

Your response

Question	Your response
Question 3c: What are some possible models for providing researchers with access to relevant information that may not exist or be widely used yet, but which might be implemented by industry?	<p>Confidential? – N</p> <p>Very useful source document with an outline of how a governance model for access to online services industry and the relevant data from Royal Holloway Unit is here https://osf.io/preprints/socarxiv/7pcjd</p>
Question 3d: What are the advantages and disadvantages of this approach? <ul style="list-style-type: none"> • These may include elements pertaining to financial, legal, security, technical or feasibility issues 	<p>Confidential? – Y / N</p>
Question 3e: What role could third party organisations, such as regulatory bodies, civil society or public sector organisations have in facilitating researcher access to online safety information?	<p>Confidential? – Y / N</p>
Question 3f: What could these third-party models look like, and what are some of the benefits and	<p>Confidential? – Y / N</p>

Question	Your response
challenges associated with this approach?	
Question 3e: What categories of information should online service providers give researchers access for the study of online safety matters? Why would this information be valuable for the study of online safety matters?	<p>Confidential? – N</p> <p>This could be divided into more and less easily accessible data.</p> <p>Categories of information that would be</p> <ol style="list-style-type: none"> (1) Meta data, so information on their accounts. So handle, location, profession etc., when they were opened, how long they have been a member. Any information provided on their profiles and location. Also in this category you could include any public content they have been exposed to, particularly ads and sponsored content from third parties. (2) Beyond this a second category could include any content from users feeds, so their posts, reposts/retweets, likes, follows, mentions, reactions to content, who they follow. Essentially this would include any individual level 'spoken' or user generated social media content (3) A category for 'heard' third party content could then be produced at the individual level this would include i.e. content from the accounts and people they follow or like and also sponsored ads. This would be possibly the most valuable for studying exposure to online content and questions of online safety. (4) A final category of aggregated data that would be the least sensitive, this would essentially be a corpus of tweets #, or posts, or urls, relating to a particular time point or event that were shared online. There would be no individually identifying information included.