Your response

Volume 2: The causes and impacts of online harm

Ofcom's Register of Risks

Question 1:
i) Do you have any comments on Ofcom's assessment of the causes and impacts of online harms?

Response:

Encryption

One of EFF's most important values is defending users' rights to have a free and private conversation. The best way to protect this basic human right in the online world, with end-to-end encryption.

We are pleased to see that at a few points in OFCOM's newest statements, OFCOM states the the Online Safety Act will not apply to end-to-end encrypted messages. For instance, in "Consultation at a glance," OFCOM states that "Automated Content Moderation" techniques may be mandated, including "hash matching," which should be applied to both large and small services. In footnotes A and B (page 7), OFCOM then states that "Measure does not apply to private communications or end-to-end encrypted communications."

We agree with OFCOM's apparent decision to not mandate or encourage scanning of any encrypted communications, since this would constitute a "backdoor" method of reading private user data. Encryption backdoors of any kind are incompatible with privacy and human rights.

However, there are places in OFCOM's documentation where this commitment can and should be more clear. For example:

The commitment to not violate user's rights to use and benefit from encryption must be kept regardless of the size and type of the online service. The commitment to not scan encrypted data must be firm, regardless of the size of the service, or what encrypted services it provides. For instance, in footnotes OFCOM suggests "file-storage and file-sharing" may be subject to a different risk profile for mandating scanning. But encrypted "communications" are not significantly different from encrypted "file-storage and file-sharing." Online communication systems routinely store and share files. Their core underlying mechanism is equivalent to file sharing.

There are other places where OFCOM should clarify that techniques to avoid or break encryption, including client-side scanning, must not be used. For instance, Annex 7 describes requirements for hash-matching with regards to detecting CSAM. This Annex should state explicitly that hash-matching techniques should not be applied to encrypted data (including client-side scanning techniques that scan data before or after the encryption algorithm is applied).

Annex 9, which discusses the difference between "private" and "public" data, barely mentions encryption. Annex 9 discusses encryption at only one point, mentioning it as merely one 'restriction' or 'friction' on viewing data that does not definitively render the data private. This is incorrect; encrypted data must be treated as private per se.

In this context, OFCOM should take note of the recent judgment by the European Court of Human Rights in PODCHASOV v. RUSSIA (Application no. 33696/19). The Court [at 76-77] emphasized that "Technical solutions for securing and protecting the privacy of electronic communications, including measures for encryption, contribute to ensuring the enjoyment of other fundamental rights, such as freedom of expression," whereas weakening of it can lead to "general and indiscriminate surveillance of personal communications [..] for all users." Such weakening is a disproportionate measure and violates the right to private life under Article 8 of the Convention.

Anonymity and Pseudonymity

Regarding Ofcom's assessment of pseudonymity and anonymity: There is ample evidence that pseudonymity is essential toward protecting certain vulnerable groups; that forcing real names can increase discrimination; and that 'stable pseudonyms' can create a more civil online environment for users. There is minimal evidence to suggest that anonymity and pseudonymity can in some cases embolden harassers, but that does not justify the overriding negative assessment.

Finally, we feel that it is important for Ofcom to continue consultations with civil society groups and human rights defenders for the overall assessment of platforms' behaviour. Their invaluable contributions can help guide Ofcom's enforcement actions.

ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response:	

The following citations provide evidence of the importance of anonymity and pseudonymity in protecting certain classes of users as well evidence that certain types of pseudonymity can provide a safer environment for users overall.

- Stable pseudonyms have been found to create a more civil online environment than real user names: Online anonymity: study found 'stable pseudonyms' created a more civil environment than real user names
- This paper analyses the role of anonymity in harassment: (PDF) Ethics for Cyborgs: On Real Harassment in an "Unreal" Place | Katherine Cross - Academia.edu
- This paper addresses anonymity in the context of online evidence: The Adobe Content Authenticity Initiative approach to authenticity infrastructure against media manipulation - WITNESS Blog
- This short article (with numerous citations) stresses the importance of anonymity or pseudonymity for various user groups: The Real Name Fallacy - Coral by Vox Media
- This article on "alt" accounts stresses that identity is multitudinous and underscores the importance of alternative identities for certain users: Alts and Automediality: Compartmentalising the Self through Multiple Social Media Profiles | M/C Journal
- This article looks at a non-normative identities and how social media platform parameters for names can be exclusionary: Constructing and enforcing authentic identity online: Facebook, real names, and non-normative identities
- This article looks at alternative models for internet trustworthiness: Karen Frost-Arnold, Trustworthiness and truth: The epistemic pitfalls of internet accountability - PhilArchive

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

No.

Question 2:	
i)	Do you have any views about our interpretation of the links between risk factors and different kinds of illegal harm? Please provide evidence to support your answer.

Response:

ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

Volume 3: How should services assess the risk of online harms?

Governance and accountability

Question 3:	
i)	Do you agree with our proposals in relation to governance and accountability measures in the illegal content Codes of Practice?
Response:	
ii)	Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 4:	
i)	Do you agree with the types of services that we propose the governance and accountability measures should apply to?
Response:	
ii)	Please explain your answer.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 5:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to requiring services to have measures to mitigate and manage illegal content risks audited by an independent third-party?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 6:	
i)	Are you aware of any additional evidence of the efficacy, costs and risks associated with a potential future measure to tie remuneration for senior managers to positive online safety outcomes?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Service's risk assessment

Question 7:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Specifically, we would also appreciate evidence from regulated services on the following:

Question 8:	
i)	Do you think the four-step risk assessment process and the Risk Profiles are useful models to help services navigate and comply with their wider obligations under the Act?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 9:	
i)	Are the Risk Profiles sufficiently clear?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Do you think the information provided on risk factors will help you understand the risks on your service?
Response:	
iv)	Please provide the underlying arguments and evidence that support your views.
Response:	
v)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Record keeping and review guidance

Question 10:	
i)	Do you have any comments on our draft record keeping and review guidance?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 11:	
i)	Do you agree with our proposal not to exercise our power to exempt specified descriptions of services from the record keeping and review duty for the moment?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Volume 4: What should services do to mitigate the risk of online harms

Our approach to the Illegal content Codes of Practice

Question 12:	
i)	Do you have any comments on our overarching approach to developing our illegal content Codes of Practice?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 13:	
i)	Do you agree that in general we should apply the most onerous measures in our Codes only to services which are large and/or medium or high risk?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 14:	
i)	Do you agree with our definition of large services?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 15:	
i)	Do you agree with our definition of multi-risk services?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 16:	
i)	Do you have any comments on the draft Codes of Practice themselves?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 17:	
i)	Do you have any comments on the costs assumptions set out in Annex 14, which we used for calculating the costs of various measures?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Content moderation (User to User)

Question 18:	
i)	Do you agree with our proposals?
Response:	

The incentivization of “swift” removal of content is likely to lead to over removal. In cases where time-related pressure is placed on moderators to make determinations, companies have little incentive to err on the side of free expression, and great pressure to remove more than necessary or appropriate. Assessing error rates is difficult from an external perspective. However, studies suggest a negative correlation between decision quality and rapidity.

Furthermore, time-based requirements incentivize platforms toward using automated technologies for content removal and upload filters, which are notoriously inaccurate and

prone to overblocking legitimate material. Ofcom should consider that such mechanisms constitute an interference with users' freedom of expression rights.

We agree with Ofcom's assessment that internal rules, standards and guidelines should be made clear to moderators; however, it is also imperative that internal standards be consistent with external standards made available to users.

As stated in the voluntary Santa Clara Principles on Transparency and Accountability in Content Moderation, "Companies should publish clear and precise rules and policies relating to when action will be taken with respect to users' content or accounts, in an easily accessible and central location."

We agree that moderators should receive ample training and materials to moderate content effectively and would also like to stress the importance, laid out in the Santa Clara Principles, of cultural competence of moderators.

Note that the Santa Clara Principles include standards for transparency around content moderation processes but are expressly not to be mandated by any government. The Santa Clara Principles specifically state, "This second iteration of the Santa Clara Principles has been developed to support companies to comply with their responsibilities to respect human rights and enhance their accountability, and to assist human rights advocates in their work. They are not designed to provide a template for regulation." In a Note to Regulators, the Principles explain that its standards do not readily scale or account for the variations among online services:

"The Santa Clara Principles seeks to set standards. Some services will appropriately meet these standards. Some will appropriately meet only some of them, while others will and should exceed them. Where any particular service falls will depend on many factors—number of users, capitalization, age, focus of service, editorial priorities, user priorities—that will vary from service to service. While companies should design their services with due process in mind from the beginning, companies must have some flexibility as to how they implement the Santa Clara Principles, from their inception, and then evolving over time as the service matures. The Santa Clara Principles are thus best seen as touchstones against which any company's practices can be evaluated and compared, not as dictates.

To maintain this necessary flexibility, governments should resist legal mandates that would be prohibitively expensive or practically impossible to meet. Such mandates discourage new entrants into the field and thus discourage innovation and competition. Even

among well-established services, there are no metrics that readily correspond to a required level of compliance.

The Principles also discuss other obstacles to employing them as governmental mandates: the potential for political exploitation, the variation among regional and national legal systems that govern these inherently international services, and the constantly evolving landscape of available services."

Our 2021 global call for inputs found cultural competence to be the most consistently addressed need in content moderation. Those we consulted stressed, for example, the importance of platforms disclosing how many moderators are working in a given jurisdiction or cultural context; what languages they operate in; as well as other diversity indicators.

Additional research has demonstrated that platforms often lack cultural and linguistic competence in content moderation; it is therefore imperative that they address this both internally (hiring those with requisite expertise to address complex concerns) and externally (through civil society consultations).

ii) Please provide the underlying arguments and evidence that support your views.

Response:

The Santa Clara Principles on Transparency and Accountability Open Consultation report clearly indicates the need for cultural competence in content moderation: The Santa Clara Principles on Transparency and Accountability in Content Moderation

- This article explores the relationship between errors in content moderation decision-making and decision quality: Decision Quality and Errors in Content Moderation | IIC - International Review of Intellectual Property and Competition Law
- The rapid removal of content can make it more difficult to pursue criminal complaints: New School Speech Regulation as a Regulatory Strategy Against Hate Speech on Social Media: The Case of Germany's NetzDG by Rachel Griffin
- Article 19's research on the importance of cultural competence and the role of civil society in working with platforms: Content Moderation and Freedom of Expression: Bridging the Gap between Social Media and Local Civil Society
- Some examples which underscore the importance of cultural competence in content moderation:
    - Algorithmic misogynoir in content moderation practice
    - Inequalities and content moderation - De Gregorio - 2023 - Global Policy - Wiley Online Library

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Content moderation (Search)

Question 19:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Automated content moderation (User to User)

Question 20:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 21:	
i)	Do you have any comments on the draft guidance set out in Annex 9 regarding whether content is communicated 'publicly' or 'privately'?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Do you have any relevant evidence on:

Question 22:	
i)	Accuracy of perceptual hash matching and the costs of applying CSAM hash matching to smaller services;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 23:	
i)	Ability of services in scope of the CSAM hash matching measure to access hash databases/services, with respect to access criteria or requirements set by database and/or hash matching service providers;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 24:	
i)	Costs of applying our CSAM URL detection measure to smaller services, and the effectiveness of fuzzy matching for CSAM URL detection;;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 25:	
i)	Costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services;
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 26:	
i)	An effective application of hash matching and/or URL detection for terrorism content, including how such measures could address concerns around 'context' and freedom of expression, and any information you have on the costs and efficacy of applying hash matching and URL detection for terrorism content to a range of services.

Response:

Our primary concern with respect to hash matching for terrorism content is the lack of transparency and oversight present in existing models, such as the GIFCT. Without clarity as to what content is being submitted to such databases, it is impossible to assess the impact on freedom of expression. We know that the moderation of terrorism-related content is prone to error; therefore, it is imperative that any efforts such as hash matching or URL detection be provided with expert oversight. Moreover, the hash-matching service offered by GIFCT, for example, is designed to assist individual determination by sites, not to be the final determination of either illegal or standards-violating images. But although large and well-resourced sites may do such individual assessments, the smaller services (which still serve perhaps millions of users) are more likely to simply depublish all hashed images.

ii)	Please provide the underlying arguments and evidence that support your views.

Response:

There are numerous examples of errors suggesting the need for oversight:

- CDT's Comments to Facebook Oversight Board on Case Regarding the Use of 'Media Matching Bank' in the Takedown of a Colombian Police Cartoon - Center for Democracy and Technology
- The Rise of Content Cartels | Knight First Amendment Institute
- Platforms Want Centralized Censorship. That Should Scare You | WIRED
- The moderation of extremist content is prone to error, causing real-world harm – Verfassungsblog

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

No.

Automated content moderation (Search)

Question 27:	
i)	Do you agree with our proposals?

Response:

ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

User reporting and complaints (U2U and search)

Question 28:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Terms of service and Publicly Available Statements

Question 29:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 30:	
i)	Do you have any evidence, in particular on the use of prompts, to guide further work in this area?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Default settings and user support for child users (U2U)

Question 31:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 32:	
i)	Are there functionalities outside of the ones listed in our proposals, that should explicitly inform users around changing default settings?
Response:	

ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 33:	
i)	Are there other points within the user journey where under 18s should be informed of the risk of illegal content?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Recommender system testing (U2U)

Question 34:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 35:	
i)	What evaluation methods might be suitable for smaller services that do not have the capacity to perform on-platform testing?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

We are aware of design features and parameters that can be used in recommender system to minimise the distribution of illegal content, e.g. ensuring content/network balance and low/neutral weightings on content labelled as sensitive.

Question 36:	
i)	Are you aware of any other design parameters and choices that are proven to improve user safety?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)

Response:

Enhanced user control (U2U)

Question 37:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 38:	
i)	Do you think the first two proposed measures should include requirements for how these controls are made known to users?
Response: EFF supports users having greater control over what content they see and interact with. While we do not support enforcing this as law, we believe that users should be equipped with knowledge about how various controls operate and how they can use them to their advantage.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Question 39:	
i)	Do you think there are situations where the labelling of accounts through voluntary verification schemes has particular value or risks?
Response: Voluntary verification can serve as a useful tool for users to make determinations about what to trust or interact with; however, it is important that platforms make clear to users the parameters used in determining which accounts to verify.	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

User access to services (U2U)

Question 40:	
i)	Do you agree with our proposals?
Response:	
The "reasonable grounds" standard is insufficiently demanding and will surely result in false labelling of terrorist affiliation and resulting state-mandated censorship. International human rights standards require a level of certainty in order to justify suspension of an account or removal of a post on such grounds. Implementation of the standard must be accompanied by strong protections against false positives, such as robust internal review and prompt appeal processes.	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
The following reports and papers provide evidence of the above: • Caught in the Net: The Impact of "Extremist" Speech Regulations on Human Rights Content | Electronic Frontier Foundation • Bad Speech, Good Evidence: Content Moderation in the Context of Open-Source Investigations • Regulating terrorist content on social media: automation and the rule of law | International Journal of Law in Context | Cambridge Core	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: No.	

Do you have any supporting information and evidence to inform any recommendations we may make on blocking sharers of CSAM content? Specifically:

Question 41:	
i)	What are the options available to block and prevent a user from returning to a service (e.g. blocking by username, email or IP address, or a combination of factors)?
Response:	
ii)	What are the advantages and disadvantages of the different options, including any potential impact on other users?
Response:	

iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 42:	
i)	How long should a user be blocked for sharing known CSAM, and should the period vary depending on the nature of the offence committed?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

There is a risk that lawful content is erroneously classified as CSAM by automated systems, which may impact on the rights of law-abiding users.

Question 43:	
i)	What steps can services take to manage this risk? For example, are there alternative options to immediate blocking (such as a strikes system) that might help mitigate some of the risks and impacts on user rights?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Service design and user support (Search)

Question 44:	
i)	Do you agree with our proposals?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Cumulative Assessment

Question 45:	
i)	Do you agree that the overall burden of our measures on low risk small and micro businesses is proportionate?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 46:	
i)	Do you agree that the overall burden is proportionate for those small and micro businesses that find they have significant risks of illegal content and for whom we propose to recommend more measures?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 47:	
i)	We are applying more measures to large services. Do you agree that the overall burden on large services proportionate?
Response:	

ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Statutory Tests

Question 48:	
i)	Do you agree that Ofcom's proposed recommendations for the Codes are appropriate in the light of the matters to which Ofcom must have regard?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Volume 5: How to judge whether content is illegal or not?

The Illegal Content Judgements Guidance (ICJG)

Question 49:	
i)	Do you agree with our proposals, including the detail of the drafting?
Response:	
ii)	What are the underlying arguments and evidence that inform your view?
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 50:	
i)	Do you consider the guidance to be sufficiently accessible, particularly for services with limited access to legal expertise?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Question 51:	
i)	What do you think of our assessment of what information is reasonably available and relevant to illegal content judgements?
Response:	
ii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Volume 6: Information gathering and enforcement powers, and approach to supervision.

Information powers

Question 52:	
i)	Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Annex 13: Impact Assessments

Question 54:	
i)	Do you agree that our proposals as set out in Chapter 16 (reporting and complaints), and Chapter 10 and Annex 6 (record keeping) are likely to have positive, or more positive impacts on opportunities to use Welsh and treating Welsh no less favourably than English?
Response:	
ii)	If you disagree, please explain why, including how you consider these proposals could be revised to have positive effects or more positive effects, or no adverse effects or fewer adverse effects on opportunities to use Welsh and treating Welsh no less favourably than English.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	