015 1:17 PM
56	There should be no exceptions whether commercial or personal. Everyone should have the right to use privacy and proxy services. It should not be limited based on the use or activity behind it.	6/26/2015 12:23 PM
57	1) No	6/26/2015 4:16 AM
58	31 (1) No. This is not a useful position to take and forces a domain registrants to abuse and spam for which the p/p services have been most effective at controlling. 31 (3) No. This is likely to be difficult to maintain and not of much use.	6/25/2015 6:56 PM
59	1. No, no, no. Because people will redefine financial transaction to suit their needs. Only ferally or internationally regulated industries like banking should be subjected to such an over reaching and bullshit loophole. Clearly this loophole was written and paid for by the organizations pushing for these changes to outlaw privacy in the name of catching those utilizing piracy.	6/25/2015 4:04 PM
60	I don't know if it's feasible to implement but I agree that it would be best if sites performing online financial transactions be barred from P/P service usage.	6/25/2015 3:41 PM
61	1. I do not agree, they should NOT be prohibited, all commercial websites that take payment could be considered as being associated with online financial transactions. If I sell you a mobile website and use paypal or authorize.net I am associated with online financial transactions. Spammers use 3rd party sites to take money so this will not stop them, it will be the innocent domain owners who get damaged by a provision like this.	6/25/2015 2:59 PM

62	1. Domain names used for commercial financial transactions should be allowed to use privacy and proxy services. This will protect home business owners, among others (particularly depending on the definition of 'commercial' that is in use). Existing law and regulation is sufficient to provide relevant disclosure of details. If the domain owner's jurisdiction requires businesses to publish contact information, as Germany does, they can do so via WHOIS or via a link on their web site. Payment processors will already have obtained sufficient information from the business owner to handle fraud cases. It is not necessary for ICANN to impose this kind of requirement worldwide. Barring commercial transaction domains from using P/P services would place onerous requirements on users who engage in one-time commerce, such as offering up a service or soliciting donations via PayPal in an otherwise non-commercial blog. It would be further complicated by the particular definitions of 'commercial'. Is a blog that contains a link to the author's Patreon commercial? What about their KickStarter? Do affiliate links make a web site commercial?	6/24/2015 8:18 PM
63	Registrants of domain names associated with commercial activities which are used for online financial transactions should not be prohibited from using, or continuing to use, privacy and proxy.	6/24/2015 2:04 PM
64	Registrants of domain names associated with commercial activities and which are used for online financial transactions should be prohibited from using, or continuing to use P/P services. Consumers have a right to know who they are doing business with, and instituting a requirement that operators of domain names involved in commercial activity not be permitted to hide their identity behind privacy/proxy services is a step in the right direction in this regard. Whether it is an adult, gambling, counterfeit product, child abuse, multimedia download/streaming, or drug trafficking website, it is these type of websites where privacy/proxy services are utilized to obfuscate the identity of the website operator. Individuals operating these type of websites are typically also involved in other cyber criminal behavior, including identity theft , fraud, spam, and malware. Legitimate commercial businesses have no need to hide their identity; brick and mortar businesses do not have that option, nor should cyber commercial businesses. Commercial Domain Name: A definition for consideration; a website utilized to market goods or services intended to be purchased by the general public, whereby a profit is made from the sale of such marketed goods or services. Transactional Domain Name: A definition for consideration; a website where payment for goods or services is processed via credit card, e-check, or any other method of payment accepted by the website. Yes, it would be helpful to make a distinction in WHOIS data fields to identify commercial and transactional domain names.	6/24/2015 1:37 PM
65	No distinctions should be made. P/P services should be available to everyone.	6/24/2015 1:11 AM
66	1) continue using proxy/privacy While a major corporation may be at less risk, small businesses and sole traders/individuals may include victims of domestic abuse who may wish to avoid being tracked by an abusive ex. Such a threat could restrict individuals from pursuing the ability to earn a living online out of simple fear (eg my father being an abusive alcoholic poured lighter fluid on my mother and set her on fire...I am not comfortable with the idea of having my contact details made readily available as I have sought to avoid his being made aware of where I am or what I am doing...he terrifies me...loss of privacy runs the risk of me retreating from the idea of building a website to seek financial independence and I can only assume this would be a cause for concern for any victim of domestic violence.) In regards to dealing with the public, bloggers who may operate a blog as a commercial activity (just by way of incorporating advertising to fund their website) may be affected if a statement is found offensive by an unstable element in the community who may seek to harm the blogger, thereby restricting free speech. This can in turn affect anyone dealing with the public face-to-face who may not desire contact details to be readily available. (In my case, I do deal with the public face-to-face and have been threatened by individuals (ranging from junkies to mentally unbalanced obsessive individuals)...the idea of them being able to access my personal contact details just by looking up my website is cause for concern)	6/23/2015 12:13 PM
67	Privacy and proxy services should NOT be restricted based on commercial or non-commercial use. In fact, how a company, organization, agency, or person uses a domain is not in the purview of ICANN or part of its charter. Plenty of offline regulatory bodies are already present to facilitate this information. These bodies predate ICANN and are charged with working in this particular area of regulation. ICANN needs to leave this matter alone for ever as the disagreement in the working group shows ICANN will make no one happy unless they leave this issue alone.	6/22/2015 1:08 PM
68	1) No. Commercial is too static and broad	6/22/2015 12:15 PM
69	no opinion -- lack of expertise in this area.	6/21/2015 7:32 PM
70	It is not clear if online financial transactions means a bank or transfer of money from point a to b versus a sale of an Item. Many sole proprietors, an artist or photographer, sell one work of art online and register as an individual. If that is a "transaction", I object! Icann may publicly reveal the true Name, but the address, telephone, email contact info are abused by criminals and threaten the safety and life of single women and men who sell online. P/P protects us from criminals.	6/20/2015 10:21 PM
71	1: Everyone deserves the right to privacy even if the domain is being used for commercial activities. 2: Everyone Should be allowed private whois. 3: Everyone should be allowed private whois.	6/20/2015 2:24 PM

Q32 Please include any additional comments or suggestions for the WG here.

Answered: 57 Skipped: 295

#	Responses	Date
1	Keep it simple: Just ban P/P services totally.	7/7/2015 7:36 PM
2	None	7/7/2015 9:36 AM
3	I suggest the introduction of a new top level domain solely for personal rights purposes, like freedom of speech. Registering Domains under that TLD should be possible completely pseudonymous, without giving any contact details but a working email address. The commercial use of that TLD must be strictly prohibited, including any kind of advertising. Only strictly personal use by non-commercial individuals should be allowed.	7/7/2015 7:15 AM
4	I urge you to respect internet users' rights to privacy and due process. Please let my explain why WHOIS Guard is required, from my personal perspective. -- The principal reason is the home address. I have a small blog, but why do I have to put my home address on the whole world just because I run a blog on a domain? Why do I have to open the door of harassment just because I have a website? -- If people know my home address, they can physically do almost anything if they do not like my website. Especially in my country Bangladesh, there is a tradition of killing the blog author if some group just do not like what blogger said. For example, one blogger, Avijit Roy, was murdered recently because some Islamic activists did not like his blog. See: https://en.wikipedia.org/wiki/Avijit_Roy -- How do you define whether a site is commercial or not? I am planning of placing adds on my blog, but not selling anything. Thereby, how can you classify whether it is a commercial or personal site? Putting adds on a website does not make it a commercial site, unless it sells something. -- And even if it is a commercial site, it may need privacy. Yes, I know that big commercial firms do not need Whois protection. But what about small business owners? Some of them definitely need this protection. For example, if I sell my books from my own website that also hosts my bolg, do I have to disclose my home address? -- Besides, I use Whois privacy because otherwise spammers will know my personal email address, and I have to spent substantial amount of time and energy every day to find out which mail is spam and which is not. As I mentioned, I have to do this checkup in my inbox on a regular basis. As you see, if you prevent domain owners from using WhoisGuard protection, it will create more problem than that it will solve. Therefore, disclosure of Whois information should only be made upon a court order.	7/6/2015 12:39 PM
5	thank you for the opportunity to comment on your work.	7/6/2015 12:11 PM
6	The privacy and rights of regular internet users are the greatest concern above all others such as IP rights and law enforcement.	7/6/2015 3:33 AM
7	ICANN risks losing the confidence of the people if it enacts the proposed policies.	7/6/2015 1:07 AM
8	All domains should be able to use privacy services. Only LEA should be able to request publication or disclosure.	7/5/2015 6:52 PM
9	This document is a hall of mirrors. State legislation is crystal clear by comparison. Please reduce the amount of incorporation by reference, especially in cases where the terms are neither defined nor linked.	7/5/2015 2:49 AM
10	Individuals need to be protected. However, it is better that these are done at the local level (eg. my .co.uk are protected by my UK level registrar; I simply declare myself as an individual) - so if that was done across the board, then there would be no need for third party privacy services ... and hence a lot of grief would be saved.	7/5/2015 2:36 AM
11	Please simply discontinue the WHOIS database.	7/4/2015 1:44 AM
12	Abandon accreditation entirely.	7/2/2015 7:51 PM
13	Get out of the P/P business. Kill the accreditation program.	7/2/2015 9:53 AM
14	ICANN, no offense intended, needs to disappear. I'm not a proponent of deregulation of commercial processes, but ICANN takes things too far. Just... Go away and leave individuals alone, please.	7/2/2015 9:06 AM
15	All I care about is being spammed. If our email is publicly available someone will write a bot to harvest and sell this and we will be buried in spam mails meaning any mail to this address will be treated as spam and ignore, completely defeating the whole purpose of it.	7/2/2015 6:19 AM
16	KEEP MY INFORMATION PRIVATE!!	7/1/2015 7:11 PM
17	My privacy is more important than your right to know my personally identifying information.	7/1/2015 3:32 PM
18	The voice of the IPC is way too loud in this proposal. This flies in the face of consensus and developing an internet everybody can use and enjoy.	7/1/2015 9:00 AM
19	Online privacy needs to be taken as seriously as medical and lawyer secrecy. It must be made clear that a Chinese dissident, or a Saudi blogger face death penalty or 1000 whip lashes when privacy is breached.	7/1/2015 5:03 AM
20	The intentions in these recommendations seem to have good intentions, but I am against any proposal which makes it easier for large organizations with power and for dangerous individuals to be able to find and threaten to silence their critics. Policies with low standards for this disclosure threaten to harm that privacy. Furthermore, imposing these sorts of requirements onto proxy/privacy service providers may threaten to only further disorganize and disintegrate the system in place. These practices and their implementation are best left to the domain registrars themselves, as it is both in their interest and the interest of their customers.	6/30/2015 11:33 PM
21	Please let the existing system continue. We need the right to privacy and right to free speech preserved. There is absolutely no use in these new processes and in turn stealing users of their freedom. We do not need accreditation for these providers in the first place. Let the existing system continue. In this age of deteriorating privacy protections, such moves are detrimental and harmful for people's freedom and right to privacy. It's appalling that such moves are even being considered.	6/30/2015 10:53 AM
22	Spam, harassment, and other third-party attacks are too numerous for WHOIS to operate as intended; in fact, the presence of privacy and proxy services is largely due to this vulnerability. ICANN should not seriously restrict the availability of these services, nor make rules that impair their ability to adapt to changing conditions, at least as long as WHOIS data is available to third parties who might want contact information for malicious purposes.	6/29/2015 6:47 PM

23	Please don't hinder privacy and proxy providers from being able to provide the service they already provide. Privacy is a fundamental human right, a single organization can't decide who "deserves" that right, as everyone does. Even if the intentions are "good", every small concession grants more power to the already powerful, and takes away from everyone else.	6/29/2015 1:30 PM
24	This sort of accreditation/verification/enforcement activity is outside ICANN's scope and expertise	6/29/2015 8:01 AM
25	I think the planned changes are foolish and would prefer that no changes occur.	6/28/2015 6:07 PM
26	Thank you for the chance to provide input. :)	6/28/2015 5:34 PM
27	fuc|{ off!!!!	6/28/2015 4:59 PM
28	Please abandon this ill fated attempt to assert control over something that will do more harm than help by enabling the "legitimate" authorities or violent people to seriously injure random people on the internet.	6/28/2015 2:28 PM
29	Please stop being the puppet of large business interests. While it is inconvenient for them to not be able to violate the privacy of everyone who threatens their 20th century business models, this a matter of life and death for those of us who engage in unpopular political speech. All frameworks for defining and violating privacy will be abused. A momentary leak of private information means death for atheist bloggers in Bangladesh, death for political dissidents in Russia, and death for transgender individuals in the United States. Please do not kill us because a record company wants to marginally improve how efficiently they exploit some dumb kids with music instruments.	6/28/2015 2:05 PM
30	These regulations might trigger the end of ICANN, it makes domain holders conscious of the urge of looking for an alternative system of url resolving.	6/28/2015 10:57 AM
31	Hosting own domain with some required software is a good defense against online profiling for various purposes. The infrastructure in place has been good enough, there is from my point of view nothing to fix. Why would ICANN try to stop that ??	6/28/2015 10:00 AM
32	DO NOT CHANGE ANYTHING, YOU NEED A WARRANT, I NEED PRIVACY	6/28/2015 9:26 AM
33	P/P services should be prohibited from disclosing information to any third party, unless compelled by a court order or similar legal document, and even in that circumstance not without notifying the user, unless specifically prohibited by the order.	6/28/2015 8:01 AM
34	The free market will remain free, and there is plenty of technology to build around the police state. You need to get on the side of freedom and privacy, and be better than the police state. Make a choice. Let freedom reign.	6/28/2015 7:56 AM
35	Thank you for this opportunity to voice my concerns.	6/28/2015 5:21 AM
36	You are troubling millions of good-faith users with significant threats to their personal safety, while creating a set of rules that a malicious user could trivially circumvent!	6/28/2015 4:22 AM
37	I am worried about the threat to privacy posed by ICANN. As an organization it is going to dark places. It should be standing up for freedom, not serving those who are opposed to it.	6/28/2015 3:52 AM
38	Everything about ICANN continues to become more and more backwards. As fishing and hacking get worse and there are constantly state-sponsored thefts of personal information it should be moving away from linking the DNS system with personal information that can easily be used for fishing and target hacking. The Whois system is walking giant security vulnerability and they only reason it hasn't blown up in your face is that regular everyday people can hide their personal and contact information from spammers, hackers, and the Chinese.	6/28/2015 3:41 AM
39	Please don't drive more of a wedge between the Internet for the people and the Internet for corporations. Trying to reduce the freedoms of users will lead to splits in the network, reducing value for everyone.	6/28/2015 3:32 AM
40	Please don't make P/P services useless. Please don't break the internet. Thanks.	6/28/2015 3:24 AM
41	Respect Privacy!	6/27/2015 9:54 PM
42	Leave it like it is. In fact make our domain privacy more secure than it is now.	6/27/2015 5:51 PM
43	ICANN don't apply their own rules to themseleves with regards to their own whois entry in their own whois database - so why should me as a single person company put my name home address and phone number on the internet to facilitate identity theft and unwanted attention from many different sources? Even on Facebook I do not publish my address or phone number -and my account is limited to my friends - why the hell should I publish it on ICANNs whois?	6/27/2015 1:31 PM
44	It's not fair to individuals, bloggers and small businesses that have their home address listed for their domain. Large corporations and bigger companies with brick and mortar addresses have the luxury of not having their personal information listed. Security and safety: Let's say I'm a blogger and I make money from my site. I'm guessing this would mean commercial. But I happen to blog about anti muslim type stuff. If my address were revealed this would put my life, my wife and kids life and even my dogs life in harms way, not to mention my property. According to the law, I have a right to feel safe and secure in my own home without distress. I'm not a lawyer but this new proposal seems like it would put certain peoples safety in harms way. And to be clear I don't blog about anti muslim stuff, it was just an example. Plus, we pay for this service. So the executives at ICANN came up with the brilliant idea of "hey, let's cut this so our revenues decrease." Any other corporation in the world would fire the people who came up with this idea. Jus saying.	6/27/2015 12:24 PM
45	This is an assault on small business and people concerned with the truth.	6/26/2015 11:54 PM
46	The purpose of the P/P services is to protect the registrants privacy, so they need to do so no matter what the registrant's activity is. Only the justice system can ascertain if the registrant did something illegal and if his/her details needs to be disclosed.	6/26/2015 1:20 PM
47	Keep our privacy safe, secured, and legal. Thank you!!	6/26/2015 12:23 PM
48	Anonymity is essential	6/26/2015 4:19 AM
49	Thanks for the opportunity to comment.	6/25/2015 6:56 PM
50	These rules that are meant to expose private data must not be allowed to move forward. These companies paying tons of Mon&y to get these rules already have the legal framework to work within. There is no need to take away a service that makes it possible for millions of people and businesses to have privacy bc a few organizations are throwing money at it. Kick them to the curb and tell hem tonuse the laws and regulations already in place. If they don't like having to work for the data they want, then tell them that's too bad bc 99.9% of the businesses and people out there do nothing wrong and they are risking the backbone of the internet by being greedy.	6/25/2015 4:09 PM

51	IP, trademark and copyright infringement is on everyone's mind because the companies that profit from those activities are spending large amounts of money to make sure it is. The same was true of the publishing industry when libraries first started to appear. I think many would find it hard to argue that libraries have been good for mankind. Here too the publishing companies have flourished. I think the same will be said when history looks back on this period of time. However the loss of privacy is irreversible and should be guarded against. Individuals lack the resources to stand up to the giant corporations that want all of their information - so they can profit from it. I believe the internet should not be for the profit of a few companies but for the sharing of ideas and betterment of mankind overall. Please protect the privacy of the individual.	6/25/2015 3:48 PM
52	WHOIS privacy should be maintained at all costs to protect commercially sensitive information, prevent a massive deluge of spam to domain owners. GoDadddy needs to relay ALL domain registration information to other sites, they are NOT a special case. You can email me at jwilson0@ymail.com	6/25/2015 3:01 PM
53	I use privacy to assist in limiting my exposure to spam, as well as to feel secure when operating online due to the knowledge that my abusive father (and other unstable members of the public) are less likely to track me down. In the event that the option to make my contact details privacy is removed, I have a very real fear for my life. I see this as a major concern for all victims of domestic violence or bullying, along with any social service that seeks to assist those in such situations, especially when seeking financial independence.	6/23/2015 12:24 PM
54	Dear ICANN – Regarding the proposed rules governing companies that provide WHOIS privacy services (as set forth in the Privacy and Policy Services Accreditation Issues Policy document) I urge you to respect internet users' rights to privacy and due process. - Everyone deserves the right to privacy. - No one's personal information should be revealed without a court order, regardless of whether the request comes from a private individual or law enforcement agency. Private information should be kept private. Thank you, Jeff Walsh	6/22/2015 6:47 PM
55	THANKS for collecting input before action.	6/21/2015 7:32 PM
56	Please remember many individuals do some "commercial" work that is different from multi-national commercial operations.	6/20/2015 10:23 PM
57	This whole policy is totally stupid! Put it in the trash and start again.	6/20/2015 2:25 PM