February 2024

Element's response to the Ofcom consultation on protecting people from illegal harms online

Element is an encrypted messaging startup founded in the UK, which employs over 80 people, and develops solutions based on an open standard for secure communications called Matrix. We develop a secure and interoperable communication platform for customers ranging from governments (including the UK Ministry of Defence, the German Bundeswehr, the UN, the US Navy and Marine Corps, NATO…), to large enterprises and individual consumers. We also provide the infrastructure and support for the Matrix.org Foundation's[1] free and publicly accessible Matrix server, which will fall under the scope of the Online Safety Act.

We welcome the opportunity to participate in the first major consultation related to the Online Safety Act. We appreciate the care and consideration taken to develop these proposals, although we would like to reiterate that it is extremely challenging for small and medium sized organisations, such as Element, to read, understand and comment on the full extent of the guidance. All efforts were made to understand all the complexity and nuance included in the full guidance. However, we would welcome more clarity in certain areas which we will detail below. To make better use of our limited resources we have responded to the consultation via this document as opposed to the form.

Although we broadly agree with Ofcom's assessment of the causes and impacts of online harms, we believe that there are some important considerations missing, particularly in relation to end-to-end encryption. We would like to make it

[1]About the Matrix protocol and the Matrix.org Foundation, 2024: https://matrix.org/about/

clear that we do not consider online safety, security, and privacy to be mutually exclusive. Presently we have a series of measures in place which allow for the active monitoring and protection of the users of our services, which do not require encryption to be compromised. We also note that in Volume 2 Ofcom identifies organisations at earlier stages as being of higher risk, due to the assumption that they would not prioritise the safety of their services. We at Element, as many other organisations in the UK and the EU, provide a service which focuses on privacy as well as safety. We have staff dedicated to Legal, Compliance and Trust & Safety issues who work hard at preventing our service from being misused. This generalisation unfairly singles out "early-stage services", whereas we would welcome a more in-depth consideration of the role of business models as a factor instead.

While there is mention of some of the important benefits of end-to-encryption, we believe that these benefits have not been considered holistically. For example, children in unsafe homes might be able to use end-to-end encrypted services to obtain support in a safe manner. Encryption benefits and protects everyone, including children. The assessment of E2EE as a standout risk is repeated through volume 2, with very little accompanying data and evidence to support these claims. We would also like to note that the sources cited in relation to E2EE were often not presented in a way that addressed both risks and benefits. For example, point 6B.46 of Volume 2 refers to a Tech Against Terrorism Paper[2] which details that terrorist actors prefer E2EE services as evidence of it being a standout risk factor. However, the same paper offers recommendations for both companies offering E2EE and law enforcement agencies to address this risk, without the use of backdoors or other forms of undermining encryption.

[2] Tech Against Terrorism, 2021. Terrorist use of E2EE: State of play, misconceptions, and mitigation strategies.

In addition, it is not clear what other measures might be recommended by Ofcom to address these harms at a root level. As Ofcom's assessment rightly mentions, online harms can affect people's lives offline. In this same vein, we also believe that real world approaches can prevent the escalation of harms to online spaces, where they can be amplified. It is also our view that whilst service providers have responsibilities in relation to the features they introduce, some consideration also needs to be taken in relation to the safeguarding roles of other institutions. Specifically, we would like to understand what guidance Ofcom will be providing to law enforcement, educators, parents and children on how to prevent some of these harms.

We have been very public[3] about our concerns related to the Act and its potential impacts on privacy and security. Encryption, particularly end-to-end encryption, is an essential technology that keeps everyone safe, including children, so we need to apply caution when proposing measures that could jeopardise it. Whilst we appreciate some of the safeguarding measures introduced by the Act, and how it limits the scope of Technology Notices which would require proactive detection technologies (e.g. client-side scanning) to be introduced to encrypted communications to the most egregious types of content, such as Child Sexual Exploitation and Abuse (CSEA) and terrorism, we are now surprised to see this scope potentially being widened by Ofcom's proposed guidance.

[3] Element blog, 2023: The Online Safety Bill: An attack on encryption. Element blog, 2023: The UK's Online Safety Bill undermines everyone's safety. Element blog, 2023: End-to-end encryption; the will of the British people.

Our view is that Ofcom's interpretation of end-to-end encryption as a functionality that "stands out as posing a particular risk" goes beyond the scope of the Online Safety Act. Section 121 of the Online Safety Act limits the scope of Technology Notices which may require encrypted services to screen messages in order to detect CSEA material. Ofcom's interpretation of the links between risk factors and illegal harms identifies end-to-end encryption as a risk factor for twelve categories of illegal content. If Ofcom's approach is implemented as defined in this consultation, the scope of monitoring and risk assessment considerations for encrypted services would increase considerably. We do not believe this to be in line with the principles of proportionality included in the safeguarding clauses of the Act.

In fact, it seems that this misalignment and potential contradiction has already been identified by Ofcom, as the guidance states that encryption increases risk levels, while also stating that technologies which analyse user-generated content in the ways set out in the proposal would materially compromise end-to-end encrypted services. Our interpretation of this statement would be that Technology Notices that would force providers of encrypted communications to introduce measures such as content scanning would not be possible. Unfortunately, undermining encryption is a binary choice: with or without legal safeguarding, once code exists to allow for (legally approved) backdoor access to communication, that code provides a way for bad actors to hack in and access the communication too - by impersonating authorities, or changing scanning rulesets, or by exploiting bugs in the scanning code, and so on. We would welcome clarification on this section of the guidance.

There is a contradiction in the guidance between statements in Volume 4 14 and Annex 9. The introduction to section 14 states "These proposals only apply in

relation to content communicated publicly on U2U services, where it is technically feasible to implement them. Consistent with the restrictions in the Act, they do not apply to private communications or end-to-end encrypted communications. In Annex 9 to this consultation, we have set out draft guidance which is intended to assist services in deciding whether content has been communicated “publicly” or “privately” for this purpose.” In Annex 9, it is suggested that there are circumstances where end-to-end encrypted communications should be considered public, and fall under the proposals for services in 14.97 onwards. For services with a mix of end-to-end encrypted content and public content, we believe that the proposals in 14 could apply to public content, and would be a balanced approach to reducing public harms while protecting private rights.

In addition, Annex 9 details Ofcom’s guidance on whether content is communicated ‘publicly’ or ‘privately’. We would like to seek further clarification on how A9.12 would apply to services where end-to-end encryption is present by default. Given that A9.15 and A9.16 reiterate the focus of the distinction between public and private communications to be around the communication of content, can we infer that the use of end-to-end encrypted services would always signal intent for private communications? Considering all three factors from Section 232(2) of the Act, we would like to seek clarification on the ways in which encryption could impact the first two factors, namely:

- The number of individuals accessing the content would be limited by restrictions, such as requirements for accounts and encryption key sharing. In technical terms, even communications between large groups would be private due to the use of encryption. However, in social terms, the larger the group, the lower would be the expectation of privacy. Is this the same logic applied by

Ofcom in this distinction? If so, how does Ofcom determine the threshold at which communications move from being private to public?

- Does the fact that content communicated via encrypted services require an account to be accessed (as opposed to content available on the open Web) count as a blanket restriction on who may access content?

Both the Act and the proposals in the consultation are missing consideration of the complexities for decentralised systems, where content is hosted by a range of servers. We would welcome engagement from Ofcom on how to address this gap in the proposals. Annex 15.27 is one area where this is particularly glaring.

Finally, we would like to reiterate the potential impact of the administrative requirements of the Online Safety Act and accompanying guidance. We appreciate the efforts by Ofcom to make the proposals accessible, particularly via the series of webinars on this topic. However we would be remiss if we did not highlight the impact this sort of administrative requirement could have on an organisation our size. We believe a safer digital environment is possible and want to do our part to contribute to it, but as it stands we fear the Act will disproportionately impact companies like ours which focus on privacy and security, as opposed to those who use more invasive business practices and models.

We thank Ofcom again for the opportunity to participate in this consultation and hope you consider our views in this matter. We remain ready for further discussions related to this issue.