DRCF roundtable on end-to-end encryption

Hosted by the FCA, the ICO and Ofcom: Summary report

1. INTRODUCTION

The Digital Regulation Cooperation Forum's (DRCF) plan of work for 2021 to 2022 identified end-to-end encryption (E2EE) as a key technology. It has implications for policy objectives relevant to the current and future remits of DRCF members. The workplan committed to bringing together a range of perspectives on E2EE and identifying priority areas for future joint work.

On 27 January 2022, Ofcom, the ICO and the FCA held an E2EE roundtable. The event brought together voices from the digital technology industry, academia, civil society and the legal profession to help guide future joint regulatory work. The objectives were to understand:

- the benefits and risks of E2EE for online services and their users; and
- its implications for digital regulation.

This report provides a summary of that roundtable. The views that this report expresses are those of the roundtable participants rather than the DRCF member regulators. **This report does not intend to set out regulatory policy proposals. It simply aims to capture the views expressed by participants during the roundtable discussions.**

2. KEY THEMES

Participants said that regulators coming together jointly to discuss E2EE was a crucial step. Regulators may have different starting points and objectives in regulating E2EE services and online safety technology. However, establishing mutually-shared fundamental values allows DRCF members to navigate the challenges and adopt a coherent regulatory approach. A co-ordinated approach is also important, to guard against any unintended consequences of regulatory interventions.

We discussed the following key themes:

The importance of establishing common terminology regarding E2EE for the DRCF member regulators.

- A range of perspectives exist on what constitutes E2EE, depending on what aspects of the service are encrypted. By using a common terminology around E2EE, regulators will be able to articulate their expectations more clearly regarding different E2EE services.

The need to avoid a 'one size fits all' approach to countering illegal activity on E2EE services.

- Regulators need to differentiate between specific threats or harms (eg child sexual exploitation and abuse, sharing of terrorist content). They also need to articulate the desired outcomes (eg in relation to safety, security, privacy) in each area. Participants noted that issues such as the reliability and accuracy of technological solutions can only fully be assessed in the context of their application to counter specific threats.

The importance of considering a broad range of measures to address concerns about safety in E2EE environments, not just technological remedies.

- The existence of technological, social and legal challenges means that technological remedies can never provide a comprehensive solution to ensuring safety in an E2EE environment. Businesses and regulators should not overlook other approaches, such as incorporating user safety into the design and development of E2EE services.

The benefits of regulators providing industry with more clarity about their expectations (eg about privacy, safety and security).

- This provides certainty and could incentivise innovators to develop online safety measures.

The need for engagement with the public on technological measures intended to counter threats on E2EE services.

- The public may be hesitant to accept technical solutions that they perceive as intruding upon private communications. Effective communication from both industry and regulators about privacy safeguards is crucial for the success of any technological measures.

The importance of a principles-based, outcomes-focused regulatory approach.

- Regulators should adopt an approach focused on the principles and outcomes that technological solutions could deliver, rather than mandating specific technologies. This allows industry to innovate.

The need to foster innovation to tackle the threats and harms found on E2EE services.

- When fostering innovation, it is crucial to provide clarity about the problems that innovation should solve and the principles that organisations need to respect when doing so.

- Participants welcomed the DRCF's cross-regulatory approach. Regulators should consider providing safe spaces to develop innovative solutions across multiple regulatory remits.

3. SUMMARY OF ROUNDTABLE DISCUSSION

3.1. Current capabilities to tackle illegal activity within E2EE services

DRCF members began the roundtable by asking attendees for their assessment of the current technical capabilities for addressing illegal activity within E2EE services. Participants told us that this question was too broad for a meaningful answer.

Attendees explained that to assess technological capabilities, regulators need to consider the specific use cases for measures intended to tackle illegal activity within E2EE services. They told us that factors such as reliability, accuracy, and privacy can only fully be assessed in the context of applying specific technological solutions to counter specific threats. We also heard views that there is an information gap about what "good looks like" for online safety solutions and that this uncertainty is hindering development of online safety measures.

There was a consensus that regulators and industry should set out and differentiate the specific threats and harms that they intend to address. They should also define the desired outcomes and the parameters of technological measures for each category. This modelling could help to provide clarity for businesses which, in turn, provides incentives for innovation.

Current level of technological capability

Attendees differed in their views about the current level of technological capability to identify illegal content in E2EE environments. Some believed that on-device technology currently in development will soon be able to provide meaningful interventions against illegal activity, such as child sexual exploitation and abuse (CSEA). Others maintained that client-side scanning technology is vulnerable to evasion attacks and is not currently robust enough to be deployed at scale.

We discussed technological interventions in terms of whether these weakened or compromised E2EE. We heard that, because there is no commonly agreed definition of E2EE, it is challenging to measure the level of privacy and security provided by E2EE and the privacy and security impact of any technological interventions. For example, some definitions of E2EE stipulate complete privacy between the individuals communicating at every stage of the information flow. Others accommodate intervention prior to encryption. This matters because it goes to the heart of debates about whether detection mechanisms weaken E2EE.

The majority view was that E2EE does not guarantee privacy in practice. For example, vulnerabilities may exist within E2EE systems that allow information to leak. Other concerns include:

- metadata being accessible;
- E2EE providers not always being secure; and
- third parties accessing devices.

Public engagement

We heard that it is important for both industry stakeholders and regulators to find a meaningful way to discuss the privacy impact of interventions and to effectively communicate this to the public. Gaining an understanding of the public's views on E2EE is key to this process.

We were also advised to bear in mind that, in general, the public do not understand E2EE. However, they understand that firms providing E2EE services offer private user communications, accessible only by the parties to the communication.

This has implications for public trust in on-device scanning technologies, which the public may perceive as intruding upon private devices and communications, regardless of whether companies have privacy-preserving measures in place. Participants noted that public perception of such technologies may pose a significant barrier to their take-up.

'Slippery slope' argument

The DRCF members asked the roundtable for views about concerns that have been expressed that, once organisations implement client-side scanning technology, it is inevitable that its scope will be expanded beyond detection of CSEA and terrorist material.

Some participants pointed out that other countries could choose to mandate deployment of scanning technology for different (and wider) types of content. This is likely to be a concern for service providers that operate globally. There was, however, no consensus in the discussion about the emphasis that UK regulators should place on this as a factor. Some participants advised that UK regulators should focus on upholding standards and safeguards for UK users. Others expressed concerns that relevant safeguards in UK law may not be replicated in other jurisdictions.

Alternatives to client-side scanning

Some attendees highlighted that a focus on scanning might detract from the development and use of more achievable and less intrusive alternatives to prevent harm. They said that these could have the potential to provide better outcomes. Suggestions of alternative measures for regulators to consider included the below:

- A safety-by-design approach to the development of E2EE services focused on preventing online services from being used for illegal activity.
- User controls that allow blocking or verifiable reporting within E2EE environments. We heard that it's less likely for attackers to target user controls. They may therefore be easier to develop and maintain than a scanning system.
- Flagging and removing accounts that violate platform standards or display potentially dangerous activity.
- The use of non-content signals, such as metadata, to identify and address suspicious behaviour and coordinated information networks.
- The potential for law enforcement to gain access to encrypted communications by accessing end-user devices.

3.2. Future developments in E2EE and technical capabilities to address illegal activity within E2EE services

We heard little concrete detail from attendees on future technological developments that might allow organisations to tackle illegal activity within E2EE environments. This suggests that either the capability of technology to effectively address illegal activity is not yet clear, or that obstacles to development may prevent organisations from pursuing viable or scalable solutions.

Technical challenges

Participants told us that tackling illegal online activity is something of an arms race between safety solutions and circumvention or disruption measures adopted by bad actors. This presents technological challenges to the development of robust and sustainable solutions.

Participants were unclear about the possibility of fully overcoming challenges such as false-positive and false-negative attacks or the risk of reverse-engineering. We also heard that client-side scanning technologies may risk handing an advantage to bad actors. It could give them access to the outputs of the scanning technologies, allowing them to test an image for matches against known CSEA images.

Another attendee advised that the accuracy of scanning must be extremely high. Otherwise, millions of legal, consensual images may be subject to human review on a daily basis. This could be a disproportionate approach that presents risks to privacy and personal data rights.

Other challenges

Some attendees advised that legal, political, and social concerns may present bigger obstacles than technical challenges to the take-up and successful deployment of technological solutions. The potential reluctance of the public to accept technology that could be perceived to be making their private device a tool for third parties is a problem without a technological remedy. It would require major political and regulatory collaboration to resolve.

Limits of technological measures

We were cautioned against thinking that there will be a technological 'magic bullet' that comprehensively addresses illegal activity on E2EE services.

As well as the concerns outlined above, there are challenges that mean that such solutions can never provide comprehensive protection. Measures such as content scanning might simply drive bad actors to alternative services.

Taken alongside other challenges such as admissibility requirements for evidence within different jurisdictions, and that technological measures only fit specific use cases, there was a view that there should be an acknowledgement of the limits of technological interventions in tackling illegal activity.

3.3. The role of regulators

We heard that DRCF member regulators must provide clarity about what E2EE means to them. This is so that regulators and online services can use a common language when discussing developments involving E2EE services.

In terms of regulatory approach, the majority opinion was that this should focus on principles and outcomes, rather than mandating specific technologies. Participants expressed the following views:

- Defining standards for scanning technologies would represent a challenge for regulators. Better outcomes could be achieved by setting desired outcomes and allowing companies to develop innovative solutions.
- If regulators overly focus on standards and frameworks for encryption and online safety technologies, breaking technologies designed to those standards would become a prime focus of bad actors.

- Mandating standards could also slow or stop the cycle of continuous development that organisations require to stay ahead of bad actors.

Participants suggested instead that regulators should establish clear expectations for the safety and privacy outcomes required of E2EE services. Regulators could consider setting standards for how they would assess safety technologies under their respective and joint remits. From the discussion, we inferred that clarity over expectation, combined with the ability to innovate safely, are key for future technological development.

Participants suggested that DRCF members could host a joint regulatory sandbox. This could stimulate innovation by providing a safe environment for innovators to develop measures to combat illegal activity, while ensuring regulatory compliance. One attendee added that, whilst a sandbox could facilitate the development of technology, it would remain crucial to be clear about the problem that the technology is intended to solve.

4. Next steps

Based on the stakeholders' views at the roundtable, the DRCF Plan of Work for 2022 to 2023 commits to developing a collective understanding of E2EE to inform a joined up regulatory approach. The DRCF identified two areas of work which, given the importance of E2EE to their remits, Ofcom and the ICO are going to take forward over the coming year:

Jointly agree a working terminology about E2EE

A range of perspectives exist on what constitutes E2EE, depending on what aspects of the service are encrypted. Ofcom and the ICO are going to therefore jointly agree on shared terminology to describe E2EE services to support informed discussion with stakeholders.

Conduct a landscape review

Ofcom and the ICO are going to conduct a landscape review, collaborating with stakeholders where appropriate. This aims to identify knowledge and policy gaps which future work could cover.

We thank the participants in the roundtable. Their contributions provide a valuable reference for all stakeholders working in this area and we look forward to continuing our engagement in the future.