HR-RT worksheet: Review questions framework from RFC 8280				
		Questions		**Notes**
6.2.1	**Connectivity**	*Freedom of expression, Freedom of assembly and association*		
	1	Does your protocol add application-specific functions to intermediary nodes?		
	2	Could this functionality be added to end nodes instead of intermediary nodes?		
	3	Is your protocol optimized for low bandwidth and high-latency connections?		
	4	Could your protocol also be developed in a stateless manner?		
6.2.2	**Privacy**	*Freedom of expression, Non-discrimination*		
	1	Did you have a look at the guidelines in Section 7 of [RFC6973] ("Privacy Considerations for Internet Protocols")?		
	2	Could your protocol in any way impact the confidentiality of protocol metadata?		
	3	Could your protocol counter traffic analysis?		
	4	Could your protocol improve data minimization?		
	5	Does your document identify potentially sensitive data logged by your protocol and/or for how long that data needs to be retained for technical reasons?		
6.2.3	**Content Agnosticism**	*Freedom of expression, Non-discrimination, Equal protection*		
	1	If your protocol impacts packet handling, does it use user data (packet data that is not included in the header)?		
	2	Does your protocol make decisions based on the payload of the packet?		
	3	Does your protocol prioritize certain content or services over others in the routing process?		
	4	Is the protocol transparent about the prioritization that is made (if any)?		
6.2.4	**Security**	*Freedom of expression, Freedom of assembly and association, Non-discrimination, Security*		

	1	Did you have a look at [BCP72] ("Guidelines for Writing RFC Text on Security Considerations")?		
	2	Have you found any attacks that are somewhat related to your protocol yet considered out of scope for your document?		
	3	Would these attacks be pertinent to the features of the Internet that enable human rights (as described throughout this document)?		
6.2.5	**Internationalization**	*Freedom of expression, Political participation, Cultural life-art-science*		
	1	Does your protocol have text strings that have to be understood or entered by humans?		
	2	Does your protocol allow Unicode? If so, do you accept texts in one charset (which must be UTF-8) or several (which is dangerous for interoperability)?		
	3	If character sets or encodings other than UTF-8 are allowed, does your protocol mandate proper tagging of the charset?		
	4	Did you have a look at [RFC6365]?		
6.2.6	**Censorship Resistance**	*Freedom of expression, Political participation, Cultural life-art-science, Freedom of assembly and association*		
	1	Does this protocol introduce new identifiers or reuse existing identifiers (e.g., Media Access Control (MAC) addresses) that might be associated with persons or content?		
	2	Does your protocol make it apparent or transparent when access to a resource is restricted?		
	3	Can your protocol contribute to filtering in such a way that it could be implemented to censor data or services? If so, could your protocol be designed to ensure that this doesn't happen?		
6.2.7	**Open Standards**	*Freedom of expression, Cultural life-art-science*		
	1	Is your protocol fully documented in such a way that it could be easily implemented, improved, built upon, and/or further developed?		
	2	Do you depend on proprietary code for the implementation, running, or further development of your protocol?		
	3	Does your protocol favor a particular proprietary specification over technically equivalent and competing specification(s) -- for instance, by making any incorporated vendor specification "required" or "recommended" [RFC2026]?		

	4	Do you normatively reference another standard that is not available without cost (and could you possibly do without it)?		
	5	Are you aware of any patents that would prevent your standard from being fully implemented [RFC6701] [RFC8179]?		
6.2.8	**Heterogeneity Support**	*Freedom of expression, Political participation*		
	1	Does your protocol support heterogeneity by design?		
	2	Does your protocol allow for multiple types of hardware?		
	3	Does your protocol allow for multiple types of application protocols?		
	4	Is your protocol liberal in what it receives and handles?		
	5	Will your protocol remain usable and open if the context changes?		
	6	Does your protocol allow well-defined extension points? If so, do these extension points allow for open innovation?		
6.2.9	**Anonymity**	*Non-discrimination, Political participation, Freedom of assembly and association, Security*		
	1	Did you have a look at [RFC6973] ("Privacy Considerations for Internet Protocols"), especially Section 6.1.1 of that document?		
6.2.10	**Pseudonymity**	*Non-discrimination, Freedom of assembly and association*		
	1	Have you considered [RFC6973] ("Privacy Considerations for Internet Protocols"), especially Section 6.1.2 of that document?		
	2	Does the protocol collect personally derived data?		
	3	Does the protocol generate or process anything that can be, or that can be tightly correlated with, personally identifiable information?		
	4	Does the protocol utilize data that is personally derived, i.e., derived from the interaction of a single person or from their device or address?		
	5	Does this protocol generate personally derived data? If so, how will that data be handled?		
6.2.11	**Accessibility**	*Non-discrimination, Freedom of assembly and association, Education, Political participation*		
	1	Is your protocol designed to provide an enabling environment for people who are not able-bodied?		
	2	Have you looked at the W3C Web Accessibility Initiative [W3CAccessibility] for examples and guidance?		

6.2.12	**Localization**	*Non-discrimination, Cultural life-art-science, Freedom of expression*		
	1	Does your protocol uphold the standards of internationalization?		
	2	Have you taken any concrete steps towards localizing your protocol for relevant audiences?		
6.2.13	**Decentralization**	*Freedom of expression, Freedom of assembly and association*		
	1	Can your protocol be implemented without one single point of control?		
	2	If applicable, can your protocol be deployed in a federated manner?		
	3	What is the potential for discrimination against users of your protocol?		
	4	Can your protocol be used to negatively implicate users (e.g., incrimination, accusation)?		
	5	Does your protocol create additional centralized points of control?		
6.2.14	**Reliability**	*Freedom of expression, Security*		
	1	Is your protocol fault tolerant?		
	2	Does your protocol degrade gracefully?		
	3	Can your protocol resist malicious degradation attempts?		
	4	Do you have a documented way to announce degradation?		
	5	Do you have measures in place for recovery or partial healing from failure?		
	6	Can your protocol maintain dependability and performance in the face of unanticipated changes or circumstances?		
6.2.15	**Confidentiality**	*Privacy, Security*		
	1	Does this protocol expose information related to identifiers or data? If so, does it do so to each of the other protocol entities (i.e., recipients, intermediaries, and enablers) [RFC6973]?		
	2	What options exist for protocol implementers to choose to limit the information shared with each entity?		
	3	What operational controls are available to limit the information shared with each entity?		

	4	What controls or consent mechanisms does the protocol define or require before personal data or identifiers are shared or exposed via the protocol? If no such mechanisms or controls are specified, is it expected that control and consent will be handled outside of the protocol?		
	5	Does the protocol provide ways for initiators to share different pieces of information with different recipients? If not, are there mechanisms that exist outside of the protocol to provide initiators with such control?		
	6	Does the protocol provide ways for initiators to limit which information is shared with intermediaries? If not, are there mechanisms that exist outside of the protocol to provide users with such control?		
	7	Is it expected that users will have relationships that govern the use of the information (contractual or otherwise) with those who operate these intermediaries?		
	8	Does the protocol prefer encryption over cleartext operation?		
	9	Does the protocol provide ways for initiators to express individuals' preferences to recipients or intermediaries with regard to the collection, use, or disclosure of their personal data?		
6.2.16	**Integrity**	*Freedom of expression, Security*		
	1	Does your protocol maintain, assure, and/or verify the accuracy of payload data?		
	2	Does your protocol maintain and assure the consistency of data?		
	3	Does your protocol in any way allow the data to be (intentionally or unintentionally) altered?		
6.2.17	**Authenticity**	*Privacy, Freedom of expression, Security*		
	1	Do you have sufficient measures in place to confirm the truth of an attribute of an entity or of a single piece of data?		
	2	Can attributes get garbled along the way (see Section 6.2.4 ("Security"))?		
	3	If relevant, have you implemented IPsec, DNSSEC, HTTPS, and other standard security best practices?		
6.2.18	**Adaptability**	*Education, Freedom of expression, Freedom of assembly and association*		

	1	Is your protocol written in such a way that it would be easy for other protocols to be developed on top of it or to interact with it?		
	2	Does your protocol impact permissionless innovation (see Section 6.2.1 ("Connectivity") above)?		
6.2.19	**Outcome Transparency**	*Freedom of expression, Privacy, Freedom of assembly and association, Access to information*		
	1	Are the effects of your protocol fully and easily comprehensible, including with respect to unintended consequences of protocol choices?		