Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
1. Definition of Terms				
1.1. The “Requestor”: Law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the privacy or proxy service provider is established or maintains a physical office;	Michele Neylon (and others)--we must stick to this definition and limit this to the provider's jurisdiction Janelle McAlister (on list): 1.1. This must be limited to the providers local jurisdiction only. Law enforcement or government consumer protection agencies should be included, but I question whether non-government consumer protection agencies should be included.	Nick Shorey (on 6 June call); LEA is defined here, but the document says (See Section 6) that any request from LEA outside the jurisdiction--the provider may voluntarily choose to action those where you deem it does not conflict with national law		

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
1.4. The “Requested Information”: The data asked for by the Requestor. This must be detailed in the request submission, and may include, but is not limited to: Customer registration data directory service records; contact data including email addresses, usernames, contact telephone numbers residential addresses and any other subscriber number or identity; billing and payment information including bank account numbers, billing records, credit and debit card details; verification documents; account access data including session times, duration and associated IP addresses.	Greg DiBiase (6 June IRT call): this definition includes more than the definition of "disclosure" in the Policy Recs. Is that extra information (cc info, banking #s) included in your definition of disclosure here? Chris Pelling (on list): please confirm that the "Requested Information" part 1.4 will not be in breach of GDPR, as it is pertaining to personal information. Moreover, as a quick thought, information like Credit card details - simply wont be provided (as for wholesale registrars like myself, we wont have it). Also from a technical point, session duration is probably not logged by most registrars - the platform we use certainly doesn't.	Nick Shorey (6 June) Yes, that's correct, the requested information details are non-exhaustive and include information that may be requested.		

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
1.5 The “Priority Level”: The urgency with which the disclosure request should be actioned	Greg DiBiase (on list): Section 1.4: “Requested Information” significantly exceeds the scope of the policy and the type of information contained in WHOIS data (e.g., credit card information and account access data/session times). Depending on the jurisdiction, a subpoena or court order may be required for some of the information contained in this definition. Janelle McAlister (on list): 1.4. The requestor should be required to provide a subpoena for the additional, non-contact information including billing and payment information including bank account numbers, billing records, credit and debit card details: verification documents: account access data including session times, duration and associate IP addresses; this additional information may not be easily accessed or available Chris Pelling (on list): 1.5 - I don't believe we have had priority levels before, but, this will no doubt piggy back on the RAA whereby its upto 24 hours. (similar your 3.2.1 section mentions this time-frame)			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
	Michele Neylon (on list): 1.5 – is there a list of priority levels? One of my concerns with this is that the lazy method would be to always set the level as “fastest” or “top priority”. I see there are two rather vague ones mentioned elsewhere in the document. Greg DiBiase (on list): Section 1.5: “Priority level” and various priorities should be better defined. Perhaps in a tiered system with defined turnaround times? (e.g., High Priority requests require a response time of 48 hours)			
2. Minimum requirements for disclosure request submissions				
2.1. As a minimum standard for acceptance, disclosure request submissions must contain:	Greg DiBiase (on list): Section 2.1: The Minimum Requirements should include some form of verification statement, e.g., all provided information is true and correct.			
2.1.1 Domain name or URL involved	Janelle McAlister (on list): 2.1.1. should be limited to Domain Name only – remove “URL involved”			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
2.1.2. Deciding authority (i.e. prosecutor, judge) behind this request; 2.1.3. Details of Requested Information; 2.1.4. Priority Level and / or deadline for response;	Chris Pelling (on list): 2.1.2 states authority of request, this needs clear allowable requesters', police authority would be another one to add for example Greg DiBiase (on list): Section 2.1.3: This clause should include the legal authority justifying the provision of data. Something like, “Details of Requested Information and legal authority to obtain each element thereof”. Currently, there is no requirement in the document for the legal authority justifying the provision of data to be spelled out (just the identity of the authority in 2.1.2 and the optional “reference” to laws in 2.2.3). Chris Pelling (on list): See 1.5 above Roger Carney (on list): 2.1.4 Priority Level – 4.1.2 mentions providing justification of priority, should that be a requirement here? Deadline – probably should be “requested” deadline			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
2.1.5. Instructions regarding timeline requirements for customer notification;	Chris Pelling (on list): 2.1.5 Unless similar to current requests it is stamped "restricted" then this should be instant notification to customer that their personal data (thinking GDPR here and common decency) has been requested.			
3. Receipt process				
3.1.1 The Provider will establish a designated Requestor point of contact for submitting disclosure requests. These details will be published on the Provider website.	Michele Neylon: I don't see why the LEA point of contact should be public; I'm happy to share it with the government but if we put it on our site it'll just get junk	Nick Shorey (on call) this was for ease of access so that LEA can find it		

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
		Nick Shorey (on call): I'd be interested to hear your thoughts about how to proceed--we could discuss the possibility of having a page telling LEA how to proceed if you can ID precisely how this could be done, examples of how these contact points are abused. The important point is that there is an accessible contact for LEA to make requests. It may be a new provider that they haven't contacted before and they need to have a quick mechanism to make a request.		
	Luc Seufer: Same here, it would be more efficient to have the details for emergency action communicated to the local LEA			
	Michele Neylon: We created an email alias for domain registries + put it on our site - all we've got was spam + other stuff sent to the wrong place			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
	Michele Neylon: I disagree strongly Nick Luc Seufer: @Nick in such case then it can't be the emergency poc Chris Pelling: agreew ith Michele Graeme Bunton: Operationally, any public contact get filled with garbage. Luc Seufer: it can only be a generic one for agencies to obtain the emergency one Michele Neylon--publicly available emails get scraped, added to lists. The only way to have a responsive contact point is if the contact is only shared within a circle of trust--making it publicly available won't work. We could add something on the website--if you are LEA and want the dedicated LEA contact please contact us... fine, but putting an emergency PoC on the website won't work, it will just get abused.			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
	Janelle McAlister (on list): 3.1.1. Providing the email address on a website will drastically increase the spam and abuse of the email address and may delay responses to legitimate request.			
3.2.1. Within 24 hours of the disclosure request been submitted, the Provider will review the request, and confirm it has been received and contains the relevant information required to meet the minimum standard for acceptance. If the request does not meet the minimum standard, the Provider will notify the Requestor.	Luc Seufer: 24 hours is not reasonable, even the Requestor don't all have a 24 hour service. Michele Neylon: +1 Luc, it's completely unworkable Volker Greimann: We do have week-ends and holidays where NO STAFF is available	Nick Shorey (on call)--this is why we distinguished between high priority and other requests and the process of receipt and action is a 48-hour period for high-priority requests.		

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
	Michele Neylon: the 24 hours is hugely problematic. Obviously you got this from the 2013 RAA but the RAA provision is limited to abuse, which is purely operational--this goes more broadly than that and may require consultation of outside counsel, etc, which can't usually be done in 24 hours. Steve Metalitz (on 6 June IRT call): Re: the 24-hour turnaround, I just want to clarify what the doc says--24 hour deadline for the receipt process (3.2.1)--that request satisfies requirements and seems that it wouldn't require consultation with counsel; and then the high priority deadline comes after so it's really 48 hours. In terms of high priority requests, is the list in 4.1.1 an exclusive list so that the 48 hour process would only apply to imminent threat to life, critical infrastructure, child exploitation etc?	Nick Shorey (6 June IRT call): you are correct, there's a timeline--24 hours for receipt process and 24 hours for response; in terms of making 4.1.1 exclusive list, that's an interesting point that we can discuss further if that would make it significantly improved for providers to be able to sign off for it and action high priority request		

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
	Chris Pelling: @Nick just to make sure, our office is in the UK, if we get a request from a German or Australian LEA, we can simply reply wihtin the time frame stating it is rejected as not out local LEA (or quasi.....) ?			
	Chris Pelling: @Nick, this really needs to be put back to LEA ie. any worldwide requests are put throught the LOCAL LEA of the provider or where they have an office			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
3.2.2. Where the Requestor is not known to the Provider, the Provider will verify the identity of the Requestor	Janelle McAlister (on list): 3.2.1. Change to "Within 48 hours during standard working days and 72 hours during weekends and holidays" Stephanie Perrin: That is what I thought. I would have expected the procedure to be done in reverse....i.e. requestor has the burden to prove the entity is authorized Stephanie Perrin: I think either a request should come with proof that the requester meets the requirements as an LEA requestor or the request should be rejected rather than requiring the provider to verify Greg DiBiase: What is the process for the Provider verifying the identity of the Requestor? Is there a databse we will be able check?	Nick Shorey (on call)--we have required that requester include their contact information so that the provider can verify		

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
	Greg DiBiase (on list): 3.2.2: How does the Provider verify the identity of the Requestor? Would governments maintain a page with all of the law enforcement contacts that could submit a valid request, and we'd have to go check against that each time we received a request? Greg DiBiase (on list): Section 3.2.2: How will the Provider verify the identity of the Requestor and ensure that such requests are not fraudulent? Authentication and verification are critical. Janelle McAlister (on list): 3.2.2. The burden to prove the identity of the requestor should be on the requestor			
4. Provider response actions				
4.1 Prioritization 4.1.2. Where a disclosure request has been categorized as High Priority, this must be actioned within 24 hours. The Requestor will detail the threat type and justification for Priority Level.	Michele Neylon--You need to define/differentiate this because otherwise all requests may default to "high priority" Roger Carney (on list): 4.1.2 How is "actioned" defined			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
	Janelle McAlister (on list): 4.1.2. Change response time to 48 hours during standard working days and 72 hours during weekends and holidays			
4.2.1. Within the appropriate timeframe consistent with the Priority Level, the Provider will disclose to Requestor using a secure mechanism the Requested Information it holds against the account.	Theo Geurts (6 June IRT call) Re: "secure mechanism" perhaps we should park this until this work is finished steve metalitz (6 June IRT call): @Michele, @Nick , perhaps this concern would be addressed by adding a parenthetical after "secure mechanism" -- "(if available) "		See Transfer Policy, Change of Registrant Process, Section C.1.2, "...The Registrar must use a *secure mechanism* to confirm…" Examples of "secure mechanisms" are included in the Policy's implementation notes: (1) sending an email requiring an affirmative response through a tool-based authentication method such as providing a unique code that must be returned in a manner designated by the Registrar; or (2) calling or sending an SMS to the Registered Name Holder's telephone number providing a unique code that must be returned in a manner designated by the Registrar; or (3) calling the Registered Name Holder's telephone number and requiring the Registered Name Holder to provide a unique code that was sent to the Registered Name Holder via web, email or postal mail.	This has already been defined in the transfer policy implementation (the implementation notes defining "secure mechanism are based on the RAA WHOIS Accuracy Program Specification), IRT should consult this list to confirm whether this would work in this context or whether this should be separately defined for this policy.

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
4.2.2. Disclosure can be reasonably refused, for reasons consistent with the general policy stated herein, including without limitation any of the following:	Chris Pelling (on list): GDPR?			
4.2.2.3. where the customer has provided, or or the Provider has found, specific information, facts, and/or circumstances showing that disclosure will endanger the safety of the customer.	Roger Carney (on list): 4.2.2.3 How is safety defined? Greg DiBiase (on list): Section 4.2.2.3: Disclosure can be refused where "disclosure will endanger the safety of the customer." That's a high standard and will be difficult for Providers to interpret in practice. It's conceivable people other than the customer could be endangered as well. At a minimum, the language should be "…disclosure may endanger the safety of the customer or others."			
4.2.3 If disclosure is refused, the Provider must state to the Requestor in writing or by electronic communication its specific reasons for refusing to disclose. This must be completed prior to any Customer Notification, irrespective of the reason for refusal;	Chris Pelling (on list): So, 2.1.5 above, unless it is marked "restricted" we would have already told the customer that a request for information had been received.			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
4.2.5. For all refusals made in accordance with the policy and requirements herein, the Provider must accept and give due consideration to Requestor's requests for reconsideration of the refusal to disclose.	Michele Neylon (on list): 4.2.3 – "This must be completed prior to any Customer Notification irrespective of the reason for refusal" – I don't see how or why we would agree to this. Unless you have a court order or similar gagging us. Also it's inconsistent with the grounds for refusal. Greg DiBiase (on list): Section 4.2.3: Provider must respond to Requestor with specific reasons for refusal, which must happen before any Customer Notification. While Providers generally will and likely should notify Requestor before issuing a Customer Notification, there could be exceptions. Chris Pelling (on list): 4.2.5 A "limit" must be placed on this, it cannot keep being returned to the provider by the requester knowing that the requester is wasting the time of the provider each and every time of request thereafter. Example - Say the requester never changes the request, if it did not stand up the first time, it wont the 2nd, 3rd, 4th and 10th time either.			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
4.3 Customer Notification 4.3.1. The Provider will notify the Customer of the disclosure request in accordance with the timeframe identified by the Requestor.	Greg DiBiase (on list): Section 4.2.5: This is a very vague reconsideration provision. There is no standard for reconsideration requests. Janelle McAlister (on list): 4.3. The provider will notify the customer of the disclosure request unless the requestor has provided a subpoena Chris Pelling (on list): 4.3.1 I would suggest this is unacceptable unless "restricted" marked. Darcy Southwell (on list): ¶4.3.1 - I'm not certain that the Requestor (LEA) always has authority to set this timeframe.			
4.3.2. The Provider may voluntarily set a generic timeframe for Customer Notification (for example 90 days), which can be extended at the behest of the Requestor. Details of any generic timeframe must be published on the Provider website, and the Requestor must always be informed in advance of any time limit being implemented or changed.	Chris Pelling (on list): Er 90 days, I appreciate its an example, but, 1 day in my eyes is too long.			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
4.3.3. The Provider must notify the Requestor at least three working days before Customer Notification takes place.	Chris Pelling (on list): 4.3.3 Unless "restricted" customer is automatically notified on receipt of request (or within 24 hours), and the requester as notified by providers website must accept that. Michele Neylon (on list): 4.3.3 – sorry, but again I don't see why we'd agree to this.			
5. Issues of non-response/non-compliance with LEA requests				
6. Additional guidance				
6.1 The Provider may voluntarily action disclosure requests from non-designated government authorities in accordance with the processes detailed within this document, where such action does not conflict with national or international law(s).	Chris Pelling (on list): 6.1 So we have gone from LEA etc, now to "any" tom, dick or harry sending in a request ? Darcy Southwell (on list): ¶6.1 – this language is simply not necessary. What a provider may or may not do goes far beyond the single consideration of "where such action does not conflict with national or international law(s)." It may be based on legal advice from the Provider's counsel relating to a variety of issues.			

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
6.2. A Requestor must comply with all applicable data protection laws and to use any information disclosed to it solely for the purpose to determine whether further action on the issue is warranted, to contact the customer, or in legal proceeding concerning the issue for which the request was made.	Chris Pelling (on list): GDPR			
6.3. Customer notification should take place at the earliest opportunity, unless such disclosure would pose a risk to operational sensitivity; safety of individuals; or is prohibited by law or court order. Such circumstances must be detailed in the disclosure request.	Luc Seufer: "pose a risk to operational sensitivity" I am having trouble understanding Stephanie Perrin: I'm concerned about this bc data protection law requires more precision re: customer notice, what the delay is, is it a perpetual delay, etc. We are not trying to stop investigation but we need to put some parameters around what one might call fishing expeditions. "unless such disclosure would pose a risk"---practically any investigation has operational sensitivity so be more clear about what needs to go in the request to the provider.	Nick Shorey (on call): we stated in the document that it should take place at the earliest opportunity which I think is a positive thing. As we mentioned those details must be included in the request (re operational sensitivity)--the details may vary from jurisdiction to jurisdiction and from law to law		

Relevant Text From Draft Framework	IRT Feedback	PSWG Feedback	Notes	Possible Paths to Resolution
	Stephanie Perrin--we have made clear that certain groups (political groups, LGBT, churches, etc that are not necessarily protected by data protection law but do have privacy interests). What sort of protections/notifications do you envision here related to notifications? What about protections for these groups to challenge disclosure if the law does not protect them? Chris Pelling (on list): again, "restricted" Michele Neylon (on list): 6.3 – this seems to contradict the other references to customer notification	Nick Shorey (on call) what we are doing here is setting up a framework for how the process will function, including clear authority, relevant agency, minimum standard of information included in the request. I'm not going to get into the detail of national laws--what we are doing here is setting out a framework.		