Proton AG
Route de la Galaise 32, 5th floor
Plan-les-Ouates, 1228-Geneva, Switzerland

February 2024

Proton response to the Ofcom consultation on Protecting people from illegal harms online

Proton AG ('Proton') is one of the fastest growing consumer and business communications and collaboration companies in Europe. Proton provides an encrypted services ecosystem that enables everyone to have full control over their online information. It was founded in 2014 by scientists who met at European Organization for Nuclear Research (CERN). Since then, it has grown at a fast pace and now has more than 100 million sign ups. In addition to protecting millions of individuals, Proton also secures tens of thousands of businesses, including many of the world's largest public and private organizations.

Our principal product, Proton Mail, is the world's largest secure email service. The U2U service operated by Proton which falls under the scope of the Online Safety Act is Proton Drive, an end-to-end encrypted (E2EE) file-hosting and file-sharing service. We also offer other products such as encrypted calendar, Proton Calendar, VPN service Proton VPN and password manager, Proton Pass.

Proton welcomes the opportunity to provide feedback to Ofcom's proposals in relation to the Online Safety Act (OSA). We acknowledge the regulator's efforts to explain its thinking behind the proposals and make them as accessible as possible. However, we want to emphasize how challenging it is for a company the size of Proton – and by extension for other small and medium sized companies – to be able to read through the full guidance given its length and complexity. Despite all details provided, a certain degree of uncertainty remains for us around a number of issues.

We have responded to the consultation via this paper rather than via the form provided to have more flexibility to raise these doubts and questions. To ensure that it remains informative, we will structure our contribution based on the different volumes made available by Ofcom.

Proton AG
Route de la Galaise 32, 5th floor
Plan-les-Ouates, 1228-Geneva, Switzerland

Proton, end-to-end-encryption and online safety – Vol. 2

Firstly, we want to emphasise that our intent with this contribution is not to discuss or negate the harms identified by Ofcom and the British legislator in the Online Safety Act and its guidance, but rather to share our vision of online safety and explain how some of the requirements outlined in the guidance documents could impact our services and the way we operate them.

For Proton, privacy goes hand in hand with online safety. Making sure our users are safe is the most important part of our mission, and we are fully committed to it. For this reason, we would strongly nuance the statement in volume 2 claiming that "*services which focus on and emphasize growth may deprioritise safety measures".* Many services built in the UK and in Europe today prioritise privacy and safety over revenue, while still having the ambition to grow. Small and medium sized tech companies certainly may not have the same resources as tech giants, but their business model will often be less harmful to society and require different measures to be put in place. For instance, at Proton, 10% of employees work on anti-abuse measures, a significant number for a company of our size (around 400 people). Safety is not something we compromise on. Our terms and conditions already feature a comprehensive list of the unauthorised uses of our services[1], and we actively enforce these T&Cs when they are breached, through removing accounts for example. To be clear, while E2EE provides privacy to users, ensuring their data cannot be read by anyone – including Proton – there are a number of measures we take to actively protect our services from being misused, and we do our utmost to protect our users and society overall.

For this reason, we find it particularly unfair for "low capacity" and "early-stage services" to be stigmatised and be considered more at risk. This will make them face an additional compliance burden, at a time where they mostly need guidance and would benefit from a discussion with Ofcom on the best practices to adopt. We believe that a much stronger focus should be put on the business model of the companies – which can undoubtably contribute to attracting illegal and harmful content – rather than on a factor no business can fully control: being an early-stage service or having a fast-growing user base.

---

[1] https://proton.me/legal/terms. Additionally, we believe that it is important not to include too many details on our anti-abuse practices in our T&Cs to avoid abusers from guessing and bypassing these. We trust Ofcom will be sensible to the need for online services to make sure their measures are not being undermined by excessive transparency requirements.

End-to-end encryption as a major harm factor on a service – Vol. 2

Unfortunately, E2EE is often portrayed as a threat to security and a hindrance to online safety, ignoring the crucial benefits it already brings to our societies. At Proton, we sincerely believe that E2EE not only preserves people privacy, but that it also secures businesses' trade secrets, protects critical financial infrastructure and enhances the resilience of our democracies in times of active cyberwarfare. To say it bluntly, if E2EE was to become inoperant today, the internet as we know it would almost immediately stop working.

But as E2EE brings an extra layer of protection online, it is true to say that this protection applies to all actors, the legitimate and the bad ones. While we are glad to see that Ofcom realises the benefits brought by E2EE and even acknowledges that *"the role of the new online safety regulations is not to restrict or prohibit the use of such functionalities"*, we are strongly disappointed by the links made in the paper between E2EE and risk. E2EE is presented throughout this volume as posing particularly serious risks, and as a major factor to consider when building the risk profile of a service. To support this narrative, many sources quoted in footnote come from organisations and administrations that are notoriously hostile to E2EE, while academic publications and works from cryptography researchers appear to be largely under-represented. Encryption is listed as a risk factor for twelve offences in volume 2, which means that encrypted services will have to focus their efforts not only on terrorist content and CSAM but on many other issues. As we highlighted above, we do not see E2EE as a risk or as a liability in and of itself. We even argue that E2EE should be considered as a positive factor in the fight against some offences listed, such as foreign interference. But the positive aspects of E2EE are not at all considered in this volume, placing a de facto obstacle on companies who wish to offer E2EE to their users.

Risk and E2EE: the OSA could undermine online safety – Vol. 3

In practice, while Ofcom does not "*restrict or prohibit the use of*" E2EE, it strongly discourages it. When deciding to develop a specific service, any company will realise that offering E2EE will subject it to much more stringent requirements under the Act. An E2EE service will automatically fall into the "multi-risk" category, imposing very

burdensome requirements on the service provider, often equivalent to measures large services would have to put in place. If no changes are made to the guidance documents, the OSA will heavily disincentivise companies from providing any form of encryption on their services. While the regulator could see it as a win for content moderation purposes, these services would be much more vulnerable to other external threats, ultimately undermining their users' safety.

Services in scope: the risk approach should be clarified – Vol. 4

We welcome Ofcom's willingness to come up with a flexible and a differentiated approach between small and large services on one side, and between the different levels of risk on the other. While we acknowledge that there is no silver bullet that can fit all the different U2U services, we have some remarks on the approach chosen by Ofcom as it currently stands.

In order to define large services, the focus is put on the number of monthly UK users – 7 million at least in this specific case. However, in the proposals provided we did not encounter any definition of 'user' or methodology to count them.

Our service that is concretely in scope for the Act, Proton Drive, is classified as a file storage and file sharing service. There are a number of different ways in which we could count users of this service. Should we count as a UK-based user someone who has a Proton account for another part of the ecosystem, even if they do not use Proton Drive? Does this refer only to those who upload and download files and have a Proton account? Shall we also take into account non-Proton users who interact with the service, even if they only read a file shared via a link? In all these cases, there would be potential issues. To add to this, we do not know precisely where our users live, even less where people accessing links live. Attempting to obtain such information would require us to collect much more data than we currently do, and put at risk the privacy and security of those whose data we are collecting. Privacy-invasive services would be in a better position to comply than privacy-preserving ones – thus putting companies with more dangerous business models for the society in an advantageous position to comply with the requirements of the OSA.

There is a similar issue on the specific measures for file storage and file sharing services that have more than 70,000 monthly UK users. Applying stringent measures to services used by only 0.1% of the UK population lacks any form of proportionality in our opinion. And as counting UK users will be very difficult and imprecise, many small services will not be able to know whether they have more of less than 70,000 monthly users.

We were also surprised by the division in different risk levels for each service, and the three-tiered approach adopted. While a division between low risk, specific risk and multi-risk seems sensible, labelling a service "multi-risk" only when two different kinds of harms are identified as medium or high risk is excessive. Reading Annex 3, it is clear that if this classification was to be retained in the final proposals, the vast majority of U2U services in scope of the OSA would be considered "multi-risk".

According to table 7 in Annex 5, Proton Drive is automatically considered to be "high risk" for image based CSAM. We find such a classification to be unfair and disproportionate, as it does not take into account the potential measures taken by the service to mitigate harm, its number of users nor any past records of misuse. It does not seem reasonable for a service which already has measures in place against CSAM to face the same burden as a service which wouldn't.

While we are aware that the tables mentioned do not compile strict and definitive criteria but only constitute guidance, we still find it important to have some clarity, as smaller services will often choose to err on the side of caution and follow Ofcom's guidance to the letter to make sure they are compliant with the OSA.

Automated content moderation and E2EE – where do file storage and file-sharing stand? – Vol. 4

Following all the controversies surrounding automated content moderation and E2EE during the legislative debates around the Online Safety Bill, we are extremely pleased to see that Ofcom recognises that "*end-to-end encrypted services are currently unable to analyse user-generated content in the ways set-out in our proposals*". It is indeed impossible for Proton to look at the content of, for example an email sent with Proton Mail.

In the proposals, a lot of references are made to the impossibility to apply hash-matching technology in E2EE private messaging, and Ofcom makes clear that "*privacy communications or end-to-end encrypted communications do not have to implement such technologies*". However, we would welcome more clarity on where things stand with regards to our file storage and file-sharing service, Proton Drive. Proton's file-storage and sharing service is also end-to-end encrypted, meaning that Proton cannot access the content of what is being stored on it. Similarly to what happens on E2EE messaging services like WhatsApp, Proton is unable to scan files hosted on Proton Drive. A clear reference stating that no E2EE service is expected to put in place hash matching would solve this issue.

Finally, we wanted to close this contribution with some general remarks on hash matching. While our E2EE services are not expected to put this technology in place, we have on several occasions voiced our concerns[2] on its prescription to all U2U services at risk of CSAM and/or grooming. Hash matching can still lead to many false positive (or false negatives), and beyond its financial cost for smaller services, it is also not easy to implement as each service has its own specificities. Additionally, maintaining a functioning hash matching technology on a service is difficult and does not come without strong privacy and security risks. There is not technological silver bullet unfortunately, and we strongly believe that the focus should be on making sure that law enforcement has the means to rescue children in real life, as hash matching will only come into play once some harm has been done to children.

***

Ofcom's proposals represent a significant step in implementing the complex piece of legislation that is the Online Safety Act. Ofcom's efforts to make its proposals as easy to read and understand as possible are welcomed and appreciated. We believe that if our remarks above were to be addressed, it would be much easier for Proton to implement the Act in a sustainable manner. At this stage, the proposals risk creating a very important administrative burden for scale-ups like ours, while doing little to foster online safety. The burden should be borne mostly by those services whose business models harm children in real life, rather than on services which are designed on purpose to protect their users. We thank Ofcom for giving us the opportunity to contribute to this consultation on we hope to be able to keep on discussing these topics moving forward.

[2] https://proton.me/blog/online-safety-act-hash-scanning