A Framework for Analysing End to End Encryption in an Online Safety Context v1 02/11/2021.

Background

1. The ICO are often asked about end-to-end encryption (E2EE), this is a complex topic and to help people consider the issues we publish this paper setting out a framework for considering the impact of end-to-end encryption on online safety.

2. E2EE raises challenging questions for online safety which we continue to consider given the context in which we regulate the processing of personal data. It is important that any approach to E2EE seeks to reconcile addressing the immediate harms with longer term privacy and safety impacts.

3. The paper provides a summary of the Information Commissioner's Office's (ICO) current thinking to support the evolving discussion on governance of E2EE. It builds on our engagement with a range of national and international stakeholders to build up our own picture around E2EE as the UK's data protection regulator but does not necessarily represent our final settled policy position.

Introduction

4. E2EE is a technical measure that encrypts content in communications channels so that only the sender or recipient can access it. This approach prevents third parties, including the provider of the communications platform service, from accessing the content. It is increasingly used to support secure communications and content sharing between users.

5. Keeping their personal information secure matters to people. In our 2021 annual tracking research 77% of respondents said that protecting their personal information is essential[1]. Recent consumer shifts towards services with high encryption standards (for example the move to Signal and Telegram in response to WhatsApp terms and conditions changes) demonstrate how much the public value private and secure communication services[2].

6. Security is particularly important for children. In the 2020 joint research on Internet Users' Experience of Online Harms that we carried out with Ofcom, 16% of 12-15 years old's voiced unprompted

[1] Information Rights Strategic Plan: Trust and Confidence June 2021 (ico.org.uk)

[2] See for example Millions switch to Signal and Telegram amid WhatsApp privacy fears (telegraph.co.uk)

concerns about having their personal information stolen[3]. Stakeholders within the child advocacy space have told us that children need safety but they also need private spaces when they are online.

7. Systems that do not use E2EE can be abused, creating the risk for financial fraud, exposure to harmful content and other harms[4][5]. Real-life circumstances where the lack of E2EE has exposed people to harm include: children having their pictures accessed[6] or location tracked[7], access to medical data[8], collection of data for fraud[9] and misuse[10], and the acquisition of sensitive data as part of broader data collection processes[11].

8. E2EE is also crucial for businesses. It enables them to share information securely and fosters consumer confidence in digital services. The lack of E2EE has been shown as a critical vulnerability to validating data integrity[12,13,14]. The effect of weakening encryption has been assessed in a report commissioned by the Internet Society analysing the impact of the Australian Telecommunications *and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA).* The report concluded that TOLA has the potential to result in significant economic harm to the Australian economy, in part because of the likely indirect impact of customers and businesses losing trust in digital security[15].

9. From a data protection perspective, E2EE acts as a key enabler for compliance with the requirements of data protection law. It is directly relevant to the data protection principle of integrity and confidentiality which places a legal requirement on organisations to deploy measures to process personal data in a way that ensures security. More broadly, it underpins a key outcome of data protection law which is to give citizens confidence about how their personal data is processed by digital services, including confidence that it is stored and shared securely.

[3] Internet users' experience of potential online harms: summary of survey research (ofcom.org.uk)

[4] Fresh warnings over Royal Mail parcel scam - BBC News

[5] Number spoofing: meet the customers who lost thousands | Banks and building societies | The Guardian

[6] 'Pictures of children' 'in Vtech hack - BBC News

[7] EU Recalls Children's Smartwatch That Leaks Location Data | Threatpost

[8] Security and Privacy Investigation of Existing mHealth Applications (pitt.edu)

[9] International Hackers Indicted for Sniffing Credit Cards from Dave & Buster's | WIRED

[10] Download DroidSheep APK for Android (Latest Version)

[11] Google's Wi-Fi snoop nabbed passwords and emails • The Register

[12] Rogue Tor 'exit node' server added malware to legitimate downloads | PCWorld

[13] China's Great Cannon (citizenlab.ca)

[14] Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls | Electronic Frontier Foundation (eff.org)

[15] The Economic Impact of Laws that Weaken Encryption-EN.pdf (internetsociety.org). The research was carried out by Law and Economic Consulting Associates.

10. The ICO has a long history of recommending encryption, dating from our public statement in 2010 where we recommended it as a security measure under the Data Protection Act 1998. Our current guidance explicitly discusses how organisations should adopt encryption 'at rest' and 'in transit' as recommended measures to secure personal data they either store and/or transmit[16].

11. While we do not say that organisations must encrypt in all circumstances, there must be a strong justification for not doing so. This also applies to E2EE. Our position aligns with recommendations by key actors in the cybersecurity domain such as the National Cyber Security Centre (NCSC) who also recommend encryption as a security measure for protecting personal data in a number of guidance products, including the Cyber Assessment Framework, their Cloud Security principles, their guidance on protecting bulk personal data and their guidance on securing incoming connections.

E2EE and Online Safety

12. E2EE is vital to citizens and industry because of the security, safety and trust that it generates and the wider benefits that private spaces provide. It is an essential component of a safe digital ecosystem, providing safety for users online, including protection against exposure to harmful content and activity.

13. However, because it restricts the detection of harmful content, it also presents a challenge from an online safety and law enforcement perspective. The characteristics of E2EE that enable private and secure communications for the public also provide safe harbour for criminal activity. Child safety has emerged as central to the current debate, with valid concerns that encrypted channels are creating spaces where children are at risk.

14. We are mindful of this wider context and recognise that we do not regulate in a vacuum. We understand that there are real and present issues at the intersections of encryption, national security, law enforcement and online harms. However positioning E2EE and online safety as being in inevitable opposition is a false dichotomy. Instead what is needed is an approach that seeks to reconcile the different demands whilst recognising the need to create a safe online ecosystem for all users. The challenge is to create tailored and proportionate responses to the issues that manifest without unduly

[16] ICO (2018.) *Encryption and data transfer.* ICO.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/encryption-and-data-storage/.

interfering with the wider benefits that E2EE provides or the rights and freedoms of wider society. It is vital that one form of online safety is not traded off for another.

15. Measures that would introduce widespread “backdoors” to encrypted channels or otherwise enable indiscriminate widespread access, would create systemic weaknesses unacceptably undermining security and privacy rights, introducing data protection risks and adding to the overall safety concerns by creating more spaces for harm. We do not support such measures. We welcome the UK Government’s support for strong encryption[17] as well as its position that it does not support the development of so-called ‘backdoors’ in social media platforms to allow access for law enforcement or security agencies[18,19].

16. Further, when asked, the Government has also stated to us that:

- ‘HMG is not looking to undermine security on E2EE platforms, for instance by introducing ‘backdoors’. Our approach is about considering the introduction of specific additional functionality to companies’ services, to enable access to messaging content by law enforcement, or the service/platform provider, under specific and tightly controlled circumstances. This would need to be underpinned by a detailed design, implementation and management process by the company in question, to industry good practice standards, that respected the importance of cyber security and the protection of users’ data and privacy.’

Reconciling Safety and Privacy Objectives

17. Here we outline how the consideration of E2EE and the impact on privacy and online safety could be framed around reconciling objectives rather than putting them at odds.

18. Key factors that should be considered include:

- The **demand from consumers for services that safeguard their privacy** and thereby support their safety online.

- The **requirements that existing legislation places on businesses**, including the legal obligation on data controllers to process personal data securely.

[17] https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety/international-statement-end-to-end-encryption-and-public-safety-accessible-version
[18] https://www.mi5.gov.uk/news/director-general-ken-mccallum-gives-annual-threat-update-2021
[19] https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

- The **effectiveness of existing legislative and technical tools to ensure lawful access to data** for law enforcement and national security purposes without weakening or 'breaking' widely-adopted encryption standards. Consideration should be given to whether the objectives of the online safety regime can be met through these channels without introducing additional requirements on organisations to adopt processes which could undermine E2EE on their services.

- The **potential future development of technical solutions for detecting harmful content without weakening E2EE**, which offers promise for reconciling E2EE and the detection of harmful content. There are certain solutions which currently suggest a tangible roadmap. Consideration should be given to the extent to which legislative intervention will be needed as technology evolves.

- The **necessity, proportionality, targeting and effectiveness of any proposed legislative solutions**. For example, interventions that weaken E2EE across all mainstream services/users will threaten the safety and security of the majority of users and may not achieve the desired safety outcomes because bad actors can easily switch to more niche services.

- The **social impact of any proposed legislative solutions on online safety and privacy** for the population as a whole. Any proposed solutions should seek to reconcile the need to address harms on encrypted channels with the wider impact on privacy and online safety flowing from any reductions in security, and seek to reduce harms overall, particularly to vulnerable users.

- The **economic impact of any proposed legislative solutions**, both in terms of their direct costs to business and any indirect effects of weakening user trust in digital services.

19. At the ICO we will look to shape this landscape to support privacy. In practice this means both ensuring that mature access mechanisms and technologies are used lawfully, necessarily, and proportionally, and supporting the growth of more nascent privacy-preserving techniques such as homomorphic encryption as they scale.

20. We are pleased to be engaged in the Government's Safety Tech Challenge Fund which is supporting innovative solutions to tackle child sexual exploitation and abuse in end-to-end encrypted environments. Additionally, we are leading a programme with support from the Government's Regulators' Pioneer Fund to stimulate the development of privacy enhancing technologies, and we are also

developing guidance for the use of these technologies. We recommend that the development of technical solutions continues to be prioritised and supported.

A Multistakeholder Approach

21. As outlined above the policy response to E2EE and online safety requires a nuanced and detailed understanding of the broader issues. We recognise that these are problems with no easy answers. Their complexity means a truly multistakeholder approach is needed to find solutions that recognise and seek to reconcile the different perspectives.

22. At the ICO we are engaging with a variety of stakeholders so that we can better understand their priorities and concerns and be responsive to them. Through the Digital Regulation Cooperation Forum (DRCF) we are working with Ofcom, and the Financial Conduct Authority to understand the implications of E2EE for the people using digital services, as well as for industry, and its implications for us as digital regulators. We will be seeking the views of stakeholders to bring a range of perspectives on E2EE together and help set priority areas for future joint work. We will publish the outcomes of our work (which will not be limited to online safety) early next year.

Conclusion

23. In summary, E2EE is central to a safe and private online experience and benefits citizens and businesses. It enables privacy, and privacy is also safety. Privacy and child safety are critical, and we recognise this, but achieving these objectives needs to be reconciled rather than put at odds. We do not see value in proposals that seek to weaken E2EE, but we do see value in accelerating innovations that allow the detection of harmful content without compromising privacy.

24. We are taking our work forward in a multistakeholder manner. Through the DRCF we are working with Ofcom and other partners and we also continue our engagement with national and international stakeholders. We stand ready to provide further assistance to key stakeholders as required.