Roundtable Report

“Security Through Encryption and Despite Encryption: An (un)Achievable Outcome?”

6 July, 2021

A Debate on Encryption

On 16 June, 2021, the Internet Society organised a roundtable to explore in greater detail how to apply the European Council’s position on encryption, following its November 2020 Resolution; “Security through encryption and security despite encryption”[1] .

The Internet Society invited thirteen participants from EU member states, UK and Brazil, and across government, civil society and the technology sector. The roundtable was held under the Chatham House Rule.[2] NB: Due to the unavailability of all invitees, the roundtable included more advocates of encryption than representatives of law enforcement interests. This summary report aims to give equal weight to contributions from all perspectives.

1 Can We Have Security Without Encryption?

The European Council resolution, put forward by the German presidency and supported by other member-states, uses the term ‘security’ in two distinct contexts; the “digital security of governments, industry and society” which requires ‘security through encryption, and “the area of security and criminal justice” which tries to provide ‘security despite encryption’. Operationalizing this distinction is a key challenge, and seems to require different governance regimes, both to deliver secure systems and to deal with access and interception of encrypted content and communications.

[1] Resolution 13084/1/20 REV 1: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf

[2] When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed. https://www.chathamhouse.org/about-us/chatham-house-rule

All participants agreed that encryption is a vital element of digital life and the digital economy, but some distinguished between the need for encryption to secure infrastructure and services such as smart vehicles, and end-to-end encryption that secures communication for all citizens but which allows criminals to communicate in secrecy. Initial discussion suggested a trade-off that 'balances' safety and security versus fundamental rights, but later speakers said the trade-off is between safety and security on the one hand, and fundamental rights, different government regimes and norms about the rule of law, economic and societal benefits and costs, and the downstream impact in less democratic and governance-led societies.

2 How Can We Develop the European Council Resolution into Practical Policies?

The session focused largely on end-to-end encryption of communications. One suggestion was to ensure the overall security framework is as strong as it can be, but add targeted safety measures to ensure access to encrypted communications, including those involving Child Sexual Abuse Material (CSAM), terrorism and organised crime. One process for resolving competing rights is "**practical concordance**", used in Germany, which works to move beyond binary choices and absolutist positions to balance competing interests and rights. On circumventing end-to-end encryption, governments have avoided mandating specific technical solutions, Instead, the European Commission has set out five considerations for what technical solutions should achieve;

- Orders to access encrypted information must be targeted, proportionate and validated judicially
- There should be transparency and reporting procedures
- Review and redress
- The EU will not weaken or indirectly ban encryption
- This is a means of last resort, when less intrusive means are unavailable.

Several participants said while this guidance is useful, they would strongly welcome **practical proposals** from governments of how to achieve these goals, as after twenty years of debate it has not yet been possible to provide access to encrypted data without weakening or limiting encrypted communications overall. The solutions typically suggested – backdoors, access to private keys, Upload filters – weaken overall security, not just of those targeted for access. This was not because service providers wish to take absolutist positions, but due to how encryption works. The value was questioned of guidance that does not explicitly require weakening or circumvention of strong encryption, but whose implementation would.

One participant said law enforcement access service providers' to metadata, network graphs and abuse reports were sufficient for most requests, and that access to communication content did not add sufficient utility to meet a **cost-benefit analysis** of the impact on all communications of weak or broken encryption. In response, information was provided that according to the Swiss Federal Police 86% of the alleged CSAM messages reported via NCMEC[3] are not criminally relevant. A participant referenced North Rhine Westphalia in Germany where it appeared a key factor in law enforcement ability to investigate CSAM and protect victims may not have been access to encrypted data but insufficient police resources to deal with existing data.

However, a participant with expertise in law enforcement concerns said it is more complex to analyse the trade-offs between encryption and no encryption, bringing up the statistic that in 2020 there were 12 million hits on CSAM on Facebook Messenger and that if Messenger were encrypted this would be zero. While these offences might simply be displaced if that service was not available, there was nonetheless a mismatch in reporting; Whatsapp was said to ban around 300k accounts a month for CSAM, but makes only 40k reports a year.

A description of how the European Council resolution could be operationalized involved warrant-permitted access to encryption keys held either by telecoms providers or by third parties. The 'encryption bundle' would be turned off for one individual or institution and the data copied and sent to law enforcement. This model requires trust in the providers and the judges and system that oversee access to unencrypted data. Discussion would be needed on how to hinder dictatorships abroad, or even populist governments within the EU Member States, from using similar schemes, however.

However, it was noted that a crucial step that allowed us to secure the modern digital world was the development of asymmetric cryptography. This reduced the role of and trust placed in third parties, meaning security is delivered by verifiable technologies and not on the say-so of business and legal procedures. Moving back to a **trusted third party (TTP) model** would require the ability to have rational trust in both the technology and the procedures of organizations, and all those organizations' future owners. The additional cost and liabilities of a TTP model mean it could only be provided at scale. Smaller EU member-states would have little control over service-providers to their citizens, and ultimately the service-providers may not be EU-domiciled at all, with the accountability problems that brings. In this context, the goal of 'security despite encryption', i.e. increasing safety by exercising regulatory control over encryption, may not be achievable, if the encryption is being applied outside a country's jurisdictional reach.

The discussion covered many issues from the encryption debate; criminals may circumvent systems that capture law-abiding citizens; broad surveillance is ineffective against organised crime and

[3] National Center for Missing and Exploited Children

removing encryption from known services means criminals will migrate to less law-abiding ones; weakened communications encryption invites hostile state and other actors; TTP regimes are susceptible to everyday mismanagement and targeting by hostile actors; and how the Schrems II decision confirms the need for European policymakers to pro-actively ensure citizens can communicate securely. A participant countered that no system is 100% secure.

A new perspective emerged in relation to how '**safety tech**' shows the whole concept of 'targeted' interventions may be out of date. 'Safety tech' is sold to schools and required of pupils to use in their homes. It uses a "man in the middle' tool to intercept all communications and screen activity on a child's computer while connected to a school network. This type of service already goes further than policy permits, with one service provider apparently admitting to having been advised by their lawyers that the interception performed by their product at one time could result in the provider being jailed. It shows the risk of weakening privacy and security in order to protect children, when UK providers are in fact owned by firms in Bahrain and China. Policies that require 'targeted' privacy and security reductions to fight serious crime ultimately result in vulnerabilities at scale, exporting data in potentially harmful ways, to companies that may be sold in the future to owners who do not observe today's constraints. Governments that hand surveillance powers to private firms may be making unfounded assumptions about legal compliance, behavioural norms and future safety. A related point regarding children's safety was that children also need safe and secure online spaces supported by encryption.

It was also noted that despite end-to-end solutions are widely used, law enforcement has access to as many data as never before, including metadata and "forensic tools" for client-side hacking, as well as cloud access, where unencrypted data is often stored.

Ultimately, the roundtable only partly moved past the known binaries choices of the encryption debate. On one hand, no solution has been advanced that would deal with the security concerns of encryption advocates – for whom the dilemma is that you either have encryption or not have it at all –, and on the other, no policy guarantees achievement of both the stated objectives of 'security through' and 'security despite' encryption. Notwithstanding their fixed positions, participants on each side suggested working on additional law enforcement alternatives to accessing encrypted communications.

3 Possible Paths Forward

Fruitful future areas for discussion may include:

- Trust and TTPs – procedural protocols, practicalities and whether new possibilities have emerged, and the broader question of how/whether trust can move the conversation forward

- Alternatives to accessing encrypted communications, e.g. metadata, technical assistance and other improvements to law enforcement capability that do not require access to encrypted content and communications
- Broader cost-benefit analyses to identify data and case studies on law enforcement access, and also to consider economic and societal costs and downstream effects
- Specific discussion of the Carnegie report[4] , or adoption of the report's framing recommendations to structure and inform future discussions
- An in-depth discussion of ANoM[5] to identify which aspects of that initiative are workable, contentious or could be developed further.

[4] "*Moving the Encryption Policy Conversation Forward*", Encryption Working Group, September 10, 2019. Paper https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

[5] A "sting operation (known as Operation Trojan Shield or Operation Ironside) - a collaboration by law enforcement agencies from several countries, running between 2018 and 2021, that intercepted millions of messages sent through the supposedly secure smartphone-based messaging app ANOM." https://en.wikipedia.org/wiki/ANOM