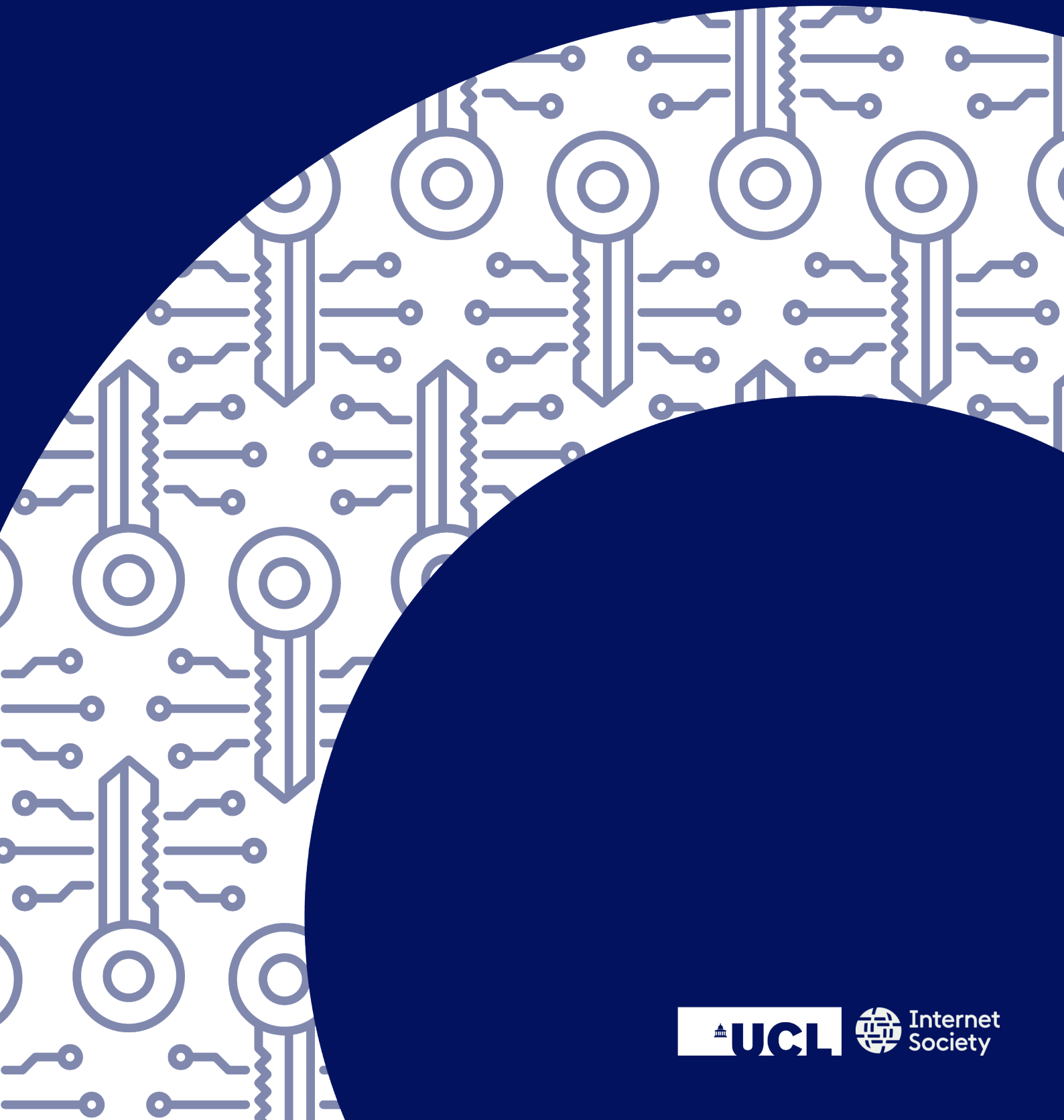
ENCRYPTION: PROS AND CONS

Adeola Akinla, Ayesha Gulley, Kirthika Selvakumar, Zoe Tilsiter



UCL Internet Society

TABLE OF CONTENTS

Acknowledgements

This research benefits immensely from a community of resources that we were privileged to access and for which we cannot express enough gratitude.

First and foremost, we would like to thank our client partner, Robin Wilton of the Internet Society for his commitment, interest and invaluable inputs during the research. Our fortnightly meetings were not just an opportunity to discuss the research, it was also a chance for us to form a cordial working relationship.

We would also like to thank our supervisor, Dr Jose Tomas Llanos for his support and guidance throughout the research. Thank you for broadening our perspectives on the research topic and encouraging us to give our very best.

Our deepest appreciation goes to the UCL STEaPP faculty who in various ways gave clarity to this research. To Dr Irina Brass, Dr Adam Cooper and Dr Leonie Tanczer, thank you for shining a light that illuminated the paths to our research strategy and methodology.

We would also like to thank Iona Preston of UCL Library Services, who always responded to our inquiries and provided pointers as we navigated the desk-based research process.

To the participants who honoured our invitations to partake in our interviews, we say a big thank you. By allowing us into your individual worlds, you gave us access to your unique viewpoints which were truly fundamental to the findings of this research.

Finally, we are grateful to our families who have been one of the biggest influences and support systems through our journeys.

Thank you.

Executive Summary

Encryption is a data security mechanism essential for providing data confidentiality and integrity of services. These improve the security of communications online, and in doing so, enhances fundamental human rights, such as privacy and freedom of expression. However, the confidentiality of communications afforded by encryption can be used to conceal criminal activity and prevent law enforcement from accessing criminal communications. As a result, there has been a recent global regulatory trend towards weakening encryption to enable access for law enforcement and national security purposes. Therefore, public debate over encryption remains polarised. While state actors claim encryption prevents access to vital evidence needed for criminal investigation, weakening encryption presents risks to privacy, cybersecurity and civil liberties. In partnership with the Internet Society, this research set out to examine the risks and benefits of weakening encryption given current contrasting stakeholder perspectives. The research engaged socio-political and economic lenses to explore different interests at stake, including privacy, cybersecurity, public safety, national security and economic competitiveness to develop a decision-making framework to guide policymakers in the ongoing encryption policy debate.

A mixed methodological approach was adopted to answer the overarching research question: What should policymakers be aware of and consider in their decisions concerning the weakening of encryption technologies? Desk-based research comprised of a Rapid Evidence Assessment, Systematic Grey Literature Review, and Causal Loop Diagram. Additionally, primary research involved conducting semi-structured interviews to inform a Variant Multi-Criteria Decision Analysis.

Findings from the research revealed minimal economic coverage on the impacts of weakening encryption and an under-representation of evidence from the Global South. The claimed benefits of weakening encryption are improved abilities of law enforcement to investigate crime and uphold public safety. However, these benefits are offset by noted risks such as disproportionate impacts on vulnerable groups, increased cybersecurity vulnerabilities, infringements of human rights, along with high economic costs and loss of consumer trust. Overall, the research found that the risks of weakening encryption outweigh its benefits.

This research has added value to the ongoing encryption-policy debate and extended the Internet Society's work in four main ways:

- Evidence has been collected from geographical regions that are under-researched in relation to the encryption debate and not currently in the Internet Society's encryption spotlight.
- Evidence relating to the economic lens which is also under-researched in relation to the encryption debate, was collected during the research.
- The coding framework categorising the main factors considered by stakeholders in the encryption debate can be applied and used in future research on the topic.
- Using Variant Multi Criteria Decision Analysis, a Decision-Making Framework (DMF) based on multiple stakeholder perspectives was developed. The DMF seeks to guide policymakers rather than prescribe a definitive set of solutions for encryption-related policies. Consequently, it should be applied with consideration to individual state contexts and priorities.

Key Findings

Key findings of this research aim to guide policymakers in their decisions regarding weakening encryption.

- Findings from the desk-based research revealed two gaps in the selected encryption literature; few discussed weakening encryption with relevance to an economic lens and the geographical region of the Global South.

- Frequently discussed means of weakening encryption concerned exceptional access to encryption through: interception warrants, technical assistance warrants, equipment interference, and compelled disclosure of decryption keys. Other discussed means included key escrow, 'brute force' and 'man in the middle' attacks, and the future capabilities of quantum computing.

- Justifications for weakening encryption technologies included providing assistance with criminal investigations, primarily related to drug trafficking and child sexual abuse material. Additional cited justifications were preserving national security, countering terrorism, upholding public safety, and surveillance activities.

- The claimed benefit of weakening encryption entails removing a barrier for LEIAs in criminal investigations for national security and public safety purposes. However, research found that this benefit could be undermined by bad actors exploiting additional vulnerabilities created by backdoors. Additionally, such benefits for LEIAs have been achieved through alternative means to weakening encryption.

- The risks of weakening encryption include infringements on human rights such as the right to privacy and freedom of expression, disproportionate impacts on vulnerable groups, economic costs, and threats to cybersecurity. Overall, the research found that the risks of weakening encryption exceed its claimed benefits.

- Findings from primary research revealed that civil society participants considered human rights and public safety as factors when evaluating proposals to weaken encryption. It was also raised that the use case argument for weakening encryption does not often seem proportionate to the purported objectives of state actors.

- Cybersecurity concerns, economic considerations, and public safety featured most in industry participants' decisions concerning weakening encryption. Weakening encryption would create new vulnerabilities for cyber-attacks, which in turn damage consumer trust and harm economic competitiveness of firms offering encrypted products and services.

- From the policymaker perspective, the most valued factors in encryption-related decisions were the need for specific use cases for weakening encryption, and human rights. This is important as the argument for weakening encryption is narrowly focused and overstates criminality at the expense of wider societal issues. Additionally, it was noted that a state's decision to weaken encryption would set a global precedent without implementing necessary safeguards.

- Collectively, these findings were used to develop a Decision-Making Framework to guide policymakers in discussions around weakening encryption. It does so by positing socio-political and economic questions to policymakers across three paradigms; purpose of weakening encryption, LEIA capacity requirements and geopolitical effects.

- Using Variant Multi Criteria Decision Analysis, a Decision-Making Framework (DMF) based on multiple stakeholder perspectives was developed. The DMF seeks to guide policymakers rather than prescribe a definitive set of solutions for encryption-related policies. Consequently, it should be applied with consideration to individual state contexts and priorities

List of Abbreviations

CSAM	Child Sexual Abuse Material
DMF	Decision-Making Framework
E2EE	End-to-End Encryption
ECHR	European Convention for Human Rights
FBI	Federal Bureau of Investigation
IA	Impact Assessment
LEIAs	Law Enforcement and Intelligence Agencies
MCDA	Multi Criteria Decision Analysis
MCM	Multi Criteria Mapping
REA	Rapid Evidence Assessment
SRP	Systematic Review Protocol
SSL/TLS	Secure Sockets Layer/Transport Layer Security
UDHR	Universal Declaration of Human Rights

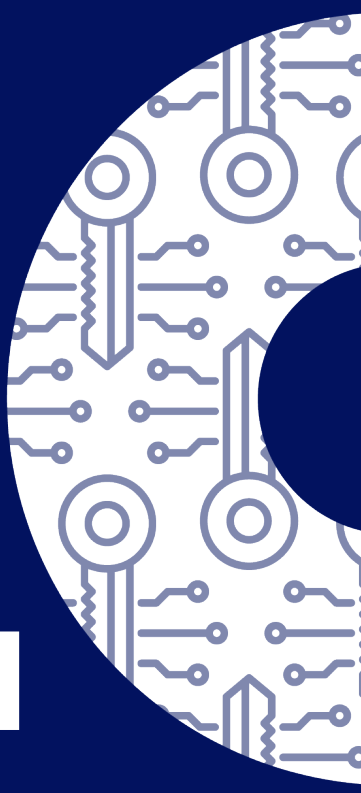
Glossary of Terms

Best Case Score	Known as 'optimistic score' on the MCM tool. A score provided by interview participants that indicates the best performance of an option under a given factor.
Clusters	Groupings of options appraised during interviews on the MCM tool.
Factor	Known as criterion/criteria on the MCM tool. A measure defined by interview participants which informs their judgements over the performance of a range of different options.
Issues	Groupings of factors that are seen to share similar features based on the MCM results. The MCMr tool provides the means to explore a variety of issues.options.
Perspectives	Groupings of stakeholder viewpoints that may share similar characteristics. The MCM tool provides the means to explore a variety of perspectives.
Rank Means	Option rankings displayed as a range between two 'extreme' averages: (i) all best-case scores and (ii) all worst-case scores
Worst Case Score	Known as 'pessimistic score' on the MCM tool. A score provided by interviewees that indicates the worst performance of an option under a given factor

List of Tables and Figures

1

INTRODUCTION



1. Introduction

Encryption is a vital technology for the fabric of the Internet which ensures safety, confidentiality, and privacy. It plays a key role in securing private information when banking, shopping and communicating online. This is especially important, given today's digital society and that many day-to-day interactions occur online. However, malicious actors are prone to abuse the protection that encryption offers to commit crimes. Consequently, law enforcement claim that their ability to investigate crimes is curtailed due to the inability to access encrypted communications; prompting the 'going dark' argument.[1,2] In recent years, there is a growing push by governments to weaken encryption by introducing 'backdoors' to allow law enforcement access to encrypted communications. However, this would create a technological point of failure that would eliminate the protection encryption provides. Additionally, bad actors could exploit vulnerabilities created by these backdoors. Therefore, the weakening encryption debate exhibits tensions between law enforcement and national security on one hand, and cybersecurity and privacy on the other. This, along with additional tensions between conflicting interest will be explored further in this research.

In partnership with Internet Society, this research seeks to uncover factors that impact civil society, industry, and policymaker stakeholders in the encryption debate through socio-political and economic lenses.

This research defines socio-political as the national security, public safety and human rights implications of weakening encryption. The human rights impacted by encryption include the right to a fair trial and non-self-incrimination, right to privacy, freedom of expression and freedom of assembly, as outlined in Articles 10, 12, 19 and 20 of the Universal Declaration of Human Rights (UDHR),[3] and Articles 6, 8, 10 and 11 of the European Convention for Human Rights (ECHR).[4] Within the scope of the research, economic lens comprises of the business impact of weakening encryption, in areas such as innovation, consumer trust in encrypted technologies, and economic competitiveness of industries and countries

Research Deliverables

This research aims to deliver an Impact Assessment (IA) and a Decision-Making Framework (DMF) for policymakers. The objective of the IA is to explore the risks and benefits of weakening encryption which will complement the DMF. The DMF intends to guide decision-making for policymakers in current discussions to weaken encryption technologies.

Research Questions

To guide this research, the following overarching research question has been formulated. Three sub-research questions (SRQs) have been articulated to contextualise the overarching question:

RQ: What should policymakers be aware of and consider in their decisions concerning the weakening of encryption technologies?

SRQ1: What are the means of weakening encryption?

Purpose: To explore the various ways state actors propose to limit, restrict, or undermine the use of encryption technologies.

SRQ2: What are the justifications for weakening encryption?

Purpose: To identify and understand the claims state actors put forward in their arguments to limit, restrict or undermine encryption technologies.

SRQ3: What are the impacts (risks and benefits) of weakening encryption?

Purpose: To answer documented or likely effects of weakening encryption technologies.

1.1 What is Encryption?

Encryption is a method by which individuals can securely store or communicate data.[5] The method uses an algorithm to generate a unique cryptographic key, where the key is a string of bits that scrambles readable plaintext into unreadable ciphertext.[5] Once encrypted, the data can be securely stored on devices or cloud servers, or transmitted across the Internet.[5] Only parties with a copy of the key can decrypt and read the data. Should the data is compromised, unauthorised third parties will only see the data in its unintelligible form.[5] Additionally, data can be encrypted at any point; this includes at rest (data that is received and stored), and in transit (data that is being sent from one location to another).[6] There are two main types of encryption systems. The first is symmetric encryption, which entails using the same keys to encrypt and decrypt information.[7] Symmetric encryption is typically used to protect data-at-rest.[5] For example, it is used by applications to protect stored files, by operating systems to protect unauthorised access to user data (full-disk encryption), and by smartphones and tablets to lock devices.[5]

The second type is asymmetric encryption where the encryption and decryption keys are different. Asymmetric encryption uses both public and private keys;[5,7] while a public key is available to everyone, a private key is only available to specific individuals.[7] In asymmetric systems, the sender uses the recipient's public key to establish a secure communication channel, but only the intended recipient can receive and decrypt the ciphertext using the transmitted public key in combination with their private key.[5] In this way, a sender can encrypt a message using a public key, but only the intended recipient, who is the holder of the private key, will be able to decrypt the message into plaintext.[7]

One type of encryption that uses both symmetric and asymmetric encryption is end-to-end encryption (E2EE), which provides confidentiality for transmitted data between two endpoints and on a recipients' device.[2] In E2EE, a message encrypted at its source cannot be decrypted until it reaches its intended recipient where it is decrypted. This means that no third party can access the plaintext or the decryption key.[2] Many communication services use E2EE protocols, including Instant Messaging (IM) applications like WhatsApp and Telegram, e-mail services such as ProtonMail, and Voice over IP (VoIP).[2] These protocols are designed so that third parties such as service providers do not have access to any of its users' private keys.[2] This prevents third parties from being able to access messages in plaintext.

1.2 Background

The policy debate surrounding weakening encryption and the tensions between privacy and security are long established. However, the nature of this debate has evolved over time; beginning with a focus on key escrow mechanisms, followed by a broader discussion surrounding law enforcement counter-terrorism capabilities and recently proposing weakening encryption to combat child sexual abuse material (CSAM) online.

First Crypto War (1990-2000)
Prior to the 1990s, encryption was restricted to military purposes and there was limited commercial use.[8] However in the early 1990s, public demand for strong encrypted communications grew alongside the adoption of the Internet.[8] Governments recognised this demand for user security but did not want to jeopardise their surveillance capabilities to access communications.[8]

This prompted the 'Crypto Wars', characterised by a focus on building backdoors into encrypted systems which would enable user security without detracting from investigatory objectives.[1,8,9] This included the USA's "Clipper Chip" proposal in 1993; a cryptographic chip which encrypted communications when installed on devices.[8] However, the US Government proposed acting as a trusted 'third party' by storing copies of the Chips' encryption keys in escrow, allowing law enforcement to decrypt communications when needed.[8] This escrow proposal was defeated in 1999 due to pressure from civil society organisations and academic consensus that the Chip was easy to exploit and therefore not secure.[8,10] In response to this Crypto War, in 1997 the OECD issued a set of Guidelines for Cryptography Policy,[11] which acknowledged the need for strong encryption, and required any lawful access measures to respect privacy rights and the confidentiality of information systems.[1,8]

Second Crypto War (2010-2018)
Between 2000-2010, public debate around access to communications and security did not overly mention encryption.[1] However, in the 2010s, the debate resurfaced. Following the Snowden disclosures in 2013, which revealed the interception capabilities of state actors such as the NSA, encryption tools became more pervasive amongst companies and individuals seeking to protect their privacy and data security. Resultantly, the debate surrounding cybersecurity and privacy, and law enforcement and national security rematerialised as the Second Crypto War.[1,9] This time, Law Enforcement and Intelligence

Agencies (collectively termed LEIA), such as the FBI, presented the going dark narrative; namely the widespread use of encryption had inhibited their ability to lawfully gain access to information needed to tackle terrorism and other serious crimes.[1,8,10] Thus, the debate did not focus on specific backdoor mechanisms like the First Crypto War, but marked a clear stance that greater access to encrypted data was necessary. [8]

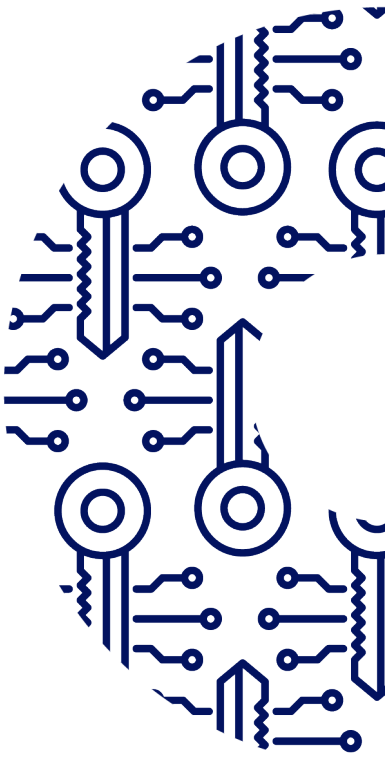
This narrative prompted a regulatory push for solutions to this going dark issue, particularly by the 'Five Eyes' intelligence alliance countries. Canada's 2016 National Security Consultation flagged encryption as an intelligence challenge that motivated the government's agenda for reform.[8] There was also a drive to compel third parties such as technology companies to provide technical assistance to LEIAs in their investigations by decrypting communications. For instance, in 2016, the FBI issued a court order on Apple to break the security of an iPhone during the investigation of the San Bernardino shooting. [9,12] Apple strongly opposed the order on grounds that this would essentially create a backdoor and undermine encryption on the iPhone.[1]

Recent Developments (2020-Present)
Recent developments have brought to the fore workarounds to weakening encryption, further complicating the tensions between public safety and privacy.

Apple's new CSAM scanning technology[13] is indicative of technology companies cooperating with law enforcement by providing technological means to access data for public safety purposes. This on-device matching technology uses cryptography to detect known CSAM images before they are stored in iCloud Photos by cross-examining them with a database of known CSAM hashes.[13] This will enable Apple to report these instances to the National Centre for Missing and Exploited Children (NCMEC) and law enforcement.[13] Apple has said this technology is designed to protect user privacy whilst finding illegal content, but critics claim that this design amounts to a security backdoor if user privacy is infringed.[14]

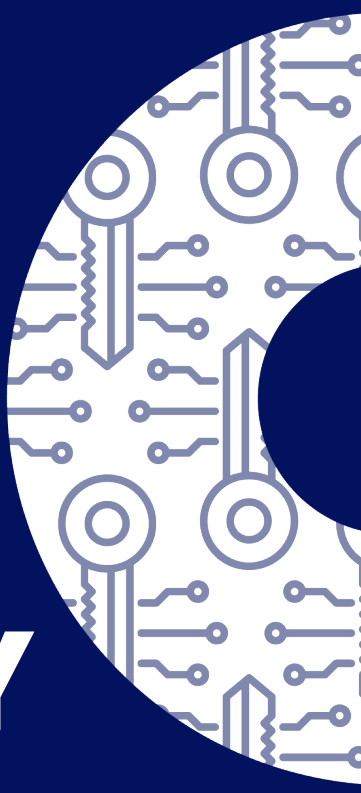
Additionally, LEIAs are beginning to turn to supply chain interference as a workaround to access encrypted communications. Recent news of the Federal Bureau of Investigation's (FBI) ANOM Operation revealed that the FBI informants had planted devices with an encrypted messaging application within criminal networks.[15] This allowed the FBI to intercept information and monitor criminal chats concerning drug smuggling and money laundering. As a result, 800 suspected criminals were arrested.[15]

Given these workarounds, and states' growing interest in mass surveillance, as exhibited by the Pegasus project database leaks in July 2021,[16] the role of encryption in ensuring the security and privacy of communications continues to be pertinent.



2

METHODOLOGY



2. Methodology

This research takes a multimethodological approach. Analytic methods were selected based on their suitability and compatibility in delivering the IA and DMF given resource and capacity constraints. Methods used both primary and secondary data.

The selected methods were:

- Rapid Evidence Assessment (REA)
- Systematic grey literature review
- Causal Loop Diagram (CLD)
- Variant Multi Criteria Decision Analysis (MCDA)

In the first phase of the research, three desk-based methods for secondary research were applied to gather a comprehensive understanding of the encryption debate such as the key actors, arguments for and against weakening encryption and the associated issue-linkages. These methods include a rapid evidence assessment, systematic grey literature review and causal loop diagram. In phase two, primary research was done through interviews as part of the Variant Multi Criteria Decision Analysis (MCDA) method which utilised the Multi Criteria Mapping (MCM) tool. Both primary and secondary data collected will be analysed using the relevant methods to produce the research deliverables. The following sections will detail the purpose, process, benefits, and limitations of each method.

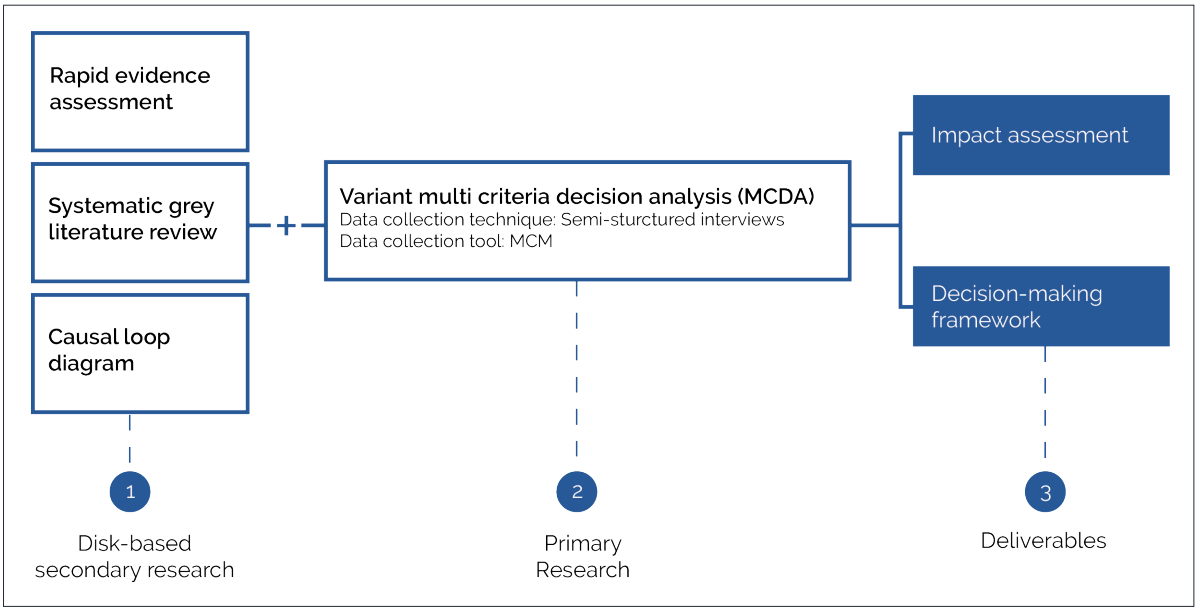


Figure 1: Analytic Methods Workflow

2.1 Rapid Evidence Assessment (REA)

REA was selected to provide a balanced assessment of the academic literature on the encryption debate by using systematic review methods. Particularly in the policy context, an REA adds value by ensuring that evidence is found in a systematic, rigorous and reproducible manner. This ensures the policy findings derived from the found evidence are defensible.[17] The purpose of the REA is to find and synthesise academic evidence on the encryption debate. Conducting an REA is suited to the nature of the research as it can be adapted to the specific policy context. Given the resource constraints, it provides a quick, low-cost, desk-based approach to identifying relevant academic literature.

The REA will be operationalised in three parts: 1) developing a search matrix using terms from the research questions, 2) defining the inclusion and exclusion criteria which will determine the breadth of the REA and 3) formulating a PRISMA framework for screening and selecting studies to be critically appraised in the final stage. Details of the REA process can be found in Appendix 1.

A limitation of the REA is it is prone to bias being introduced through the selection of search terms and their associated synonyms in the search matrix. This risk has been documented in the Risk Management Table (Appendix 5) and is mitigated by the research team collectively developing the search matrix to reduce individual bias. Furthermore, conducting an REA excludes relevant non-academic evidence such as policy-orientated documents and research reports that explore the encryption debate from different angles. Consequently, a systematic grey literature review was conducted to address this shortcoming.

2.2 Systematic Grey Literature Review

Grey literature is defined as "literature that is produced by all levels of government, academics, business and industry but which is not controlled by commercial publishers".[17] Grey literature is a valuable source of evidence as it can often contain policy and research relevant evidence.[18] Furthermore, it can convey the experience of underrepresented stakeholders not covered in the REA and insights of experts that are not associated with academia.[19] Additionally, it can contain up-to-date analysis of recent developments as grey literature can be published quicker than academic evidence. This is especially pertinent given the dynamic and policy-orientated nature of decisions related to the weakening of encryption.

The purpose of performing a systematic grey literature review is to develop a reproducible framework to identify, screen and appraise relevant grey literature that will complement REA findings to inform the IA and DMF. However, as there is no prescribed standard for conducting a systematic grey literature search, a process similar to the REA will be undertaken. The systematic grey literature search will be operationalised in four stages:

1. members of the Global Encryption Coalition[20] will be categorised by region and screened for an up to date website in English,
2. websites of members will be perused to check if they had published grey literature on encryption since 2000,
3. identified publications will be appraised against a modified AACODS framework to ensure that all selected articles are of good quality,
4. studies that pass the modified AACODS framework and answer two research questions will be screened at full text.

The limitations of the systematic grey literature review include it being time consuming as publications are not centrally located. There is also a small risk of selection bias which consequently shapes the findings. Further details on the systematic grey literature review can be found in Appendix 2.

2.3 Causal Loop Diagram (CLD)

Originating from system dynamics and systems thinking, a CLD illustrates the relational dynamics of variables present in a complex policy problem.[21] It provides a way to map out the multiple interrelationships between variables and help to understand the policy problem in a non-linear, dynamic and holistic manner. The purpose of constructing the CLD for this research is to understand how the various issues within the encryption debate interact with each other and whether they are affected positively or negatively.

Mapping out the CLD is a three-step process: 1) define the focus of the CLD which is the implications of weakening encryption 2) identify variables that might be affected if encryption is weakened and to note if these effects are positive or negative, and 3) categorise and label the relationships as balancing or reinforcing loops. The limitation of a CLD is that while it can identify possible sources of policy resistance, derived from specific sources of information and would need to be subjected to simulation or model testing before conclusions can be drawn.[22]

2.4 Variant Multi Criteria Decision Analysis (MCDA)

Multi Criteria Decision Analysis (MCDA) was selected due to its suitability to formulate a Decision-Making Framework given the complex policy nature of the encryption debate. Originating from the field of mathematics and operational research, MCDA locates itself under the umbrella term of Multi Criteria Analysis which allows for multiple objectives and decision criteria to be formally incorporated into the analysis of a problem.[23] The purpose of the MCDA for this research is to systematically account for the multiple, often competing objectives and interests of key stakeholders in their decision-making regarding the weakening of encryption.[23,24]

By including multiple objectives and criteria, MCDA can provide richer and nuanced insights into the nature of decision-making that are beyond the monetary values provided by other decision-making frameworks like cost-benefit analyses.[25–27]

For this research, the MCDA method will be tailored so that the findings do not prescribe weights to factors or champion a specific decision. Instead, a variant MCDA seeks to present policymakers with the multiple concerns and priorities that feature in key stakeholders' decision-making. It will be purposefully adapted given the complexity of the encryption debate and that policy decisions are influenced by the form, principles and values of governance which vary significantly across the world..

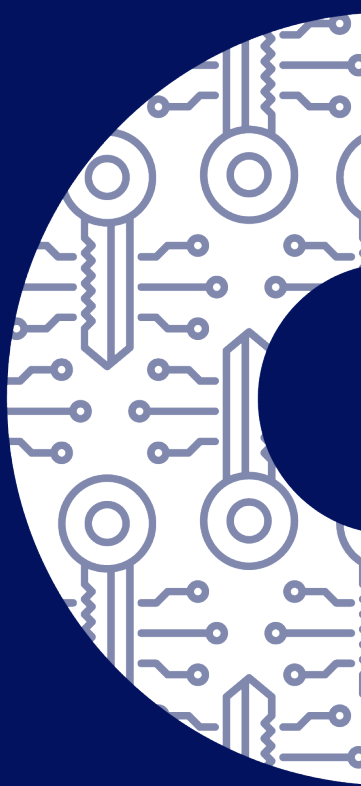
A participatory as opposed to a non-participatory approach will be selected as it more authentically reflects the different viewpoints of stakeholders and adopts a collaborative and democratic decision-making style.[23] Additionally, a participatory approach caters to the uncertain and ambiguous nature of policy decisions related to weakening of encryption.[23] To assist with the collection and analysis of data from the MCDA, the interactive web-based Multi Criteria Mapping tool ("MCM tool") developed by the Science Policy Research Unit at the University of Sussex will be deployed.[28] Using this tool, data will be collected in a structured four-part process: 1) identifying options, 2) defining criteria, 3) assessing scores and 4) assigning weights.

Primary data for the MCDA will be collected through semi-structured interviews with relevant stakeholders. Semi-structured interviews were selected as they allowed for more nuanced insights than focus group discussions[29] Additionally, the semi-structured interviews will follow the four-part process of the MCM tool while providing space to explore interviewees' responses in greater depth. Interviewees from relevant industry, government and civil society organisations whose work focuses on encryption-related issues will be identified through purposive sampling informed by the REA and systematic grey literature review. The limitations of doing interviews through purposive sampling is that they are subject to sampling bias due to the non-random selection of interviewees and findings may be significantly shaped by the availability of interviewees. Further details on the MCM method and interview guide can be found in Appendix 3.

[1] The AACODS – Authority, Accuracy, Coverage, Objectivity, Date, Significance framework was developed by Jess Tyndall as an evaluation and Critical Appraisal Tool for use with grey literature sources. Appraisal (The AACODS Checklist) - Grey Literature in Health - UC Library Guides at University of Canberra (libguides.com)

3

ANALYSIS



3. Analysis

In this section, findings from the desk-based research have been synthesised to identify the various means, justifications and impacts of weakening encryption. Findings from the MCM analysis are also expounded in this section.

3. 1 Findings from Desk-Based Research

The REA identified 28 relevant academic articles in relation to the encryption debate. References for these articles can be found in Appendix 1. Analysis of these articles revealed the following:

- Geographical focus – no articles concerned African countries and only one covered Asia.
- Thematic focus – over 60% of the articles discussed socio-political themes, a quarter were about technical themes and then 13% examined economic themes. This dearth of economic literature reaffirms the economic lens of the research.
- Stakeholder focus – state actors including state legislature, parliament and LEIA made up over 70% of stakeholders discussed, others included consumers, industry and civil society.

Given that the research focuses on economic lens as one of its main themes, the lack of economic literature was resolved by purposively targeting industry stakeholders as potential interviewees. The geographical gap in the REA was addressed by targeting potential interviewees and deliberately searching grey literature sources from a more diverse geographical coverage. The systematic grey literature review process resulted in 57 articles being identified for full analysis. References for these articles can be found in Appendix 2.

3.1.1 Means of Weakening Encryption Technologies

Findings from the REA and systematic grey literature review which discussed means to access or weaken encryption technologies could be categorised into the following means:

Legal Powers to Mandate Exceptional Access to Encryption

The desk-based research revealed legal powers that could be issued to mandate exceptional access to encrypted communications.[30] Academic articles mainly discussed what these legal powers were, whilst findings from the systematic grey literature review referenced more country specific examples. Murphy's article broadly categorised these legal means into four types of legal powers,[31] and these legal powers were discussed by various articles.

The first type of legal power were warrants to intercept communications.[31–33] For example, under Section 15 of the UK's Investigatory Powers Act, a targeted interception warrant authorises the addressed individual or organisation to secure the interception of any communication in transmission and to obtain any 'secondary data' e.g. meta-data.[33]

Technical assistance warrants or technical capability notices (TCNs) were noted as the second type of legal power. Here, TCNs are issued to request or require certain operators to technically assist the retrieval of encrypted communications.[31,34–37] TCNs can accompany interception warrants to ensure that when an interception warrant is issued, the operator has the technical infrastructure in place to provide any assistance relevant to the authorisation.[33]

Equipment Interference (EI) warrants[33,38] were the third legal power discussed, which require communications operators to not just intercept communications, but to collect communications data through hacking measures.[33]

The fourth measure discussed was compelling an individual or organisation to disclose decryption keys to their encrypted communications.[33,36] Under the UK's Regulation of Investigatory Powers Act, 2000, an authorised agent could issue a 'Section 49 Notice' compelling a criminal suspect to disclose their decryption key. Failure to surrender this key upon such demand would subject the individual to a penalty of two years imprisonment.[39] Multiple articles alerted that such compelled disclosure notices could infringe on suspects' right to non-self-incrimination, enshrined in Article 6 of the ECHR.[40,41]

A fifth legal power that was raised in the systematic grey literature review but not mentioned in the academic evidence was imposing import and export controls on encrypted devices.[42] For example, China and Ethiopia continue to impose significant restrictions on the import of any computer programmes or equipment that permit cryptography in order to retain their domestic surveillance capabilities.[42]

Distinction between Explicit and Implicit Legal Powers to Mandate Exceptional Access

The systematic grey literature review identified an interesting distinction between whether the aforementioned legal powers explicitly or implicitly mandated the weakening of encryption. Some powers specifically target encrypted communications, whilst others only imply it.

For example, Article 19's paper discussed legal powers explicitly being used to compel the disclosure of decryption keys. In 2017, Russia's Federal Security Service used the "Yarovaya Package" of laws to request Telegram, an encrypted messaging service provider, to provide decryption keys for six phone numbers.[43] Telegram could not comply with this request as the service uses end-to-end encryption meaning they do not have access to the decryption keys. Resultantly, the Russian Federation blocked access to their services in 2018.[43]

This differs from legal powers that only implied mandated exceptional access to encrypted communications. A Data Governance Network paper explained how India's Information Technology Act mandates warrants to intercept communications and to provide technical assistance.[7] Under Section 69(1) of the Act, the government can direct any LEIA to intercept, monitor or decrypt communications, whilst Section 69(3) requires intermediaries to extend "all facilities and technical assistance" to provide or secure access to the relevant computer resource.[7] However, this Act does not explicitly refer to exceptional access rather it implies it under the broader term of "electronic surveillance".[7]

Similarly, Rwanda's 2016 Information and Communication Technologies law mandates exceptional access without explicitly mentioning encryption.[44] Article 123 imposes an obligation on all service providers and electronic communications networks to "equip" their services with "technical instruments" that allow the lawful interception of electronic communications.[44]

Key Escrow

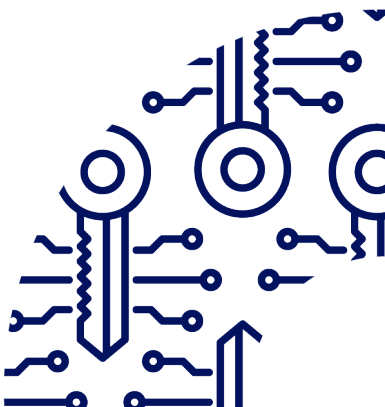
Key escrow was discussed in multiple academic articles.[45–48] This is a technique where a master key to decrypt an encrypted device is held "in escrow" by a trusted party for release to authorised actors in specific instances.[49] The master key can decrypt all ciphertext without permission of its owner.[45] One of the limitations identified in the literature was the 'key escrow problem'. Here, the trusted owner of the master key, could knowingly or unknowingly allow unauthorised access to encrypted data.[45,46] In practice, this increases the attack surface of the encryption system, and creates the possibility for decrypted communications to be repurposed by state actors for uses other than criminal investigation. This in turn abuses the integrity of the key escrow system and threatens user privacy. Resultantly, this technique has waned over time. The key escrow problem was raised during the Clipper Chip proposal. Opponents argued that governments could abuse their power as the trusted key authority to obtain confidential information under the guise of "law enforcement and national security".[47] Due to this inherent flaw, the Clipper Chip initiative was abandoned.[47]

Physical and Cyber-Attacks

Vandenberg's article discussed how encryption can be weakened by attacks on different types of data.[50] Encrypted data at rest could be compromised by physical attacks such as theft of encrypted devices. These stolen devices could be subject to 'brute force attacks' where an attacker tries to break the encryption more quickly using powerful tools. As evidenced by the notorious Heartbleed vulnerability,[50] encrypted data-in-transit protocols, such as SSL/TLS, can also be weakened via 'man in the middle' attacks, which allows plain text to be read. Although the article discussed how these vulnerabilities have been addressed to lessen the impact of these attacks, the capabilities of repressive governments to orchestrate such attacks remains an ever-present threat.

Quantum Computing

Lindsay's article also discussed the future threat of encryption being weakened by quantum computing.[51] It explained that although not fully realised yet, in theory, a fully functional quantum computer could break strong cryptographic protocols and undermine global cybersecurity. However, the coordination needed between technological infrastructure and organisational institutions for it to be widely used by decisionmakers makes this threat unlikely.[51]



3.1.2 Justifications for Weakening Encryption Technologies

The desk-based research indicates that proponents of weakening encryption technologies such as national governments and LEIA, broadly base their arguments for accessing encrypted communications on the Internet going dark.[31]

Criminal Investigations

From the academic evidence, several papers identify criminal investigation as sufficient justification to weaken the use of encryption technologies. While encryption is recognised as being a necessary safeguard to forestall data breaches,[50] state actors view it as an impediment to criminal investigation procedures. Among these procedures include gathering of evidence,[50,52,53] prosecuting criminal offences[40] and preventing or detecting criminal activity.[34,36,45] Criminal activity reported in these papers span organised crime,[38,54,55] drug and human trafficking,[50,54,55] and increasingly with the turn of the century, production and dissemination of child pornography or sexual abuse material (CSAM).[39,41] The prevailing justification to investigate child-related crimes stems from the profusion of new media technologies which can aid the wide distribution of CSAM.[39,41] Overall, a recurring theme across the reviewed papers is the claim by national governments and LEIA that their ability to track and investigate criminal activity is going dark[32,48,52] due to the rising use of encryption technologies.

Similarly, the grey literature echoes the argument that LEIA need elevated access to encrypted communications to investigate and solve crime across diverse geographical locations. These papers[5,8,9] situate the going dark narrative alongside Canadian LEIA's apparent lacking technical abilities to access certain kinds of data. This has led to concerns of LEIAs' ability to "effectively and efficiently carry out investigations".[5] To validate this claim, Canadian LEIA highlighted instances when encryption supposedly stalled investigations. However, this information was deemed insufficient by proponents of strong encryption on the basis that it presented a "one-sided account".[8,56]

Through the Information Technology Act (ITA), Indian LEIA require intermediaries to provide them with access to relevant data based on their "need to ensure accountability for online harms".[7] While in Brazil, WhatsApp has been suspended on several occasions due to the company's refusal to allow LEIA access conversation data pertaining to criminal investigations.[57,58] In its 'Non-Paper on EU Cyber Diplomacy', Germany also appears to adopt an anti-strong encryption stance given its call for "solutions that allow law enforcement and other competent authorities to gain lawful access to digital evidence concerning malicious cyber activities".[59]

Counterterrorism, National Security and Public Safety

Academic papers centre on the going dark argument which LEIA assert interferes with their ability to uphold public safety, preserve national security and effectively counter terrorism.[36,37,47,48,55] For instance, the 9/11 attacks were in part attributed to the terrorists being able to leverage protections afforded by encryption to coordinate plans undetected.[47] Cited in several papers is the more recent 2015 San Bernardino attack for which the United States' FBI unsuccessfully sought Apple's assistance to break into the terrorist's device.[48,50,55] These cases present an argument for governments and LEIA to request lawful access to encrypted content and devices within specified bounds.[53,55]

Whereas certain positions[60,61] advocate a balance between national security and citizen rights, a pro-weakening encryption stance argues that physical security for the larger public must not be subjugated by individual rights. The rationalisation being that such rights can only be enjoyed in a "peaceful and secure" environment.[48]
As noted in these papers,[35,62] the 'Five Eyes' have progressed the exceptional access debate on the basis of combatting terrorism. While New Zealand appears to have adopted a deliberative approach to the subject, Australia and the United Kingdom seem to be the most forceful in pushing for expansive legislation on accessing encrypted communications.[63] Compared to the UK however, Australia has not experienced a high level of attacks by foreign terror groups. The justification for states undermining encryption thus encompasses both domestic and foreign terrorism activity.[35]

The systematic grey literature review highlights how across several regions, state actors explicitly justify access to encrypted communications on the need to preserve national security. It has been argued in India that social media platforms "have a responsibility" to disclose data to LEIA in cases where national security is threatened.[7] According to a 2019 communique issued by the 'Five Eyes', services designed to prevent access to "terrorist and extremist material" endanger citizens and the society.[56] The Green Paper published by the Canadian Government in 2016 also claims "the

increasingly complex digital landscape" justifies the need for investigating national security threats.[9]

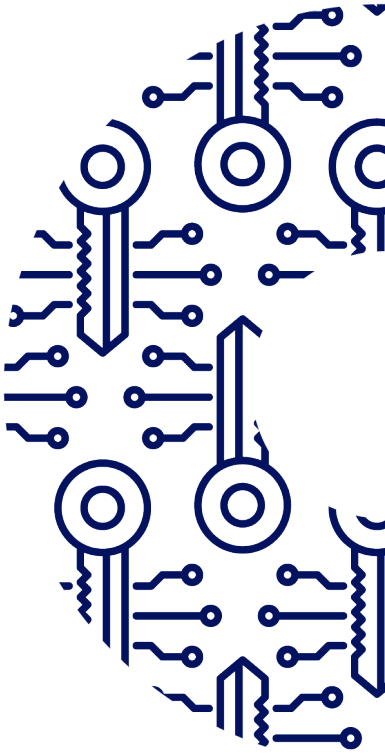
State Surveillance

As revealed in the academic research, countries like the United Kingdom and Germany relied on intelligence acquired through surveillance activities during the second World War. A key factor enabling this success was the ability to decrypt intelligence signals.[51] Following the 2013 Snowden revelations however, state actors sought to undermine the widespread use of strong encryption as it posed a challenge to their lawful surveillance activities.[31,33,52] One restrictive measure proposed was the implementation of 'backdoors' which would enable intelligence agencies to collect vast amounts of data from the public.[61,64]

Private actors like technology companies have been identified as playing somewhat conflicting roles in state actors' drive to widen surveillance reach. Harkens[64] indicates how big data spurred the data economy which has created opportunities for state actors to exploit for surveillance purposes. Conversely, private actors are also noted to complicate lawful surveillance practices through their autonomous implementation of technological changes.[37]

The systematic grey literature review further revealed surveillance-related justifications to weaken encryption. Despite the availability of data and existing surveillance capabilities,[9,56] incidents like the 2015 Charlie Hebdo attacks have influenced state actors to call for "ways to enhance surveillance on the Internet"[42] which effectively undermines encryption. In countries like China, import restrictions on encryption technologies exist to avoid situations where state actors are unable to conduct domestic surveillance.[42]

O'Shea points out that while civil society organisations in Australia assert LEIA have substantial powers to investigate terrorism, the Australian government remains set on acquiring more expansive surveillance capabilities.[65]



3.1.3 Impacts of Weakening Encryption Technologies

Findings from the desk-based research discussed the impacts of weakening encryption according to the defined research lenses: socio-political and economic.

Socio-political Impacts

An impact of weakening encryption argued in the going dark debate is that LEIAs' barrier to accessing information needed for investigations would be lifted. This would be beneficial to LEIA efforts to uphold public safety, as strong encryption often prevents access to data needed for crime and terrorism detection.[1,47,63] While citizens benefit from privacy afforded by encryption, LEIAs see E2EE as a barrier to their investigations and have requested technology service providers to voluntarily develop lawful access solutions,[38] a core argument raised in *Apple v FBI*.[63]

Privacy rights and civil liberties are also impacted by weakening encryption. The academic literature discussed that encryption is recognised as intrinsically bound with rights to privacy, freedom of expression and assembly under the European Convention on Human Rights (ECHR).[4] Throughout much of the academic literature, encryption is seen as a secure and pragmatic safeguard to confidentiality, user control, and targeted state surveillance. The systematic grey literature findings reaffirm human rights violations as a significant impact of weakening encryption. Similar themes of freedom of expression and the right to privacy. Conversely, the impact on the right to non-self-incrimination was only indicated in the grey literature. Additionally, most of the academic findings were confined to countries from the Global North, whereas the systematic grey literature review included broader geographic representation.

Vulnerable communities are disproportionately impacted by weakening encryption. Strong encryption provides confidentiality which allows people to associate online based on identities or beliefs that are illegal in some countries. Many scholars have voiced concern that vulnerable populations like the LGBT community or domestic violence victims depend on secure communications afforded by encryption, to establish trust, privacy, and safety online.[66] Consequently, weakening encryption presents an infringement of civil liberties, exposes identities of these vulnerable groups and causes them to fear prosecution and persecution.[37,39,60] While LEIAs continue to cite the difficulty encrypted communications pose to criminal investigations, expressing one's sexual identity is considered a criminal offense in many countries.[66] Without encryption, vulnerable individuals living in or traveling to these countries may not be able to safely and comfortably find communities and outlets for self-expression.

Another impact of weakening encryption noted in the literature is the potential for state actors to abuse exceptional access to surveil journalists, activists and whistle-blowers who speak out against government. The targeting of encryption and anonymity tools by authoritarian governments during social and political unrest has become an increasingly common tactic to undermine freedom of expression, assembly, and peaceful protest.[67] Therefore, weakening encryption would threaten the protection of dissidents from state power, particularly those in authoritarian regimes where online censorship or mass surveillance remains prevalent.

Economic Impacts

Encryption is critical for e-commerce, online banking, and digital services to secure their communications and financial transactions on the Internet.[37,60,64] Scholars have therefore highlighted that the economic impacts of weakening encryption are costly.[64] Infrastructure requirements for backdoor access have been argued to have adverse economic effects. For example, under the Australian Telecommunications and Other Legislation Act (TOLA), LEIA can compel a wide range of communication providers to provide access to encrypted data.[5] Yet this sharing of confidential company information poses significant threats to reputation, digital security, and most importantly trust online. Moreover, the literature expressed that the economic costs of weakening encryption provide the illusion of protection while actually crippling the economy.[47]

3.1.4 Causal Loop Diagram

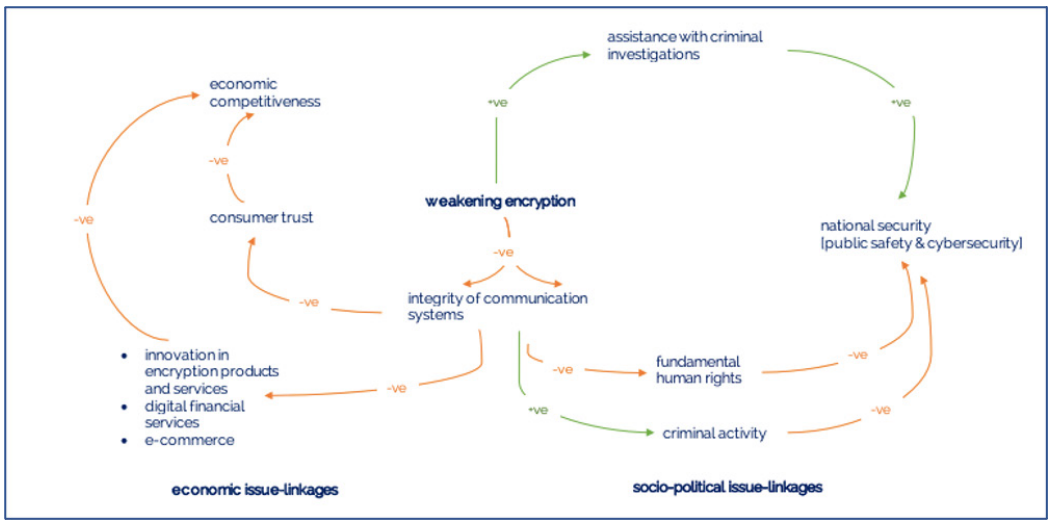


Figure 2: Causal Loop Diagram

Based on the evidence gathered from the desk-based research, the above CLD (Figure 2) was mapped to understand the issue-linkages present in the encryption debate. The left loop of the CLD maps the economic impact of weakening encryption. When encryption is weakened, it affects the integrity of the communication systems as the data no longer has the protection that encryption avails. Consequently, consumers are less likely to be drawn to using products that are not able to provide the highest form of protection, especially with regards to financial services. As consumers shift towards other services that can provide encrypted services, the economic competitiveness of the services is negatively affected. In a similar vein, when encryption is weakened, innovation in encrypted technologies is likely to be stifled as innovators are not incentivised to develop the most secure products and services. E-commerce, which is attributed to nearly a fifth of total global retail sales, will be negatively affected as online financial transactions rely on encryption. In sum, the economic impact is negative.[68]

The right loop of the CLD maps out the impacts of weakening encryption through a socio-political lens. When encryption is weakened, it negatively affects the integrity of communications systems as it is not possible to know if communication has been tampered with or has been intercepted by a third-party. When the integrity of communication systems is compromised through the weakening of encryption, it negatively affects national security as there is a greater risk of cybersecurity threat from malicious actors who can exploit vulnerabilities to access critical infrastructure.

Additionally, criminals can take advantage of vulnerabilities to commit crimes which can lead to an increase in criminal activity which negatively affects national security.

With regards to individual users, it also compromises the fundamental human rights as their private communications can be susceptible to interception, leading to greater surveillance by state actors. The only positive dynamic is that the access to communications gained through weakening encryption might assist LEIA in solving criminal investigations and consequently improve national security. Thus, it appears that the negative impacts from weakening encryption are significantly greater than the positive benefits. It should be noted that the CLD does not depict the magnitude of the impacts of weakening encryption, however these are further discussed and qualified in the Impact Assessment (Section 4.1).

3.2 Findings from Primary Research

Based on the findings from desk-based research, three core options were developed for participants to appraise during the interviews for the MCM. While the MCM tool allows for the creation of additional options by participants, this research was limited to these core options to avoid prolonging interview sessions. The options are explained as follows

Option 1: Restrict encryption technologies through technical means
Entails overt or direct technical interference by state actors to decrypt encrypted data or communications. Examples include using a key escrow system whereby service providers or Internet intermediaries are required to store copies of decryption keys with state-appointed third parties. The possibility that encryption may be weakened in the future using new technologies like quantum computing is also noted.

Option 2: Restrict encryption technologies through non-technical means

Implies state actors employing indirect means to access encrypted data and communications. Examples include governments issuing mandates for compelled disclosure of decryption keys, warrants requiring technical assistance from service providers and fines if this assistance is not provided. Other non-technical means include import/export controls restrictions on encryption technologies.

Option 3: Do not restrict encryption
Neither technical nor non-technical means should be employed to restrict use of encryption technologies.

17 stakeholder representatives comprising civil society, industry and policymaker organisations from Africa, Asia, Europe, United Kingdom and United States participated in the interviews. Interviews were conducted from 12th – 28th July 2021. Involved in the interviews, were 13 civil society organisations that included digital rights, multilateral, and thinktank groups. Three interviewees provided industry perspectives covering encrypted messaging and financial services, while a single interviewee represented the policymaker category. As reflected in Table 1, representation from policymakers was limited given the sensitivities around the encryption debate. As a result, the primary research findings were influenced by the composition of interviewees. It should be noted that the findings are not representative of broader stakeholder group views.

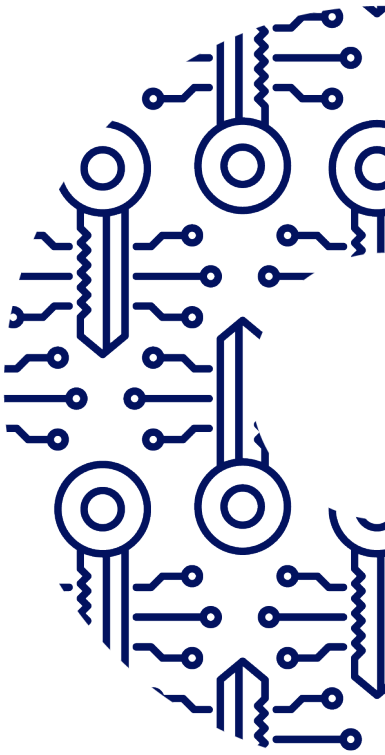


Table 1: Details of Interviewees

S/No	Organisation	Stakeholder Group	Location
1	Access Now	Civil Society	India
2	Carnegie Endowment for International Peace	Civil Society	United States
3	CIPESA	Civil Society	Uganda
4	Digital Empowerment Foundation	Civil Society	India
5	European Digital Rights	Civil Society	Belgium
6	Future of Privacy Forum	Civil Society	Belgium
7	Global Partners Digital	Civil Society	United Kingdom
8	IT for Change	Civil Society	India
9	LGBT Tech	Civil Society	United States
10	Open Rights Group	Civil Society	United Kingdom
11	Paradigm Initiative	Civil Society	Nigeria
12	Safer Internet Forum	Civil Society	United Kingdom
13	Software Freedom Law Centre	Civil Society	India
14	Encrypted financial services provider	Industry	United Kingdom
15	End-to-end encrypted messaging service provider	Industry	United States
16	ProtonMail	Industry	Switzerland
17	Open Governance Network for Europe	Policymaker	Belgium

3.2.1 Qualitative Coding of MCM Data

The MCM process began with each interviewee providing their initial thoughts on the three options scoped for appraisal. Thereafter, they were asked to share factors they considered important in evaluating the options, as well as descriptions of what these factors meant. Using a scale of 0-100, interviewees then scored each option for both best- and worst-case scenarios, under every defined factor. The MCM tool provides for scoring best- and worst-case scenarios to enable interviewees to reflect on a range of considerations before concluding on appropriate scores. This also allowed interviewees to contemplate points of uncertainty while appraising these options.[69]

The process concluded with interviewees assigning weights to each factor based on how they perceived its relative importance, which summed to 100. Using normalised weighted scores, the MCM tool then generated rankings for the options across each interviewee.

In total across all the 17 interviewees, 66 factors were raised. By conducting a qualitative coding process[1], the 66 identified factors were synthesised into 11 codes and 33 subcodes of factors (Table 2). More information on the coding process can be found in Appendix 4.

Table 2 Identified Codes and Subcodes of Factors

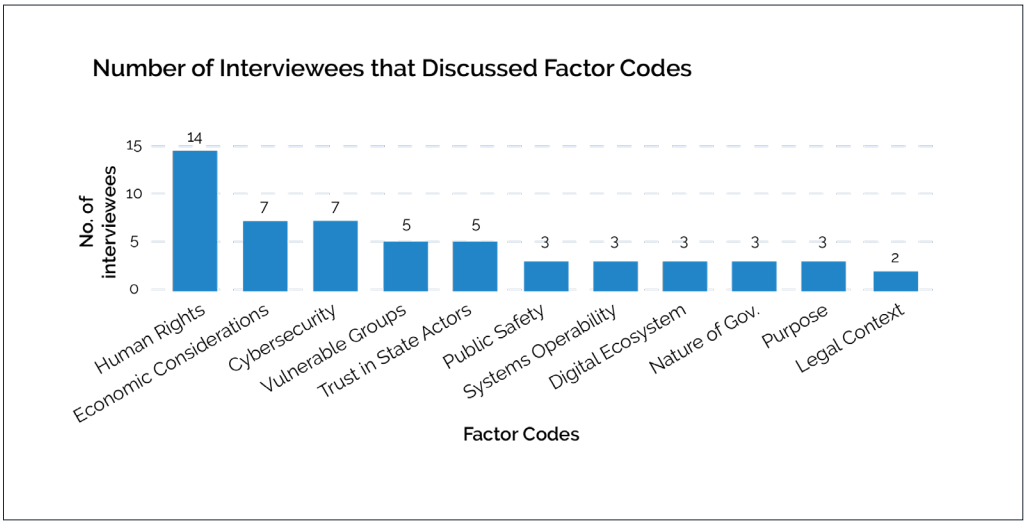
Code of Factors	Description of Code	Subcodes	Mentioned by Stakeholder Group
1- Distributional Impacts on Vulnerable Groups	Impact of weakening encryption on the safety of vulnerable groups in society.	Vulnerable populations (generally)	Industry, Civil Society
		Safety of activists	Civil Society
		LGBT community	Civil Society
2- Human Rights	Rights of individuals that are enshrined in various legal frameworks such as the Universal Declaration on Human Rights and the European Union's Lisbon Treaty.	Fundamental human rights (generally)	Civil Society, Policymaker
		Right to privacy	Industry, Civil Society
		Digital rights (human rights faring in digital realm)	Civil Society
		Freedom of expression	Industry, Civil Society
3- Economic Considerations	Impacts of weakening encryption on industry.	Innovation and choice for consumers	Civil Society
		Consumer trust in encrypted products	Industry, Civil Society
		Commerce and economic competitiveness	Industry, Civil Society
4- Public Safety	Impacts of weakening encryption on public safety and ability of LEIAs to access communications to prevent crimes.	Proactive scanning to detect CSAM	Civil Society
		Ability for LEIAs to access encrypted data for public safety purposes	Industry, Civil Society
		Ability to support victims	Civil Society
5- Systems Operability	Ability for systems to continue running smoothly if encryption is weakened, both technically in terms of the operability of software systems, and non-technically regarding the ability to for companies to comply with government mandates.	Technically (operability of systems)	Industry, Civil Society
		Non-technically (compliance with mandates)	Civil Society
		Ease of use	Civil Society
6- Impact on Digital Ecosystem	Impact of weakening encryption on the universal digital ecosystem.	Impact on digital ecosystem and regressing technology	Civil Society
		Lawless online spaces	Civil Society
7- Nature of Government	The political context of a country.	Political pressures	Policymaker
		Historical context	Civil Society
		Precedent	Civil Society
		System of government	Civil Society

[2] Qualitative coding involves identifying general themes from data collected. The coding conducted was 'open coding', where the themes were constructed and grouped from the bottom-up, directly informed by the interviewees' responses.[69]The coding was also done iteratively, moving between broader issues and more specific issues as more explicit themes emerged and as codes were refined.[69]

Code of Factors	Description of Code	Subcodes	Mentioned by Stakeholder Group
8- Trust in Government/State Actors	The possibility of trust in state actors being abused if issued with powers of weakening encryption. Includes abuse of backdoors or lawful access to increase state surveillance.	Abuse by governments	Industry, Civil Society
		Abuse by LEIAs	Industry, Civil Society
		State surveillance	Civil Society
9- Purpose/Use Case for Encryption	Weakening encryption must be justified based on a specific use case rather than a general argument. Purpose needs to adhere to necessity and proportionality principles for it to be legal (based on the European Charter of Fundamental Rights article 52(2)).	Necessity	Civil Society
		Proportionality	Civil Society, Policymaker
		Need for appropriate data retention policies	Civil society
10- Legal Context	Legal context of a region.	Effectiveness of encryption related legislation in a region	Policymaker
		Existing legal landscape of a region (regarding data governance, safeguards to protect citizens and prevention of abuse by state actors)	Civil Society, Policymaker
11- Cybersecurity	Impact of weakening encryption on cybersecurity and cybercrime.	Systems integrity (undermining security of systems that rely on encryption if security and data protection is compromised)	Industry, Civil Society
		New vulnerabilities created by backdoors increasing the attack surface exploitable by bad actors	Industry, Civil Society
		Increase in cybercrime	Industry, Civil Society

Analysis of Codes across all Interviewees

Figure 3: Number of Interviewees that Discussed Factor Codes



These codes were analysed according to the themes that emerged the most across all interviewees (Figure 3). The most discussed code was *Human Rights*, mentioned by 14 out of 17 interviewees as a factor to consider when making encryption-related policy options. Within this, fundamental human rights including the right to privacy, the right to freedom of expression, and digital rights were discussed. A representative from *Software Freedom Law Centre* considered how these rights are enshrined in international frameworks:

> The fundamental right to privacy, and the anonymity it provides is enshrined in the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR)...Encrypted communications provide anonymity and privacy to citizens, for examples journalist talking about corruption.

Another frequent code raised by seven interviewees was *Economic Considerations*. Interviewees considered the implications that encryption policies could have on industry. This entailed innovation and choice for consumers, consumer trust in encrypted products, and economic competitiveness. The prevalence of this code across interviews is notable given its underrepresentation in the desk-based research.

A less frequently mentioned but important code was *Purpose*; that weakening encryption and consequently infringing on human rights such as privacy must be justified by a defined use case.

Interviewees stressed the importance of this factor, as not adhering to a specific purpose allows misuse to occur. For this reason, under article 8 of the ECHR, any infringement of human rights must pass a proportionality test; the interference must not exceed anything that is necessary to achieve its aim.[70] A representative from the *Future of Privacy Forum* echoed this:

> [Any] weakening of encryption needs to be necessary and proportionate in society... By encryption restrictions having a general purpose it enables them [these restrictions] to be applied to so many other cases. For instance, it allows for misuse when no longer proportional and necessary. It is essential to review weakening encryption measures over time to see if the use case argument for encryption still stands and is necessary.

3.2.2 Results of MCM Analysis

Analysis of the MCM data proceeded with a high-level categorisation of all 17 interviewees into three stakeholder groups (hereafter named perspectives) to reflect their individual viewpoints i.e., civil society, industry, and policymaker. Following that, the 66 factors mentioned by interviewees were grouped according to each perspective. Finally, the three options were categorised into one cluster. These steps were required to be performed on the MCM tool to enable various analyses of the quantitative and qualitative data collected during the interviews. Results from the MCM analysis of interviewees' responses are organised into ranking and weighting sections. Ranking shows how interviewees evaluated the three options while weighting provides details of the relative importance interviewees assigned to factors in evaluating these options.

Overall ranking of options

In the overall options ranking chart (Figure 4), dark blue lines reflect the variability of interviewees' ranking of the options, with the left and right ends indicating the lowest and highest ranks respectively. The light blue bars show the distribution of rank means, with higher values indicating better performance and lower values showing worse performance. [69] From interviewees' overall ranking of the options, *Option 3: Do not restrict encryption* has the best performance with means values[3] ranging from 57 to 95. This indicates interviewees generally considered Option 3 as the optimal one. The overlap noted in Options 1 and 2 is due to interviewees considering both options as the same. Nevertheless, collective interview responses rank Option 2 higher than Option 1.

Analysis of individual rankings for each perspective reflects similar patterns to the summary ranking (Figure 5). However, given that the civil society perspective comprises over 75% of the interviewees, its chart is most closely aligned with the overall ranking chart (Figure 4). Unlike the rankings charts for the civil society and industry perspectives, the policymaker chart has no ranges as it represents findings from only one interviewee. Each interviewee perspective is further explained in the subsequent sections.

Rankings by Civil Society Perspective

11 out of 13 interviewees in this perspective preferred Option 3. Reasons for this preference comprised protection of rights such as privacy and freedom of expression, protection of vulnerable groups and enabling trust in the digital ecosystem. Option 2 was most preferred by one of the other two interviewees who did not select Option 3. Responses from this interviewee are reflective of their interests which entail protecting child rights online. For instance, the interviewee said if Option 2 were implemented correctly, it would be "less vulnerable to abuse by bad actors" and enable LEIA to "detect criminal activity". The other interviewee however did not think there was any distinction between Option 1 and 2, as implementing the former depends on procedural safeguards to prevent LEIA from abusing the privilege of exceptional access. In addition, they thought not restricting encryption would create a "societal problem" of being unable to curb crime and terrorism. Contrasting rankings within this perspective thus highlight the tension between individual rights and public safety. See Appendix 6.1.1 for individual ranking charts for this perspective.

Rankings by Industry Perspective

As two of the three interviewees in this perspective offer encrypted communications services, they both ranked Option 3 as their most preferred. The ProtonMail interviewee mentioned strong encryption was necessary for privacy. They however acknowledged that there are limits on private communications, as meta-data like geolocation, device identifier information, and time which can be linked to a person's identity are generated during these communications. Similarly, the other messaging service provider did not see a distinction between Options 1 and 2, so both were ranked similarly. While they stated E2EE preserved privacy, they admitted that it could be violated through other methods as "E2EE is not a complete solution to privacy". Their responses also indicated that by not restricting encryption, LEIA may be hindered in upholding public safety, highlighting the conflict between individual privacy and public safety.
Rankings for the third interviewee, a financial services provider, were markedly different from the others and do not show a clear preference. This could be explained by the services they provide which are subject to regulation, and the type of encryption they use. For instance, a subpoena may be issued for them to disclose financial statements of an individual under investigation which they must comply with as a regulated institution. However, because they rely on encryption to secure customers' transactions, they are "averse to [the] deliberate weakening of

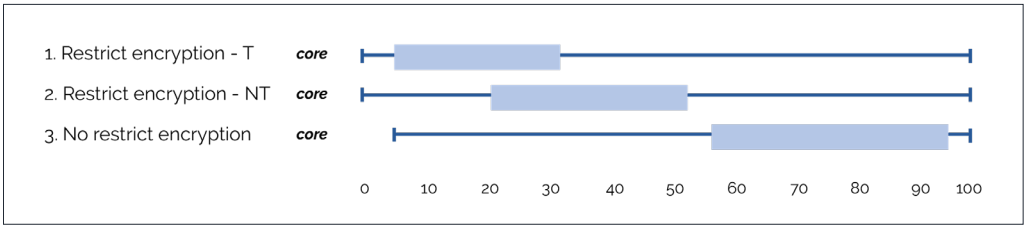


Figure 4: Summary Ranking of Appraised Options across all Perspectives

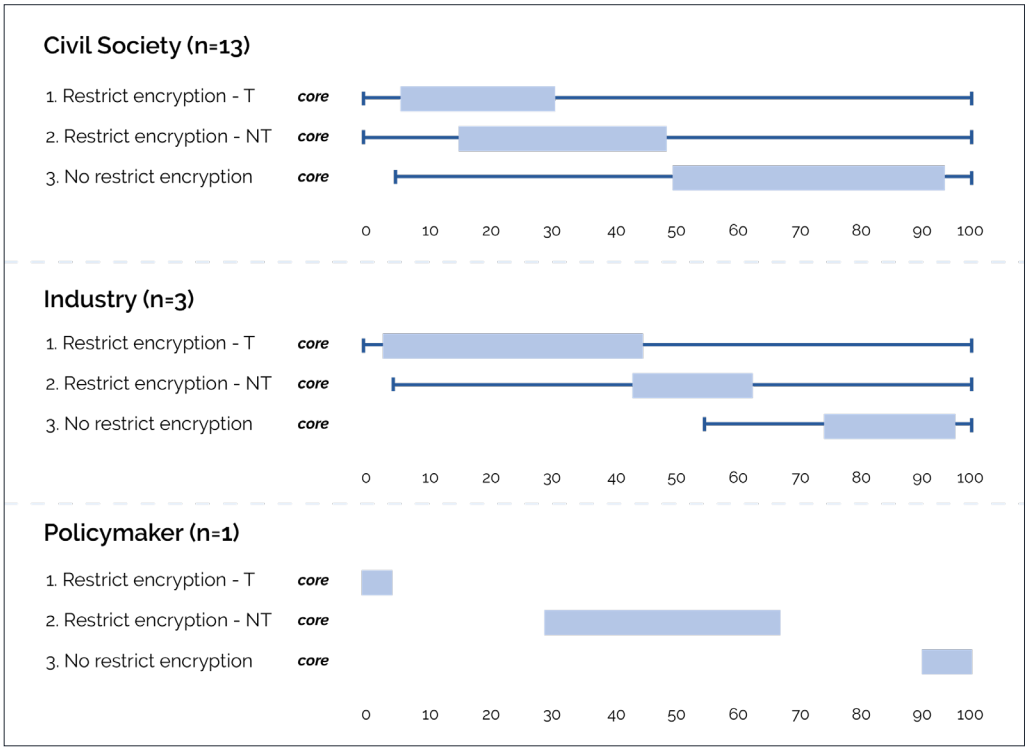


Figure 5: Rankings of Appraised Options by Individual Perspectives

encryption through technical backdoors". In sum, this perspective highlights different applications of encryption technologies. See Appendix 6.1.2 for individual ranking charts for this perspective.

Rankings by Policymaker Perspective

The interviewee in this perspective ranked Option 3 as their most preferred. Among reasons given for this are deepened awareness and protection of "fundamental rights, society and markets". Their responses also indicated that the European Union's (EU) position to improve security by restricting encryption was contradictory. Contrastingly, they stated that not restricting encryption could amplify existing negative externalities like disinformation and hate speech. This feedback thus reflects the multi-layered nature of the encryption debate. See Appendix 6.1.3 for ranking charts for this perspective.

Weighting of issues

To understand the relative importance each interviewee gave to the 66 factors, weights charts were plotted on the MCM tool using the 11 codes of factors defined in section 3.3.1. In line with the tool's configuration, the codes of factors were created as issues on the MCM tool and are reflected on the vertical axes in the weighting charts (Figures 6-8).

Similar to the ranking charts, light blue lines in the weighting charts reflect the weight ranges from lowest to highest related to a specific issue, across a selection of interviewees. For instance, the left-sides of the lines indicate the sums of all weights attached to factors in any issue by interviewees for whom these weightings were lowest, while the right-sides represent the highest issue weightings. The dark blue markers show the mean values of weightings for a selected issue across a given perspective. Where there are no ranges (i.e. light blue lines), only one interviewee provided a factor for the related issue which others did not define.[69] Figure 8 clearly illustrates this point as the policymaker perspective contains only one interviewee.

Issues weighted by Civil Society Perspective
The civil society chart (Figure 6) shows that while the highest number of weights were assigned to *Human Rights* and *Public Safety, Purpose* had the most significant weights allocated to it. Factors categorised in *Impacts on Society Groups* and *Trust in Government/State* are among those with the lowest mean weights. Interestingly, only one interviewee considered *Public Safety* important. As an advocate of online safety for children, their justifications were based on enabling proactive scanning to detect CSAM and accessing information required to provide timely support to victims of cyberbullying. When faced with dire situations, they believe safeguarding lives outweighs "privacy and anonymity". Consequently, privacy and anonymity are considered least important to this interviewee.

robust legal frameworks assures individuals the opportunities to seek redress if their rights are violated. Only two of the 13 interviewees recognised digital rights as independent from human rights, with one *(Open Rights Group)* indicating how rights applicable offline should also be recognised online. Conversely, one interviewee admitted a difficulty in delineating digital rights from offline rights, given that the Internet enables basic rights such as access to education and healthcare.

A closer analysis of issues with low weightings like *Impacts on Society Groups and Trust in Government/State* revealed interesting insights. While three respondents acknowledged the need to protect vulnerable groups, two of the three allocated low weightings to this issue.

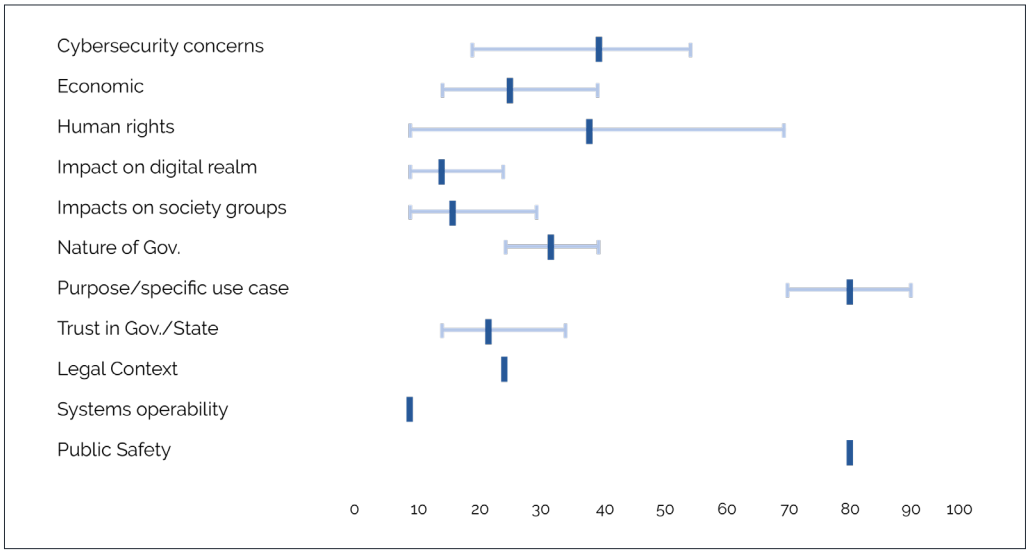


Figure 6: Weighting of issues for Civil Society Perspective

An analysis of factors under *Purpose* showed interviewees rationalised their weightings on insufficient clarity on the specific purposes that justify the need to weaken encryption. A lack of purpose for weakening encryption could therefore create potential opportunities for misuses to occur. Other statements supporting these weightings mention providing clear objectives for weakening encryption and a strong requirement that proposals to weaken encryption must pass proportionality tests before they are considered legal.

Apart from one interviewee *(Paradigm Initiative)*, every interviewee in this perspective provided weightings for factors under *Human Rights*. However, a closer analysis of this exception showed their responses indicated a rights-respecting legal landscape enables individuals to defend themselves when necessary. To them, prioritising the establishment of fair and

One (*CIPESA*) rationalised their low weighting as being dependent on privacy (which they considered most essential) and their advocacy work which is broadly concerned with the state of the Internet. Another interviewee *(LGBT Tech)* however, gave a higher weighting to this issue which can be explained by the unique dangers faced by the LGBT communities who rely on the privacy and confidentiality afforded by encryption to communicate safely. As LGBT communities are criminalised in certain jurisdictions, LEIA may view this as an opportunity to access their encrypted communications.

Similar patterns were also observed under *Trust in Government/State*. In contrast to other interviewees whose maximum weighting was 25, only one interviewee *(Paradigm Initiative)* assigned a weighting above 30. This interviewee justified their decision by recognising a breach of trust as being at the centre of the weakening

encryption discussion. They elaborate this position with an example of choosing not to obtain a National Identification Number until the Nigerian government implements requisite safeguards. Justifications provided by other interviewees include governments leveraging the encryption debate to serve other interests beyond national security and for overextended surveillance powers. Overall, trust is critical to enabling citizens' safe and secure communications. For further details on interviewee comments see Appendix 6.3.1.

Issues weighted by Industry Perspective

Of the 11 issues defined, industry interviewees considered seven important for weighting and excluded the others (Figure 7). Although more factors were weighted under *Public Safety*, it was not weighted as high as *Economic and Cybersecurity Concerns*. *Human Rights*, *Public Safety* and *Impact on Society Groups* were among the lowest weighted issues for this perspective. The two interviewees who weighted factors under *Human Rights* explained that strong encryption is an enabler of rights like privacy and freedom of expression.

One interviewee *(ProtonMail)* did not provide weightings under the *Economic* issue. A closer review of their overall responses indicates customer-related needs are prioritised over business concerns as they consider security and privacy more important. For the second industry interviewee, the ability to offer a product with encrypted messaging capabilities provides competitive advantage. They further state that selectively creating backdoors on their platform has possible negative implications for the wider customer base. With the rise in digital financial services,[71] assuring customers their transactions are confidential is central to remaining competitive in the industry as indicated by the encrypted financial services provider's responses. Collectively, interviewees expressed a link between upholding consumer trust (by offering secure services) and being economically viable.

On *Public Safety*, one interviewee admitted the inability of LEIA to access encrypted communications on messaging platforms may be detrimental to the public. However, this consideration is offset by their assessment of other factors some of which significantly

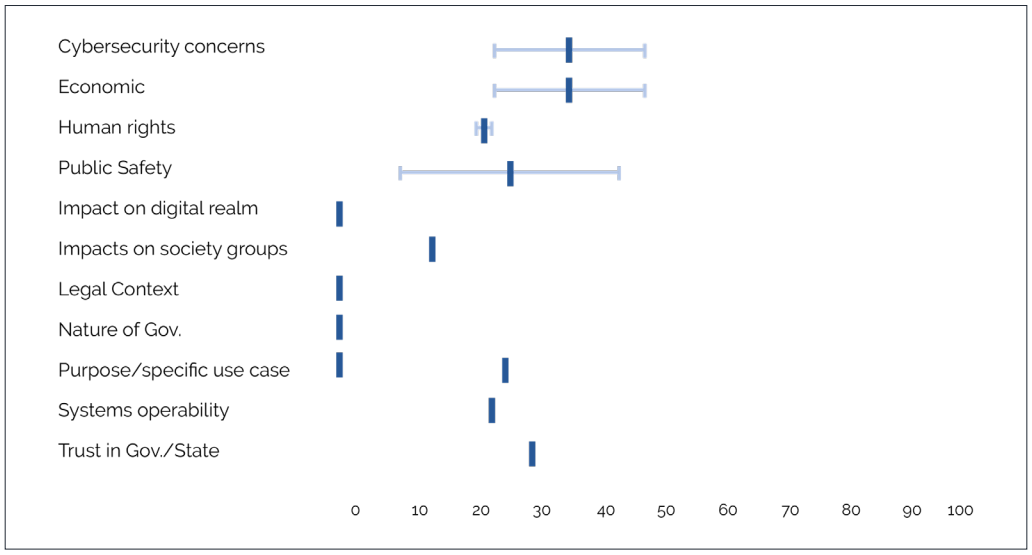


Figure 7: Weighting of issues for Industry Perspective

Analysis of industry interviewees' responses showed the highest weights were given to *Cybersecurity Concerns*. From the financial services perspective, one interviewee justified their weighting on ensuring safety and security of customer transactions. The need to minimise attack surfaces and protect their users and platform, were reasons provided by the leading encrypted instant messaging service interviewee for prioritising cybersecurity. These responses reflect customers' reliance on encrypted services to safeguard their privacy.

outweigh public safety. In fact, public safety is the least weighted factor for this interviewee. Another interviewee *(ProtonMail)* viewed *Public Safety* through two lenses. The first lens indicated LEIA's improved chances at detecting criminal activity, however this position was thought unlikely given that LEIA capabilities may not be well-funded. Similar to the first interviewee, this factor was considered the least important. The second lens suggests that the security of individuals may be widely compromised if encryption technologies are weakened, as there would be "large scale

content surveillance". In sum, interviewees tended to not view public safety in a vacuum, rather they considered it alongside other important factors. For further details on interviewees' comments see Appendix 6.3.2.

Issues Weighted by Policymaker Perspective
The policymaker interviewee weighted only four of the 11 issues analysed (Figure 8). Similar to the civil society perspective, *Purpose* and *Human Rights* were deemed to have the highest weights. For this interviewee, *Human Rights* is most important as encryption enables the protection of these rights. Likewise, *Purpose* is weighted highly as the interviewee regards the element of proportionality as being "the overarching and primary basis for any direction that legislation needs to be based upon". They further qualified their weightings around there being insufficient evidence to conclusively indicate that encryption hampers LEIA's ability to solve crime. Although *Legal Context and Nature of Government* carry the least weights, this interviewee rationalised their decision on these being dependent on the existence of *Purpose.*

Regarding *Legal Context*, this interviewee identified two main problems the EU faces in the encryption debate. First, LEIAs experience constraints to confront the challenges "in an increasingly encrypted environment". In addition, diverse legal frameworks across the EU complicate effective resolution of cross-border encryption-related issues. Without resolving these, "it would be difficult for EU LEIA to apply a consistent [legal] framework". Their responses under *Nature of Government* indicated the ongoing encryption debate is narrowly focused and overstates "criminality" at the expense of other societal problems; a position that is also reflected by the industry perspective noted in the previous section. They also highlighted the concern of less democratic states adopting restrictive encryption legislations if the EU is seen to endorse them. For further details on interviewees' comments see Appendix 6.3.3.

Although individual perspectives presented factors distinct to each group, in several areas factors tended to overlap across the groups thus showing the complex nature of the encryption debate. Finer details of these analyses and resultant implications are explored in the discussion section.

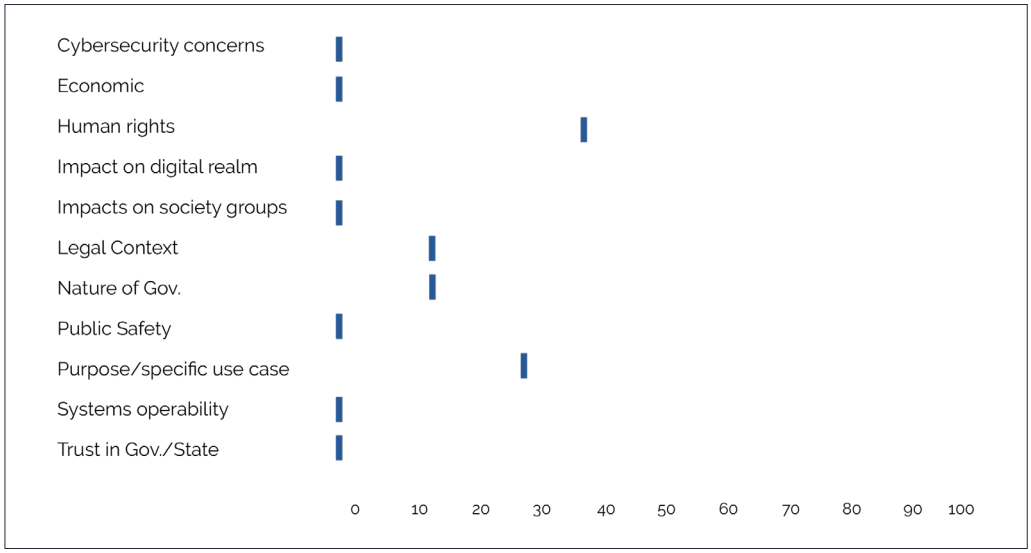
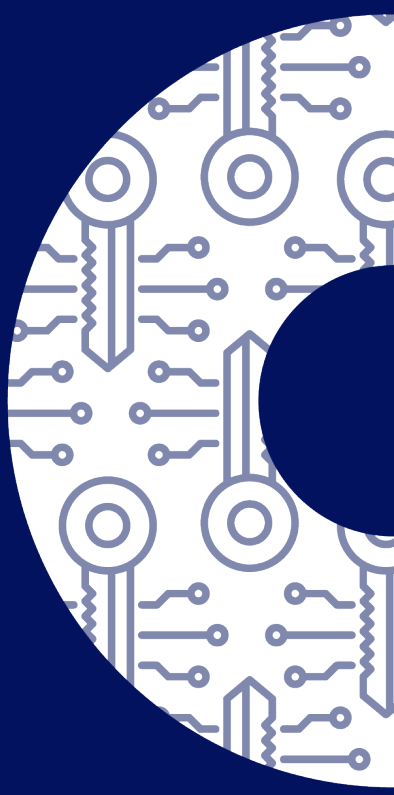


Figure 8: Weighting of issues for Policymaker Perspective

4

DISCUSSION



4. Discussion

Drawing on the above analysis, this section will explore the implications of the findings by developing an Impact Assessment and a Decision-Making Framework. The IA is a collective evaluation of the risks and benefits of weakening encryption that policymakers should be aware of. The DMF intends to guide policymakers in the encryption debate by positing questions for them to consider when making encryption-related decisions.

4.1 Impact Assessment

The purpose of the IA is to assess the socio-political and economic impacts of weakening encryption. Informed by the desk-based and primary research, the IA builds on the benefits and risks illustrated by the CLD to evaluate the magnitude of these impacts.

4.1.1 Benefits of Weakening Encryption

Socio-political benefits

National Security and Public Safety

The main argument for weakening encryption proposed by LEIA is to protect national security and public safety. This is rooted in the going dark narrative that encryption acts as a barrier to LEIA accessing encrypted data for investigative purposes.[1] A civil society interviewee claimed that "E2EE poses challenges for what information can be passed onto law enforcement, and what information can be used to interrogate the concerned parties and finding these individuals… E2EE obfuscates that". Following this reasoning, weakening encryption would remove this barrier and enable LEIAs to access encrypted data to help solve criminal investigations, particularly those regarding terrorism or CSAM.[1] An additional benefit identified by the interviewee was that restricting encryption would help to provide better support for victims who have been abused on encrypted communication platforms, such as cyberbullying helplines that "can intervene and work with platforms…to provide evidence to law enforcement". these impacts.

However, this benefit could be thwarted as weakening encryption could undermine national security.[52,60] Weakening encryption through backdoors creates new vulnerabilities in data security, which increases the attack surface for bad actors to exploit, leaving systems vulnerable to attacks that threaten national security.[52,60] This formed the basis of Apple's refusal to create a backdoor into an iPhone as requested by the FBI to access personal information relevant to the 2015 San Bernardino shooting.[60] Apple stated "[we] would do our best to protect that key, but in a world where all of our data is under constant threat, it would be relentlessly attacked by hackers and cybercriminals".[60] Thus, weakening encryption to improve national security and public safety is counterintuitive.

Additionally, this benefit to national security and public safety is minimised by the fact that increasingly, LEIAs can access data through means other than weakening encryption. The research revealed government hacking as a potential solution to the going dark debate, as it offers necessary access to communications for law enforcement purposes, without weakening encryption.[39–43] Government hacking refers to the exploitation of existing vulnerabilities in software and hardware by state actors to access data in transit and data at rest.[72] A successful case of this was Operation Pacifier by the FBI in 2015, where vulnerabilities in the Tor browser were exploited to identify users of the child pornography portal, Playpen.[72] This identified 8,000 computers that had been used to access the portal in 120 countries.[72]

However, government hacking comes with its own set of challenges such as a need for clearly defined legal standards and use frameworks, especially to determine whether the method of obtaining evidence can be disclosed in court.[74] Despite these challenges, government hacking presents a counter to the claim that encryption should be weakened to benefit public safety, as LEIAs can access encrypted data without having to weaken encryption.

Prioritising Life

According to Diab, proponents of weakening encryption on the grounds of 'moral necessity' argue that in 'ticking bomb' scenarios like terrorist attacks, the trade-off of weakening encryption is not between data privacy and law enforcement, but between data protection and human life. [9] In such instances, the justification to weaken encryption should value human life over dignity or privacy.[9] They argue that encrypted data could serve as a unique data source that LEIA might need to thwart an incoming terrorist attack.[9] In doing so, weakening encryption prioritises and protects human life. It is important to note that although a consequentialist benefit, the likelihood of this trade-off between data protection and human life occurring is extremely improbable. This argument is further counteracted by the multiple risks created by weakening encryption as detailed in section 4.1.2.

4.1.2 Risks of Weakening Encryption

Socio-political risks

Cybersecurity
Weakening encryption creates several risks to cybersecurity protection, including data loss, and theft. Findings suggest that LEIAs' requests for backdoor access, often result in compromised endpoint systems, creating several new vulnerabilities to the global Internet infrastructure that could be exploited by bad actors.[72] These exploitations could undermine the integrity and security of systems that rely on encryption, and could lead to increased cybercrime activity. One civil society interviewee mentioned that *Option 1: Restricting encryption technologies through technical means*, "would lead to increased vulnerabilities, increased attack surfaces and increased cyber-attacks. This further complicates cybersecurity efforts for security specialists."

Additionally, many businesses and organisations actively rely on encryption to protect consumer privacy and sensitive data in order to ensure user security.[10] Weakening encryption on these services therefore reduces data security which affects consumer trust. Threats to personally identifiable information (PII) such as confidential medical history, continue to be exploited by malicious actors, hacktivists, and state-sponsored attacks.[64,66] Therefore, weakening encryption poses risks to cybersecurity.

Divergence from International Norms and Legal Precedent
There is a prominent risk that a nation implementing legislation to weaken encryption could diverge from international legal and human rights norms. An interviewee from the *Open Rights Group* stated that:

> Privacy and freedom of expression are upheld internationally in the legal context. With the UK considering potentially intrusive legislation, it risks moving away from universally agreed norms and standards. Basically, the UK cannot take a standalone position in the larger global context…The Online Safety Bill could jeopardise the UK's status amongst the group of nations that adhere to human rights internationally. The 1948 UN Charter has always been incorporated into UK domestic law and has extensively shaped a lot of Internet laws and regulations. This charter enshrines privacy and freedom of expression in a legal context.

Additionally, passing such legislation could set a precedent for weakening encryption which could be abused by repressive states. The same interviewee continued by saying that "Implementing [Option 1] could inspire less democratic states to do the same; essentially causing a fallout with negative global consequences". The interviewee from Paradigm Initiative also mentioned that legislation and misuses of restricted encryption could occur in countries where the executive flouts judicial procedures. Therefore, weakening encryption risks creating a potentially dangerous legal precedent and diverging from international norms.

Transnational Cooperation
National laws that weaken encryption could cause complications for transnational practice by creating an inconsistent legal landscape. Weakening encryption via national laws would create potential conflict of legal requirements, particularly for transnational technology companies who would struggle to comply with contrasting encryption laws in different countries.[35,75] Differing laws across countries could also complicate treaties that facilitate transnational law enforcement cooperation, such as mutual assistance treaties.[76] The policymaker interviewee noted that mutual legal treaties across EU member states are weak, as

> Legal frameworks apply differently and are currently not designed to resolve cross-border issues stemming from encryption… Without increased capacity to understand the implications of encryption legislation, it would b e difficult for EU LEIA to apply a consistent framework and enforce such legislation.

It was additionally discussed that inconsistent legislation and agreement across these mutual assistance treaties could have international implications by "creating more loopholes for violations". The literature echoed this point, discussing how this could lead to 'jurisdiction forum shopping', a term for purposefully collaborating with overseas LEIAs as a way of circumventing national rules relating to the conduct of an investigation.[32] This was raised when 'Five Eyes' member Australia in December 2018 passed legislation that permitted law enforcement to issue technical assistance and capability notices to communication companies in Australia.[5] As a result, there were concerns that other 'Five Eyes' members could use Australia as the go-to place for such allies to undermine encryption.[5] Resultantly, the law was reviewed months after the legislation was passed.[5]

Consequently, legislation weakening encryption could create an inconsistent international legal landscape, which could implicate mutual assistance treaties and create opportunities for jurisdiction forum shopping.

However, such transnational issues could be managed if broader legal infrastructure was implemented beyond the encryption legislation. The policymaker interviewee gave the example of the European Commission's Electronic Evidence Directive,[77] noting that it

> Provides a basis for improved cooperation and facilitating of investigations across EU member states, more avenues for redress, stricter data evidence sharing and retention safeguards and defined obligations to the public and private sector tech companies. This could be an effective avenue for resolving some of the problems driving the encryption debate.

Applying a similar directive to varying encryption policies could therefore minimise these risks to international cooperation.

Disproportionate Impacts on Vulnerable Groups

Weakening encryption can have critical implications for many vulnerable groups. The confidentiality that encryption affords allows individuals and minority groups to associate freely, providing a safe environment for people seeking support or concerned that their communications may be subject to interference. Encryption has helped protect the speech of vulnerable and marginalised communities who are more likely to be subject to abuse, violence, and discrimination because of their identity. For instance, research has demonstrated that women and young people are disproportionately impacted by the chilling effect of online surveillance, feeling greater pressure to self-censor and self-regulate online.[8] For instance, domestic abuse survivors heavily rely on encrypted services to communicate securely when abusers are in their homes. Additionally, as articulated by the *LGBT Tech* interviewee:

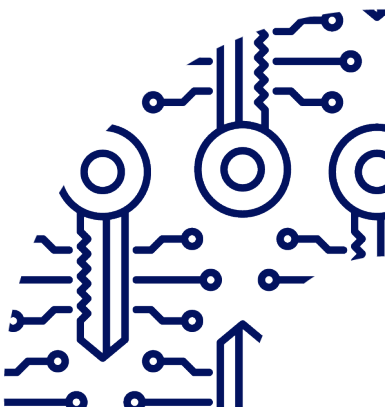
> The purpose of encryption is to ensure the complete privacy and anonymity of communications. This means making sure those who use encryption, specifically minority and vulnerable communities, won't have their information compromised such as sensitive health data or threats to safety.

Consequently, the research highlights how stakeholders neglect the importance of encrypted services for vulnerable communities within the current encryption debate.

Human Rights

It can be argued that the right to privacy, protected by Article 12 of the UDHR, is supported by the availability and use of strong encryption. It guarantees that an individual's private communication and information will be secure. In addition, encryption is closely associated with freedom of expression, enshrined in Article 19 of the UDHR, along with privilege against self-incrimination under Article 6 of the ECHR. [4] This right against self-incrimination is vital, as it safeguards individuals from being forced to disclose incriminating evidence that can be used against them. Therefore, a problem with legal powers enforcing individuals to surrender decryption keys is the potential to infringe on their fundamental rights to not self-incriminate.

In an age where communication progressively occurs online, strong E2EE affords the integrity and security of digital interactions. As such, efforts by state actors to limit or undermine these rights can have detrimental effects on personal freedoms. The civil society interviewee from the European Digital Rights stated, "without the right to privacy it is difficult to win any of the other social struggles, which means defending encryption". Encryption is pertinent to the work of human rights advocates, journalists, and other individuals who criticise state actors and therefore face heightened surveillance risks. Additionally, persistent Internet censorship threatens the rights to freedom of expression and assembly.[43,58] Consequently, encryption serves as an essential shield against persecution in repressive regimes.



State Abuse of Power
Governments seek to access encrypted devices through several means, including legal mandates, issuing warrants and compelling the disclosure of keys. Weakening encryption could therefore give states more exceptional access, creating additional opportunities to abuse power. A civil society interviewee highlighted that while LEIA say they will only use access to investigate crime, once a telecommunication service provider has a key, there are no guarantees of who abuses it, creating many concerns to user privacy. They argued that governments need to explain how they plan to address crime through 'mutually-assured disclosure', mentioning he was "more willing to accept certain types of surveillance if [I] know what's going on and why it's going on." They went on to express issues with the US intelligence electronic cellular surveillance tool, StingRay, stating:

> I do not have a problem with StingRay if Governments are only using it to track a handful of cell phones, I have a problem when they decide to track every cell phone coming in and out of Washington DC.

Moreover, state actors have attempted to regulate encryption by outrightly restricting access to the technology. For instance, in response to WhatsApp's failure to comply with orders to intercept user messages, Brazilian authorities ordered all telecommunications service providers to block the platform.[58] This reaffirms the problem that weakening encryption creates as an opportunity for exceptional access to be abused by states.

Economic Risks

The research findings emphasised that the modern digital economy relies on encryption for digital transactions and storage of sensitive information such as financial and medical records.[5,8,40,65] Encryption secures financial transactions and preserves public trust in the digital marketplace.[8,65] Therefore, weakening encryption would cause a myriad of economic impacts.

Limited Innovation and Choice
The safety and trust enabled by encryption incentivises innovators to create a range of products and services. A representative from the Open Rights Group stated that "encryption creates an enabling environment for entrepreneurs to flourish". Weakening encryption would therefore limit this entrepreneurship,[65] as industry would not be incentivised to innovate. This reduces the choice of services available to consumers. In response to Option 1: Restricting encryption from a technical means, a *Software Freedom Law Centre* representative mentioned that

> Innovation would be impeded because protocols that have technical vulnerabilities intentionally introduced into them, say Free and Open-Source Software, would not be adopted by other organisations that want to build strong encrypted services.

Additionally, it was noted that limited consumer choice would eventually lead to "encrypted communications services being only developed by governments". This position was reaffirmed by another civil society interviewee who opposed Option 1, as it would not enable start-ups to provide consumers with more choices.

Economic Impacts of Cybercrime
Installing backdoors in encrypted systems creates technical vulnerabilities that could be exploited to commit cybercrime. This renders products and services that rely on encrypted systems vulnerable to cyber-attacks.[78] Cyber-attacks include security breaches, theft or loss of customer or corporate data which can have significant economic impacts.[32] A report by IBM and the Ponemon Institute found that the average total cost to an Australian business which suffered a data breach in 2017 was $2.51 million.[65] Therefore, weakening encryption could cause cyber-attacks which in turn incur economic costs.

Loss of Consumer Trust
Encrypted services instil confidence and trust in consumers that the service they are using is secure from data breaches, and that their data will not be improperly accessed by the state.[5,8] The encrypted financial service interviewee stated that "It [encryption] gives assurance to customers that their financial transactions, such as savings and investments, are secure, safe, and not accessible by unauthorised persons". This trust could be undermined if encryption was weakened, either by backdoors being built into systems, or companies being compelled to provide the state with technical assistance. The same interviewee highlighted that "Consumer trust would be negatively impacted if non-government or other state actors had access to information and exploited mandated backdoors."

Conversely, the loss of consumer trust is dependent on a company's decision to comply with requests to weaken encryption. Companies can choose to act in the interest of their users and not comply with government mandates to weaken encryption. This would re-instil confidence and trust in consumers that

the security and confidentiality of their data would not be compromised. An interviewee from *CIPESA* mentioned that in the best-case scenario, platforms would have their independent procedures to assess government mandates to decide whether to comply with such requests. This interviewee cited the example of Google declining to comply with a Ugandan government request to block accounts belonging to opposition leaders promoting sectarian content. Resultantly, this risk is dependent on a company's level of compliance to state actors' requests.

Additionally, industry has opposed weakening encryption given the importance of consumer trust for growth of the digital economy. In 2015, industry actors such as Apple and Facebook wrote a letter to the Obama administration stating that "Consumer trust in digital products and services is an essential component enabling continued economic growth of the online marketplace…Accordingly, we urge you not to pursue any policy or proposal that would require companies to weaken encryption".[76] Companies have thus attempted to preserve consumer trust, hence reducing the severity of this risk. However, this should be considered with caution as technology companies have allegedly collaborated with state actors for surveillance purposes as seen in the PRISM program mentioned in the Snowden disclosures.[79]

Economic and International Competitiveness

Weakening encryption could affect the competitiveness of individual companies or industries, where there is high customer demand for companies to offer strongly encrypted services.[36,80] Deeks' article noted that American customers desire the privacy protections afforded by E2EE. Additionally, E2EE is a selling point for American products in European and Chinese markets.[76] The encrypted messaging service provider interviewee stated that "encryption for private messaging has become the expectation. From a competitive perspective, being able to offer a product that does this is essential to functioning of the company." Mandates to weaken encryption would therefore affect the attractiveness of a company's products and services. This was also noted by an industry interviewee that weakened encryption "could affect us negatively because customers would search for alternatives".

Weakening encryption could also affect the economic attractiveness of a country. If regulations to weaken encryption were present in one country, a potential loss of customers or compliance difficulties might influence a company to move to another country where such encryption regulations do not apply. It is noted that US corporations for example would prefer not to implement different technical requirements on the same products sold in different markets.[76] The interviewee from the Open Rights Group noted that a company may no longer justify its continued operations in a market if it involves complying with such restrictions. Additionally, it was remarked that if the UK were to impose weakening encryption laws "large compliance obligations may compel companies to leave the UK entirely" or "exclude all UK customers from using their services". Therefore, weakening encryption could influence a consumer's decision to stop using a product and lead to a company's withdrawal of operations from a country.

Trade Agreement Repercussions

A country's decision to implement encryption regulations could have repercussions on existing trade agreements. Deeks' article noted that weakening encryption in a country would compromise free trade agreements, such as the Trans Pacific Partnership (TPP);[76] an agreement among 12 states in North America, South America, Australia, and Asia. There is a prohibition in the TPP that parties may not require manufacturers or suppliers to provide access to a commercial product's encryption-based technologies as a condition of manufacture, sale, or use, unless a sale to a party's government.[76] Therefore, weakening encryption could complicate states' participation in such agreements. However, the extent of these repercussions could be limited, as there is a catch-all national security provision in the TPP that states:

> Nothing in this Agreement shall be construed to . . . preclude a Party from applying measures that it considers necessary for the fulfilment of its obligations to the maintenance or restoration of international peace or security, or the protection of its own essential security interests.[76]

Therefore, such a clause would permit participating states to weaken encryption on national security grounds, without implications for their membership of the TPP. Such a blanket clause allows member states to bypass their commitment to strong encryption on the grounds of their self-determination.

Impact Assessment Conclusion
In sum, this Impact Assessment has identified various risks and benefits that policymakers should consider when deliberating decisions to weaken encryption. On balance, it appears that the risks of weakening encryption outweigh claimed benefits. Socio-politically, weakening encryption would affect vulnerable groups in society, infringe upon human rights, create an opportunity for state abuse of power, produce new cybersecurity vulnerabilities and set a dangerous precedent. Economically, weakening encryption affects the economic competitiveness of countries and businesses, whilst harming innovation and consumer trust. These risks cannot be reconciled against the seeming benefits of weakening encryption as doing so counterintuitively impacts national security. In addition, the Impact Assessment notes how the benefits can be achieved through alternative means.

4.2 Decision-Making Framework

Informed by the factors identified in this research, the Decision-Making Framework (DMF) intends to guide stakeholders, including policymakers, in their decisions in encryption-related discussions. Accordingly, the DMF is not expected to be used prescriptively, rather it should be applied reflectively, considering a diverse range of contexts and interests which stakeholders prioritise. These elements, which differ across geographical expressions, may include economic interests, legal landscape, societal dynamics, and systems of governance.

The DMF emphasises economic and socio-political concerns and is crafted around a set of deliberative questions posited to policymakers under three separate sections: Purpose of weakening encryption technologies, LEIA capacity requirements, and Geopolitical effects.

4.2.1 Purpose of Weakening Encryption Technologies

As revealed by the research, the multi-layered nature of this debate requires stakeholders to address multiple factors when contemplating encryption-related decisions. In some areas, these factors tend to overlap across the three interview groups (civil society, industry, and policymaker) while in others, there are clear distinctions between these groups. The research, for instance, notes that among all interview groups, encryption is acknowledged as essential in protecting rights like privacy, preserving data integrity, and enabling secure communications and transactions (see Appendix 6.4.1). Conversely, issues surrounding trust in state actors, cybersecurity and economic factors are more confined to the civil society and industry groups. Here, interviewees identify the importance of encryption in securing technology systems, reducing harms to vulnerable groups, providing competitive advantage and upholding consumer trust (see Appendices 6.3.1-2). These outcomes enabled by encryption are also mentioned in existing literature.[10,36] The far-reaching impacts and uses of encryption are thus evident across these diverse groups.

Noted overlaps and intersects notwithstanding, the research highlights a pertinent point that acts as the linchpin for the aforementioned factors raised by the interviewees. While over 80% of interviewees indicate *Option 3: Do not restrict encryption* as their preferred choice, they also allude to a lack of clarity on the purpose of exceptional access or interception requests to encrypted data. For instance, regarding India's Traceability guidelines, the interviewee from *Software Freedom Law Centre* raises the question "[i]s the traceability act genuinely to combat fake news or is it for surveillance or interception?". More directly, the interviewee from *Future of Privacy Forum* states the need to establish use cases for weakening encryption to avert possible abuse by LEIAs; a position that is also echoed by other interviewees (see Appendix 6.3.1). Incidentally, across the three interviewee groups, the highest significance is attached to factors that imply the purpose to weaken encryption appears undefined (see Appendix 6.4.3). Furthermore, existing literature point to inconclusive evidence that strong encryption limits LEIA's investigatory powers.[5,8] These observations show a possible absence of coherent justifications for weakening encryption in light of the benefits it affords. For example. innovative security solutions are shown to be advantageous to digital communications and national economies.[7,50]

Taking these diverse stakeholder interests into context, the prevalent going dark narrative discounts the ripple effects that may arise from adopting a pro-weakening encryption stance. As illustrated in the CLD in section 3.1 and Impact Assessment in section 4.1, the research findings illuminate how the resultant positive effects of weakening encryption are seemingly offset by its negative impacts. Consequently, the argument that national security, for instance, is enhanced through undermined encryption technologies

seems contradictory as compromising encryption has a net negative outcome for national security. In this light, Box 1 provides guiding questions for stakeholders to consider in clarifying the purpose of weakening encryption.

Box 1: What is the purpose of weakening encryption technologies?

Socio-political

Context

- Under what context(s) should the weakening of encryption technologies be considered? Eg: Criminal investigation, National Security/Public Safety or Surveillance?
- What other national policies or regulations would encryption policies conflict with? How would these be resolved?

Means

- Are encryption restriction measures necessary and proportionate i.e. are these measures limited to a defined legal objective and are they minimally intrusive?
- What other measures besides weakening encryption have been considered to access data in these contexts? Have these measures been explored by LEIA?
- What protections i.e. legal and procedural safeguards exist to limit the misuse of exceptional access powers by LEIA? Such as data protection and retention policies.
- Do these safeguards adhere to or conflict with regional or international agreements and frameworks such as ECHR, ICCPR, UDHR? What measures exist to reconcile conflicts across agreements?

Impacts

- How have the downstream effects of weakening encryption, such as an increase in attack surfaces and system complexity, been assessed? What safeguards exist to curb these downstream effects if they occur?
- What safeguards exist to protect vulnerable groups, such as children, LGBT, domestic violence victims and activists, from disproportionate effects of weakening encryption?
- How would a country's decision to weaken encryption conflict with clauses in trade treaties that it has agreed to?

Accountability

- What avenues do citizens and individuals have to seek redress if their rights to: privacy, freedom of expression, freedom of association and privilege against self-incrimination are violated through weakened encryption?
- Who bears the responsibility for compensating citizens subjected to unintended harms caused through weakened encryption? Industry or State actors?

Economic

Impacts

- What are the costs of implementing changes to encrypted products and services to meet the requirements of exceptional access?
- How would these changes impact the national economies of countries that produce encryption technologies, and encrypted products and services?
- How would a country's decision to weaken encryption conflict with clauses in trade treaties that it has agreed to?
- In what ways would weakening encryption impact consumer trust? How has this impact been measured and mitigated?
- What competitive advantages does weakening encryption provide to industry, both domestically and internationally? What are the competitve disadvantages?
- What would be the effects of weakening encryption on innovation?

Accountability

- Who bears the costs of implementing system changes to meet exceptional access requests? Industry or State actors?

4.2.2 LEIA Capacity Requirements

Findings from the research also suggest the argument that strong encryption is detrimental to LEIA efforts appears unsubstantiated. While a legitimate need exists for LEIA to preserve public safety (see Appendix 6.3.1) and investigate crime, particularly sensitive ones like CSAM,[7] findings show this should not be at the disadvantage of individual rights. The reason for not violating individual rights is further supported by the fact that encryption does not completely prevent state actors from accessing user data for investigatory purposes. As noted in research findings, encryption does not fully conceal user data (see Appendix 6.2.2) given that digital trails created on the Internet can provide clues to facilitate investigatory procedures.[8,64] In addition, there are recorded instances of LEIA using easily accessible meta-data to investigate crime.[7,30,73] As cited in the benefits section of the Impact Assessment, governments have successfully exploited system vulnerabilities on the Telegram messaging application and Tor browser to access data and convict criminals. While some of these procedures have been used for less than ideal purposes,[8] they present a less intrusive technological means to facilitate criminal investigation than outrightly weakening encryption technologies. Hence, the oft-repeated narrative of going dark perhaps may be better captioned as dimmed lights given the existing possibilities presented by alternative means.

Additionally, the research findings imply that by LEIA arrogating expansive surveillance capabilities, there is a possibility of either creating or widening imbalanced power structures between the state and citizens (see Appendix 6.4.2). Regardless of the system of government practised in a country, this trend could prove harmful to citizens' trust which, as seen in the CLD and literature,[50] has wider negative implications for economic competitiveness and freedom of expression. Rather than the argument to weaken encryption technologies to facilitate LEIA's investigations, an understanding of their underlying capacity challenges (see Appendix 6.3.3) suggests a more useful approach to addressing investigatory barriers holistically.

Outlined in Box 2 are guiding questions for stakeholders to consider in assessing LEIA capacity requirements.

Box 2: How can LEIA capacity be enhanced to resolve investigatory challenges presented by strong encryption technologies?

Socio-political

LEIA capacity and capability

- What evidence exists to conclude that strong encryption impedes criminal investigation by LEIA? How has this evidence evolved?
- Of crimes facilitated through technological or digital means, which ones have proven more difficult to investigate due to strong encryption? How do these compare to other crimes facilitated through the same means?
- How effective is the coordination among LEIA at different levels? Nationally, regionally and internationally? What measures can be adopted to improve this coordination?
- How effective are training programmes for LEIA? How are these programmes kept updated in line with technology advancements?
- Have LEIA established Research and Development (R&D) functions/capacities to enhance digital investigatory capabilities? Do LEIA collaborate with R&D institutions? How have LEIA incorporated knowledge from R&D collaborations to enhance investigatory capacities?

Alternative means

- What alternative mechanisms do LEIA currently use to surmount barriers imposed by encryption technologies? How effective are these mechanisms? How have these mechanisms improved overtime?
- Have any downstream impacts resulted from the use of alternate means to access data for investigatory purposes? How have these impacts been mitigated?

Economic

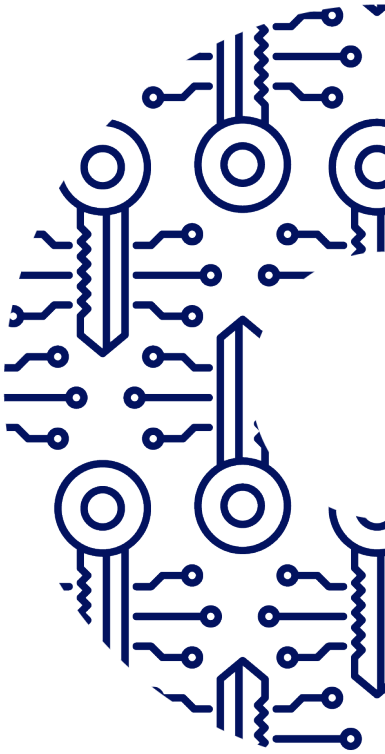
- What are the funding requirements to enhance LEIA's digital investigatory capabilities?

4.2.3 Geopolitical Effects of Weakening Encryption Technologies

According to the research findings, proposals to weaken encryption have intensified since Apple refused to cooperate with the FBI to unlock a device implicated in the 2015 San Bernardino incident.[48,50] To this end, various legislations targeted at achieving exceptional access by LEIA have either been or are in the process of being enacted by state actors in several countries.[31,50] While the current encryption discourse seems to be centred in the USA, Europe, UK and Australia, other parts of the world are also engaged in various forms of this issue. In 2018, for instance, India revised its guidelines for intermediaries that now require them to disclose data on request in the interest of national security.[7] Russia has since 2016, implemented a package of laws which on the basis of 'countering extremism', is geared at granting exceptional access to communications to Russian security agents.[81] In noting these developments, the research also finds the possibility of other states adopting variants of these restrictive positions. As mentioned in the IA in section 4.1, given that traditionally democratic societies appear to be implementing laws that threaten strong encryption, less democratic states may see this as enough justification to act the same. This is however a potentially tricky situation especially if there are fewer to no effective procedural safeguards to check state overreach and excesses.

To buttress these observations, the interviewee from *Paradigm Initiative* mentions how authoritarian or flawed democratic states could weaken encryption to follow suit and "...look good in international contexts and to Western leaders (DC, Brussels)...". Similarly, the *Open Rights Group* interviewee alludes to how perverse incentives are created for service providers "...to partner with state actors to provide these compliant [restricted encryption] services...". Other concerns expressed by interviewees point to how non-existent safeguards could lead to harmful outcomes if encryption restriction policies are applied. Particularly, in states with ineffective judicial systems, the research notes that inadequate understanding of technology by the judiciary prolongs technology-related cases (see Appendix 6.4.2).[58] To highlight the role that may be unwittingly played by western governments, Parsons' article mentions that in pushing legislation to weaken encryption, they "will lose the moral authority" to criticise undemocratic states that do the same.[56] Collectively, these factors illustrate how extensive the possible geopolitical effects of encryption policies could be in the near future. As mentioned in section 4.1, the flipside of pushing these policies to weaken encryption could also lead to companies migrating their services to less restrictive states, thus benefiting these organisations who can continue operating unhindered. This further indicates the multi-layered sides to the encryption debate.

Guiding questions to understand these geopolitical effects of weakening encryption are detailed in Box 3.



Box 3: What are the possible geopolitical consequences of states adopting policies and legislation that weaken encryption?

Socio-political

Divergence from established norms

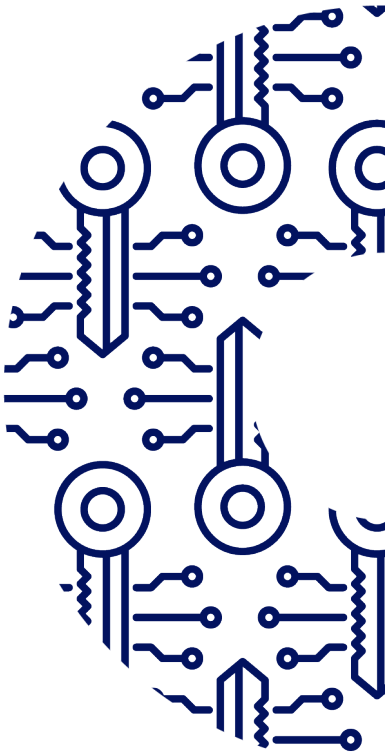
- Would treaties or agreements with other countries, such as mutual assistance treaties, be impacted by a nation's decision to weaken encryption? How would these impacts be measured?
- If such policies to weaken encryption are implemented in one nation but not another, is there broader legal infrastructure in place to ensure that the legal landscape (in terms of LEIA cooperation and data safeguards) does not become inconsistent and create loopholes for jurisdiction forum shopping to occur?
- Would implementing such legislation diverge from international norms?

Precedent

- In what ways would adopting legislation that enforces exceptional access set a precedent for other countries to follow? How would potential abuses of these exceptional powers be mitigated?
- What downstream effects (rights suppression, denial of access to services etc) may arise if less democratic societies follow and adopt restrictive encryption policies? How would these be mitigated?

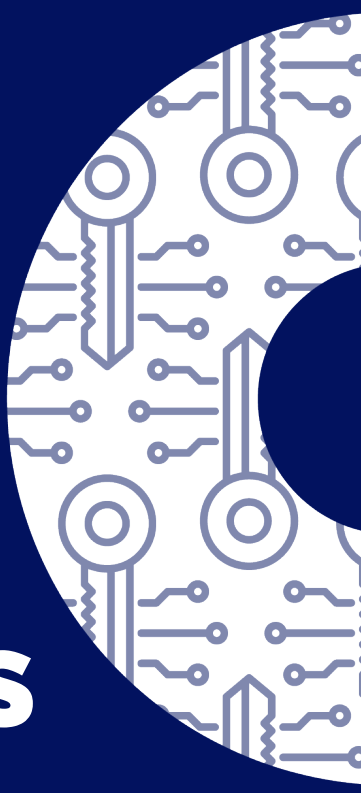
Economic

- What would be the effect be on national economies if encryption service providers transfer operations to less restrictive states?
- What mitigation plans are in place to prevent transnational technology companies from complying with conflicting legal requirements if encryption is weakened in some of their operating countries and not in others?



5

RECOMMENDATIONS



5. Recommendations

1. Application of Decision-Making Framework (DMF) to country-specific context

- The DMF serves as a guide instead of a prescriptive account of all the factors that should be considered in encryption-related discussions. Accordingly, it is recommended that it be adapted to suit a country's local context while considering national priorities, political beliefs, and differing governance systems.

- To adapt the DMF to a country's local context, it is recommended that policymakers adopt a participatory approach by engaging with key stakeholder groups to include a wider representation of voices in the encryption-related decisions.

2. Need for international dialogue

- While these decisions can be considered within a national context, it is recommended that they also be deliberated in an international forum. This is because encryption-related decisions have international implications, such as:

    - The cross-border nature of the Internet and consequently encryption which underpins it
    - The trans-jurisdictional issues that could arise from weakening technologies
    - The possibility that a legal precedent could be set if encryption was weakened
    - Inconsistent legal landscapes could be created where countries implement different encryption-related measures, thus creating loopholes and jurisdiction shopping.

- Existing international forums, such as the UN General Assembly Third Committee, recognise the importance of encryption as an enabler of human rights through its resolutions on the safety of journalists and the right to privacy.[83] However, there is currently a lack of international fora exclusively discussing the cross-border implications of encryption

3. Based on research findings, it is recommended that policymakers consider:

- The risks posed to cybersecurity by weakening encryption. Doing so creates new vulnerabilities that can be exploited by bad actors and undermines system integrity which is central to the functioning of various organisations.
- Given the reliance of e-commerce, online banking, and digital services on encryption, policymakers should be aware that weakening encryption could cripple economies by eroding consumer trust, stifling innovation, and damaging the economic competitiveness of firms and nations.
- Weakening encryption would infringe on civil liberties and human rights, including rights to privacy, freedom of expression and assembly, and privilege against self-incrimination. Additionally, weakening encryption could disproportionately impact vulnerable individuals, including victims of abuse and the LGBT community who rely on encryption to communicate privately. It is highly encouraged that policymakers account for the security encryption affords to those most in need.

4. Guidelines for exceptional access

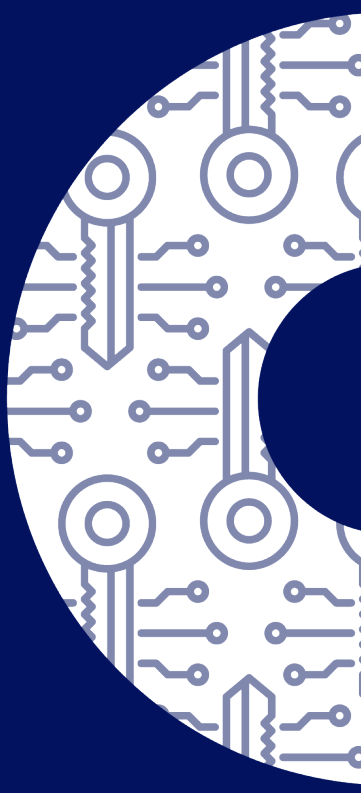
When developing guidelines for exceptional access, policymakers should consider establishing:

- A clearly defined purpose with limitations on its use occurring only in the most severe cases, i.e. applied against the principles of proportionality and necessity set out under international frameworks such as the ECHR.
- Legal frameworks and strong safeguards when weakening encryption i.e. data retention practices.
- Judicial oversight with checks and balances for ensuring accountability to prevent state abuse.

Participatory processes in policy formulation around exceptional access that include lesser represented voices

6

CONCLUSION



6. Conclusion

In conclusion, this research intends to guide policymakers in their decision-making related to encryption. It seeks to provide the perspectives and priorities of different stakeholders involved in the encryption debate. By adopting a mixed methodological approach, the research aimed to answer the overarching research question: ***What should policymakers be aware of and consider in their decisions concerning the weakening of encryption technologies?*** It has done so by highlighting the factors relevant to different stakeholders, the associated risks and benefits and posed questions that policymakers should consider when making decisions related to the weakening of encryption technologies.

This research emphasised the complexity within the encryption debate. On one hand, encryption presents challenges to national security, public safety, and law enforcement capabilities. Conversely, weakening encryption would present challenges for cybersecurity, impact the economy, and infringe upon individual human rights such as the right to privacy, freedom of expression and assembly, and the right to non-self-incrimination. Contradictions arise within this tension, as findings highlighted that national security may not be improved by weakening encryption if it creates opportunities that could be exploited by bad actors. Additionally, the argument purporting weakening encryption for the greater good of public safety is at odds with the safety of individuals, their ability to express themselves freely and communicate safely without fear of state interference.

Value of Research

This research has added value to the ongoing encryption-policy debate in four ways:

1. Evidence has been collected from geographical regions such as the Global South that are under-researched in relation to the encryption debate.
2. Evidence has been collected from an economic lens which is seemingly lacking in academic research concerning the encryption debate.
3. The coding framework categorising the main factors considered by stakeholders in the encryption debate can be applied and used in future research on the topic.
4. Using Variant Multi-criteria Decision Analysis, a Decision-Making Framework was developed. This framework does not prescribe answers or solutions for policymakers to adopt; rather it incorporates multiple perspectives that indicate what different stakeholders consider important in making encryption-related decisions.

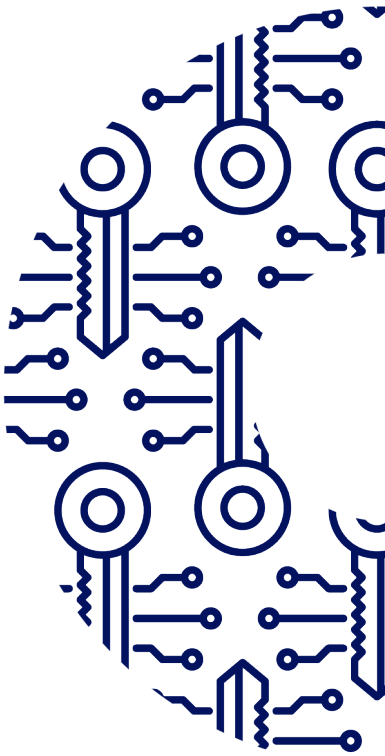
Limitations of Research

With growing regulatory discussions around the implications of strong encryption for LEIA and intelligence efforts, this research set out to understand diverse stakeholder perspectives on the topic. The methodology selected to answer the research questions proved beneficial to uncovering factors relevant to current deliberations on encryption-related policies. Specifically, the MCM tool presented a more expansive means to interpret and analyse data than traditional cost-benefit analysis methods would have allowed. Notably, the analysis was able to accommodate contrasting opinions within the same perspective. For instance, while most interviewees in the civil society category favoured strong encryption, a couple did not for reasons such as ensuring the online safety of children. Hence, this research highlighted nuances which are indicative of the complex nature of the topic.

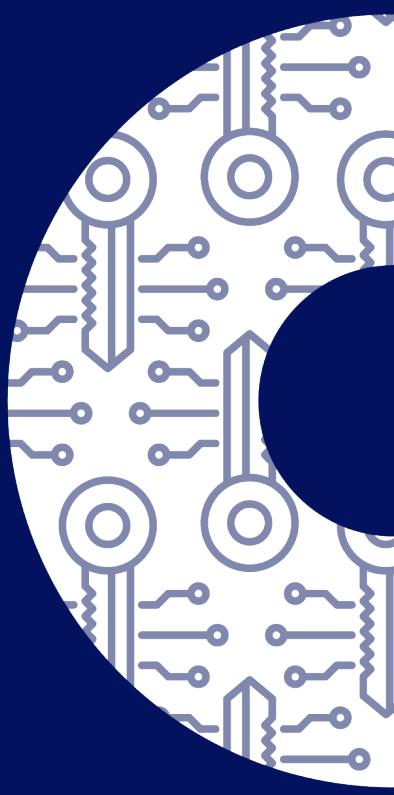
Although this research offers useful outputs, the sample size of 17 means the findings may not be fully representative, and thus should be considered cautiously. For example, one interviewee was categorised in the policymaker perspective and was limited to a largely homogenous geographical location. There is an opportunity for this research to include more policymaker perspectives to further enrich the discussion. Additionally, input from the industry perspective mainly concerned applications that enable messaging and financial capabilities. However, with the rising use of Internet-enabled technologies like the Internet of Things by both individuals and industries,[82] an understanding of factors critical to service providers in this sphere would be equally important. Of particular importance would be understanding the distributional impacts of undermining encryption on these technologies. Finally, while there were deliberate efforts to include lesser-heard perspectives during the research, the encryption discourse appears predominantly Western-centric. As indicated in the DMF, assessing the geopolitical effects of encryption policies is essential to understanding how the discourse would unfold globally.

Future Research

Additional research could focus on testing the robustness and utility of the designed DMF. Scenarios using the DMF could be developed and simulated to stress-test how it fares under different contexts of systems of governance and stakeholder priorities. This could be via personas or wargaming where participants role-play different stakeholder groups and use the DMF in multiple scenarios to understand how these groups would respond.[83] This could uncover the strengths and weaknesses of the DMF, reveal and challenge any assumptions and uncertainties incorporated in the framework, and assess how useful it would be in informing encryption-related policy decisions.[83] Subjecting the framework to such tests could identify ways in which it can be further refined to improve its utility to guide policymaker decisions in the encryption debate.



REFERENCES



1. Koops B-J, Kosta E. Looking for Some Light Through the Lens of 'Cryptowar' History: Policy Options for Law Enforcement Authorities Against 'Going Dark' [Internet]. Rochester, NY: Social Science Research Network; 2018 [cited 2021 Aug 10]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3249238

2. Moraes T. Sparkling Lights in the Going Dark: European Data Protection Law Review 2020;6(1):41–55.

3. United Nations. Universal Declaration of Human Rights [Internet]. United Nations [cited 2021 Aug 25];Available from: https://www.un.org/en/about-us/universal-declaration-of-human-rights

4. European Court of Human Rights. European Convention on Human Rights [Internet]. [cited 2021 Aug 25]. Available from: https://www.echr.coe.int/documents/convention_eng.pdf

5. Dheri P, Cobey D. Lawful Access & Encryption in Canada: A Policy Framework Proposal [Internet]. Rochester, NY: Social Science Research Network; 2019 [cited 2021 Aug 10]. Available from: https://papers.ssrn.com/abstract=3470957

6. Encryption Europe. An Introduction to Encryption Europe [Internet]. Position Paper2021 [cited 2021 Aug 10];Available from: https://encryptioneurope.eu/positionpaper/

7. Bhandari V, Bailey R, Rahman F. Backdoors to Encryption: Analysing an Intermediary's Duty to Provide "Technical Assistance" [Internet]. Rochester, NY: Social Science Research Network; 2021 [cited 2021 Aug 13]. Available from: https://papers.ssrn.com/abstract=3805980

8. Gill L, Israel T, Parsons C. Shining a Light on the Encryption Debate: A Canadian Field Guide [Internet]. The Citizen Lab2018 [cited 2021 Aug 9];Available from: https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/

9. Diab R. The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking-Bombs, and the Future of the Encryption Debate [Internet]. Rochester, NY: Social Science Research Network; 2019 [cited 2021 Aug 10]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3393172

10. Wilson A, Park C. Privacy's Best Friend [Internet]. New America Open Technology Institute2020 [cited 2021 Aug 9];Available from: http://newamerica.org/oti/reports/privacys-best-friend/

11. OECD. Recommendation of the Council concerning Guidelines for Cryptography Policy [Internet]. 1997 [cited 2021 Aug 17];Available from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289

12. Crocker NC and A. The FBI Could Have Gotten Into the San Bernardino Shooter's iPhone, But Leadership Didn't Say That [Internet]. Electronic Frontier Foundation2018 [cited 2021 Aug 14];Available from: https://www.eff.org/deeplinks/2018/04/fbi-could-have-gotten-san-bernardino-shooters-iphone-leadership-didnt-say

13. Child Safety [Internet]. Apple [cited 2021 Aug 14];Available from: https://www.apple.com/child-safety/

14. Robertson A. Apple's controversial new child protection features, explained [Internet]. The Verge2021 [cited 2021 Aug 14];Available from: https://www.theverge.com/2021/8/10/22613225/apple-csam-scanning-messages-child-safety-features-privacy-controversy-explained

15. ANOM: Hundreds arrested in massive global crime sting using messaging app [Internet]. BBC News2021 [cited 2021 Aug 14];Available from: https://www.bbc.com/news/world-57394831

16. Emmanuel Macron identified in leaked Pegasus project data | France | The Guardian [Internet]. [cited 2021 Aug 14];Available from: https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data

17. The National Archives. What is a Rapid Evidence Assessment? [Internet]. Government Social Research Service - Rapid evidence assessment toolkit2014 [cited 2021 Aug 12];Available from: https://webarchive.nationalarchives.gov.uk/ukgwa/20140402163359/http://www.civilservice.gov.uk/networks/gsr/resources-and-guidance/rapid-evidence-assessment/what-is

18. Godin K, Stapleton J, Kirkpatrick SI, Hanning RM, Leatherdale ST. Applying systematic review search methods to the grey literature: a case study examining guidelines for school-based breakfast programs in Canada. Systematic Reviews 2015;4(1):138.

19. Young A. Library skills essentials: Grey literature [Internet]. UCL [cited 2021 Aug 17];Available from: https://library-guides.ucl.ac.uk/library-skills-essentials/grey-literature

20. Global Encryption Coalition. About Global Encryption Coalition [Internet]. Global Encryption Coalition [cited 2021 Aug 24];Available from: https://www.globalencryption.org/about/

21. Steenmans I. Analytic Methods Session 9: Causal Loop Diagrams. 2021;

22. Homer J, Oliva R. Maps and models in system dynamics: A response to Coyle. System Dynamics Review 2001;17:347–55.

23. Dean M. Multi-criteria analysis [Internet]. In: Advances in Transport Policy and Planning. Elsevier; 2020 [cited 2021 Aug 17]. page 165–224.Available from: https://linkinghub.elsevier.com/retrieve/pii/S2543000920300147

24. Dodgson J. Multi-Criteria Analysis: A Manual. [Internet]. Wetherby: Communities and Local Government; 2009 [cited 2021 Aug 17]. Available from: http://www.communities.gov.uk/documents/corporate/pdf/1132618.pdf

25. Dimitriou HT, Ward EJ, Dean M. Presenting the case for the application of multi-criteria analysis to mega transport infrastructure project appraisal. Research in Transportation Economics 2016;58:7–20.

26. Leleur S. Complex Strategic Choices: Applying Systemic Planning for Strategic Decision Making. Springer Science & Business Media; 2012.

27. Macharis C, de Brucker K, van Raemdonck K. When to use Multi Actor Multi Criteria Analysis or other evaluation methods? In: Decision-Making for Sustainable Transport and Mobility: Multi Actor Multi Criteria Analysis. 2018. page 28–47.

28. Science Policy Research Unit. Multicriteria Decision Analysis Software, Multicriteria Mapping, MCM [Internet]. multicriteriamapping [cited 2021 Aug 24];Available from: https://www.multicriteriamapping.com

29. Williamson C. Questionnaires, individual interviews and focus groups. Research Methods: Information, Systems, and Contexts 2013;349–72.

30. Liguori C. Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate [Internet]. Rochester, NY: Social Science Research Network; 2020 [cited 2021 Aug 10]. Available from: https://papers.ssrn.com/abstract=3606601

31. Murphy CC. The Crypto-Wars myth: The reality of state access to encrypted communications. Common Law World Review 2020;49(3–4):245–61.

32. Davies G. Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers. The Journal of Criminal Law 2020;84(5):407–26.

33. Keenan B. State access to encrypted data in the United Kingdom: The 'transparent' approach. Common Law World Review 2020;49(3–4):223–44.

34. Santos M, Faure A. Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption. Social Media + Society 2018;4(3):2056305118795876.

35. McGarrity N, Hardy K. Digital surveillance and access to encrypted communications in Australia. Common Law World Review 2020;49(3–4):160–81.

36. Penney S, Gibbs D. Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter. mlj 2019;63(2):201–45.

37. Rozenshtein AZ. Surveillance Intermediaries. SLR 2018;70(1):99–189.

38. West L, Forcese C. Twisted into knots: Canada's challenges in lawful access to encrypted communications. Common Law World Review 2020;49(3–4):182–98.

39. Chatterjee B. Fighting Child Pornography through UK Encryption Law: A Powerful Weapon in the Law's Armoury. Child & Fam L Q 2012;24(4):410–27.

40. Šepec M. Digital data encryption – aspects of criminal law and dilemmas in Slovenia | Digital Evidence and Electronic Signature Law Review. Digital Evidence and Electronic Signature Law Review 2014;10:147–54.

41. Chatterjee BB. New but not improved: a critical examination of revisions to the Regulation of Investigatory Powers Act 2000 encryption provisions. International Journal of Law and Information Technology 2011;19(3):264–84.

42. Article 19. Right to Online Anonymity [Internet]. Right to Online Anonymity2015 [cited 2021 Aug 10];Available from: https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf

43. Article 19. Russia: Blocking Telegram is a serious violation of freedom of expression and privacy [Internet]. ARTICLE 192018 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/russia-blocking-telegram-serious-violation-freedom-expression-privacy/

44. Article 19. Rwanda: 2016 Law Governing Information and Communication Technologies Legal Analysis [Internet]. 2018 [cited 2021 Aug 10];Available from: https://www.article19.org/wp-content/uploads/2018/05/Analysis-Rwanda-ICT-Law-April-2018.pdf

45. Lin G, Hong H, Sun Z. A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing. IEEE Access 2017;5:9464–75.

46. Wang S, Liang K, Liu JK, Chen J, Yu J, Xie W. Attribute-Based Data Sharing Scheme Revisited in Cloud Computing. IEEE Transactions on Information Forensics and Security 2016;11(8):1661–73.

47. Voors MP. Encryption Regulation in the Wake of September 11, 2001: Must We Protect National Security at the Expense of the Economy? 2003;55:23.

48. Spinello RA. The ethical consequences of "going dark." Business Ethics: A European Review 2021;30(1):116–26.

49. Academic: The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption - Schneier on Security [Internet]. [cited 2021 Aug 13];Available from: https://www.schneier.com/academic/archives/1997/04/the_risks_of_key_rec.html

50. Vandenberg DT. Encryption Served Three Ways: Disruptiveness as the Key to Exceptional Access. Berkeley Technology Law Journal 2017;32:531–62.

51. Lindsay JR. Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. Security Studies 2020;29(2):335–61.

52. Bellovin SM, Blaze M, Clark S, Landau S. Going Bright: Wiretapping without Weakening Communications Infrastructure. IEEE Security Privacy 2013;11(1):62–72.

53. Bharadwaj P, Pal H, Narwal B. Proposing a Key Escrow Mechanism for Real-Time access to End-to-End encryption systems in the Interest of Law Enforcement. In: 2018 3rd International Conference on Contemporary Computing and Informatics (IC3I). 2018. page 233–7.

54. Savona EU, Mignone M. The Fox and the Hunters: How IC Technologies Change the Crime Race. 2004;24.

55. Donahue JL. A comparative analysis of international encryption policies en route to a domestic solution. 2018;

56. The Citizen Lab. Canada's New and Irresponsible Encryption Policy: How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy [Internet]. The Citizen Lab2019 [cited 2021 Aug 10];Available from: https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/

57. Henrique Atta P, Moraes T. Summary Report on the judgement of ADPF nº 403 and ADI nº 5.527: The WhatsApp Case [Internet]. LAPIN2020 [cited 2021 Aug 10];Available from: https://lapin.org.br/en-gb/2020/05/29/summary-report-on-the-judgement-of-adpf-no-403-and-adi-no-5-527-the-whatsapp-case/

58. Article 19. Brazil: WhatsApp services blocked nationwide in violation of freedom of expression [Internet]. ARTICLE 192016 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/brazil-whatsapp-services-blocked-nationwide-in-violation-of-freedom-of-expression/

59. Herpig S, Schuetze J. The Encryption Debate in Germany: 2021 Update [Internet]. Carnegie Endowment for International Peace; 2021 [cited 2021 Mar 8]. Available from: https://carnegieendowment.org/files/202104-Germany_Country_Brief.pdf

60. Lear S. The Fight Over Encryption: Reasons Why Congress Must Block the Government from Compelling Technology Companies to Create Backdoors into Their Devices. CLEVELAND STATE LAW REVIEW 2018;66:35.

61. Benson V, Turksen U. Privacy, security and politics: current issues and future prospects. Communications Law 2017;22(4):124–31.

62. Keith B. Official access to encrypted communications in New Zealand: Not more powers but more principle? Common Law World Review 2020;49(3–4):199–222.

63. Murphy CC. State access to encrypted communications: A symposium. Common Law World Review 2020;49(3–4):153–9.

64. Harkens A. "Rear Window Ethics" and Discrimination: The Darker Side of big Data. In: European Conference on e-Government. 2016. page 267–72.

65. O'Shea L, Thomas E. The Role of Encryption in Australia : A Memorandum [Internet]. Access Now; 2018 [cited 2021 Aug 9]. Available from: https://digitalrightswatch.org.au/wp-content/uploads/2018/01/Crypto-Australia-Memo.pdf

66. LGBT Tech. Encryption Essential for the LGBTQ+ Community [Internet]. [cited 2021 Aug 10];Available from: https://docs.wixstatic.com/ugd/699ad7_d6ba4d9d03f649b8aba9035b8df88bde.pdf

67. India: Tech firms should uphold privacy, free speech [Internet]. ARTICLE 19 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/india-tech-firms-should-uphold-privacy-free-speech/

68. UNCTAD. Global e-commerce jumps to $26.7 trillion, COVID-19 boosts online sales [Internet]. 2021 [cited 2021 Aug 1];Available from: https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales

69. Coburn J, Stirling A, Bone F. Multicriteria Mapping Manual [Internet]. 2019 [cited 2021 Aug 11];Available from: http://users.sussex.ac.uk/~prfh0/MCM_Manual.pdf

70. European Court of Human Rights. Guide on Article 8 of the Convention – Right to respect for private and family life [Internet]. [cited 2021 Aug 25];Available from: https://www.echr.coe.int/documents/guide_art_8_eng.pdf

71. January 2020 28th. The rise of investment apps [Internet]. FinTech Futures2020 [cited 2021 Aug 19];Available from: https://www.fintechfutures.com/2020/01/the-rise-of-investment-apps/

72. Herpig S. Government Hacking: Computer Security vs. Investigative Powers [Internet]. 2017 [cited 2021 Mar 8]. Available from: https://www.stiftung-nv.de/sites/default/files/snv_tcf_government_hacking-problem_analysis_0.pdf

73. Herpig DS. A Framework for Government Hacking in Criminal Investigations [Internet]. 2018. Available from: https://www.stiftung-nv.de/sites/default/files/a_framework_for_government_hacking_in_criminal_investigations.pdf

74. Herpig DS. Government Hacking: Global Challenges [Internet]. Stifung Neue Verantwortung; 2018 [cited 2021 Aug 10]. Available from: https://www.stiftung-nv.de/sites/default/files/government_hacking_akt.feb_.pdf

75. Callas J. The "Ghost User" Ploy to Break Encryption Won't Work [Internet]. American Civil Liberties Union2019 [cited 2021 Aug 9];Available from: https://www.aclu.org/blog/privacy-technology/ghost-user-ploy-break-encryption-wont-work

76. Deeks A. The International Legal Dynamics of Encryption [Internet]. Rochester, NY: Social Science Research Network; 2020 [cited 2021 Aug 10]. Available from: https://papers.ssrn.com/abstract=3587438

77. European Commission. DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: Laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [Internet]. [cited 2021 Aug 23];Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN

78. CPJ. Encryption Letter to Obama [Internet]. 2015 [cited 2021 Aug 10];Available from: https://cpj.org/wp-content/uploads/2015/05/Encryption_Letter_to_Obama_final_0519155B15D-1.pdf

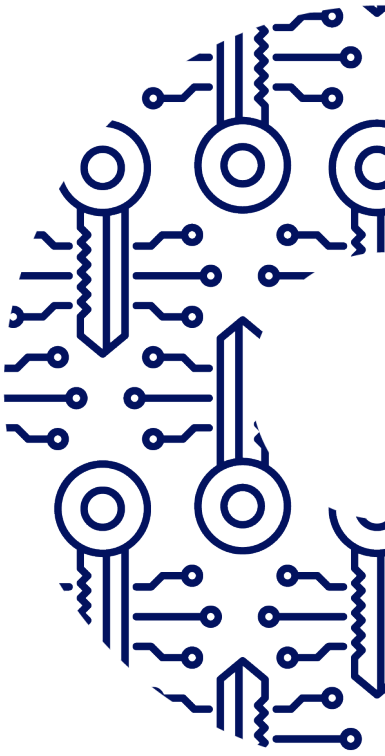
79. Greenwald G, MacAskill. NSA Prism program taps in to user data of Apple, Google and others [Internet]. the Guardian2013 [cited 2021 Aug 25];Available from: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

80. Stisa Granick J. In Latest Encryption Battle with Apple, Justice Department Still Wrong [Internet]. American Civil Liberties Union2020 [cited 2021 Aug 10];Available from: https://www.aclu.org/news/privacy-technology/in-latest-encryption-battle-with-apple-doj-still-wrong/

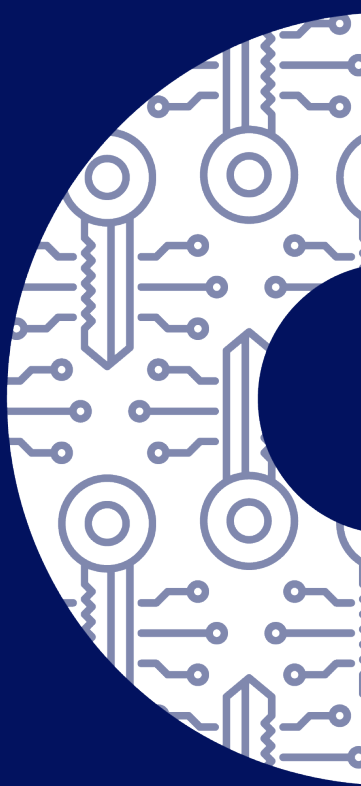
81. Article 19. Russia: Telegram block leads to widespread assault on freedom of expression online [Internet]. ARTICLE 192018 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/russia-telegram-block-leads-widespread-assault-freedom-expression-online/

82. Confederation of Indian Industry, Deloitte. Internet of Things (IoT) | The rise of the connected world [Internet]. 2020 [cited 2021 Aug 21];Available from: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-IoT_Theriseoftheconnectedworld-28aug-noexp.pdf

83. Steenmans I. Analytic Methods for Policy Session 15: (War)Gaming. 2021;



APPENDICES



Appendix Content Page

Appendix 1 Rapid Evidence Assessment

Research Question

What should policymakers be aware of and consider in their decisions concerning the weakening of encryption technologies?

Sub-research questions

- SRQ 1: What are the means of weakening encryption?
- SRQ 2: What are the justifications for weakening of encryption?
- SRQ 3: What are the impacts (risks and benefits) of weakening encryption?

Academic Databases

The following databases were selected for their multidisciplinary nature and their comprehensive coverage of all source types. This is pertinent because the research questions are nested within multiple disciplines. Additionally, all selected databases performed well in terms of transparency and reproducibility as their search systems can effectively and efficiently perform Boolean searches with precision, reproducibility and recall.

- Inspec
- International Bibliography of Social Sciences (IBSS)
- Lexis Nexis
- ProQuest Central
- Scopus
- Web of Science

Disciplines

- Science and Technology Studies
- Social Science
- Political Science
- Public Administration
- Law
- Economics

Search strategy

A scoping search was initially conducted to identify all relevant search terms. Firstly, key concepts from the research questions were identified, and extraneous terms omitted. The key concepts identified are:

- Encryption
- Weakening
- Impacts
- Policy
- Lenses
- Political justification

Secondly, the relevant synonyms for each concept were identified and combined using Boolean operators. Phrase searching and wildcards were also used to balance the sensitivity and precision of the search results.

Search Matrix

Key concepts*	Encryption	Weakening	Impacts	Policy	Lenses	Political justifications
Alternative terms / synonyms	• Encrypt* • "End to end encryption" • Cryptography	• "Weakening encryption" • Vulnerabilit*	• Impact* • Risk* • Benefi* • Consequence* • Win* • Lose* • advantage* • disadvantage*	• Policies • Regulat* • Law • Legislat*	• Econom* • Tech* • "socio-political" • "sociopolitical" • Social • politic*	• "online harm*" • Terror* • Traffick* • "CSAM" • Surveil* • "Child* Sexual Abuse Material" • "child* exploitation" • "public safety" • "National security" • Misinformation • "Offensive material" • "Hate speech" • Privacy • "Civil libert*" • Security

Scoping search – additional terms		• "exceptional access" • "lawful access" • "extraordinary access" • ("client side scanning" OR • "client-side scanning") • "key escrow" • Backdoor* • "backdoor access" • "content scanning"	• ("trade-off" OR "trade off" OR tradeoff") • Disbenefit* • Danger*	• Policymaker* • Govern* • Law enforcement • ("decision mak*" OR • "decision-mak*") • "decision making framework" • "decision making model" • "model"		

Search Syntax

Database	Search Syntax
Inspec	(((((((Encrypt* OR "End to end encryption" OR "End-to-end encryption" OR Cryptography) W/N ALL) AND (("Weakening encryption" OR Vulnerabilit* OR "exceptional access" OR "lawful access" OR "extraordinary access" OR "client side scanning" OR "client-side scanning" OR "key escrow" OR backdoor* OR "backdoor access" OR "content scanning") W/N ALL)) AND ((Impact* OR risk* OR benefit* OR consequence* OR win* OR lose* OR advantage* OR disadvantage* OR "trade-off" OR "trade off" OR "tradeoff" OR disbenefit* OR danger*) W/N KY)) AND ((policies OR regulat* OR law OR legislat* OR policymaker* OR Govern* OR "Law enforcement" OR "decision mak*" OR "decision-mak*" OR "decision making framework" OR "decision making model" OR "model") W/N KY)) AND ((econom* OR tech* OR "socio-political" OR "sociopolitical" OR social OR politic*) W/N KY)) AND (("online harm*" OR terror* OR traffick* OR "Child* sexual Abuse Material" OR "CSAM" OR "child* exploitation" OR "public safety" OR "National security" OR surveil* OR misinformation OR "offensive material*" OR "hate speech" OR privacy OR "civil libert*" OR security) W/N KY))
IBSS	((Encrypt* OR "End to end encryption" OR Cryptography) AND ("Weakening encryption" OR Vulnerabilit* OR "exceptional access" OR "lawful access" OR "extraordinary access" OR "client side scanning" OR "client-side scanning" OR "key escrow" OR backdoor* OR "backdoor access" OR "content scanning") AND TIABSU(Impact* OR risk* OR benefit* OR consequence* OR win* OR lose* OR advantage* OR disadvantage* OR "trade-off" OR "trade off" OR "tradeoff" OR disbenefit* OR danger*) AND TIABSU(policies OR regulat* OR law OR legislat* OR policymaker* OR Govern* OR "Law enforcement" OR ("decision maker" OR "decision makers" OR "decision makes" OR "decision making") OR "decision-mak*" OR "decision making framework" OR "decision making model" OR "model") AND TIABSU(econom* OR tech* OR "socio-political" OR "sociopolitical" OR social OR politic*) AND TIABSU("online harm*" OR terror* OR traffick* OR "Child* sexual Abuse Material" OR "CSAM" OR "child* exploitation" OR "public safety" OR "National security" OR surveil* OR misinformation OR ("offensive material") OR "hate speech" OR privacy OR ("civil libertarian" OR "civil libertarianism" OR "civil libertarians" OR "civil liberties" OR "civil liberty") OR security))
Lexis Nexis	(encrypt! OR "end to end encryption") AND (weakening OR "weakening encryption" OR vulnerabilit! OR "exceptional access" OR "lawful access" OR "extraordinary access" OR "client-side scanning" OR "key escrow" OR "backdoor access" OR "content scanning") AND (impact OR win! OR lose! OR benefi! OR risk! OR consequence! OR advantage! OR disadvantage! OR "trade-off" OR "trade off" OR tradeoff OR disbenefit! OR danger!) AND (policies OR regulat! OR law OR legislat! OR policymaker! OR govern! OR "law enforcement" OR "decision mak!" OR "decision-mak!" OR "decision making framework" OR "decision making model" OR "model") AND (econom! OR tech! OR "socio-political" OR "socio political" OR social OR politic!) AND ("online harm" OR terror! OR traffick! OR "CSAM" OR surveil! OR "child! sexual abuse material" OR "child! exploitation" OR "public safety" OR "national security" OR misinformation OR "offensive material" OR "hate speech" OR privacy OR "civil libert!" OR security)
ProQuest Central	((Encrypt* OR "End to end encryption" OR Cryptography) AND ("Weakening encryption" OR Vulnerabilit* OR "exceptional access" OR "lawful access" OR "extraordinary access" OR "client side scanning" OR "client-side scanning" OR "key escrow" OR backdoor* OR "backdoor access" OR "content scanning") AND TIABSU(Impact* OR risk* OR benefit* OR consequence* OR win* OR lose* OR advantage* OR disadvantage* OR "trade-off"

	OR "trade off" OR "tradeoff" OR disbenefit* OR danger*) AND TIABSU(policies OR regulat* OR law OR legislat* OR policymaker* OR Govern* OR "Law enforcement" OR "decision mak*" OR "decision-mak*" OR "decision making framework" OR "decision making model" OR "model") AND TIABSU(econom* OR tech* OR "socio-political" OR "sociopolitical" OR social OR politic*) AND TIABSU("online harm*" OR terror* OR traffick* OR "Child* sexual Abuse Material" OR "CSAM" OR "child* exploitation" OR "public safety" OR "National security" OR surveil* OR misinformation OR "offensive material*" OR "hate speech" OR privacy OR "civil libert*" OR security))
Scopus	(ALL ("encrypt*" OR "end to end encryption" OR "cryptography") AND ALL ("Weakening encryption" OR "vulnerabilit*" OR "exceptional access" OR "lawful access" OR "extraordinary access" OR "client-side scanning" OR "client side scanning" OR "key escrow" OR backdoor OR "backdoor access" OR "content scanning") AND TITLE-ABS-KEY (impact* OR risk* OR benefi* OR consequence* OR win* OR lose* OR advantage* OR disadvantage* OR "trade-off" OR "trade off" OR "tradeoff" OR "disbenefit*" OR "danger*") AND TITLE-ABS-KEY (policies OR regulat* OR law OR legislat* OR policymaker* OR govern* OR "law enforcement" OR "decision mak*" OR "decision-maker" OR "decision making" OR "decision making model" OR "decision making framework") AND TITLE-ABS-KEY (econom* OR tech* OR "socio-political" OR social OR politic* OR "sociopolitical") AND TITLE-ABS-KEY ("online harm*" OR terror* OR "CSAM" OR surveil* OR "child* sexual abuse material" OR "child* exploitation" OR "public safety" OR "national security" OR misinformation OR "offensive material" OR "hate speech" OR "privacy" OR "civil libert*" OR "security")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp")) AND (EXCLUDE (SUBJAREA , "MATE") OR EXCLUDE (SUBJAREA , "PHYS") OR EXCLUDE (SUBJAREA , "MEDI") OR EXCLUDE (SUBJAREA , "ENVI") OR EXCLUDE (SUBJAREA , "ENER") OR EXCLUDE (SUBJAREA , "CHEM") OR EXCLUDE (SUBJAREA , "NURS") OR EXCLUDE (SUBJAREA , "PSYC") OR EXCLUDE (SUBJAREA , "AGRI") OR EXCLUDE (SUBJAREA , "BIOC") OR EXCLUDE (SUBJAREA , "EART") OR EXCLUDE (SUBJAREA , "HEAL")) AND (EXCLUDE (PUBYEAR , 1999) OR EXCLUDE (PUBYEAR , 1998) OR EXCLUDE (PUBYEAR , 1997) OR EXCLUDE (PUBYEAR , 1986))
Web of Science	TOPIC:("encrypt*" OR "end to end encryption" OR "cryptography") AND TOPIC: ("Weakening encryption" OR "vulnerabilit*" OR "exceptional access" OR "lawful access" OR "extraordinary access" OR "client-side scanning" OR "client side scanning" OR "key escrow" OR backdoor OR "backdoor access" OR "content scanning") AND TOPIC: (impact* OR risk* OR benefi* OR consequence* OR win* OR lose* OR advantage* OR disadvantage* OR "trade-off" OR "trade off" OR "tradeoff" OR "disbenefit*" OR "danger*") AND TOPIC: (policies OR regulat* OR law OR legislat* OR policymaker* OR govern* OR "law enforcement" OR "decision mak*" OR "decision-maker" OR "decision making" OR "decision making model" OR "decision making framework") AND TOPIC: (econom* OR tech* OR "socio-political" OR social OR politic* OR "sociopolitical") AND TOPIC: ("online harm*" OR terror* OR "CSAM" OR surveil* OR "child* sexual abuse material" OR "child* exploitation" OR "public safety" OR "national

	security" OR misinformation OR "offensive material" OR "hate speech" OR "privacy" OR "civil libert*" OR "security")

Inclusion and exclusion criteria

The inclusion /exclusion criteria and their reasoning is as follows:

- *Type of information:* All types of information sources [articles, book chapters, conference papers] that had been peer-reviewed and were available in English were included. All grey literature is excluded. Specifying peer-reviewed articles ensured they were of high quality.

- *Range of research:* Qualitative, quantitative, mixed method, and empirical studies

- *Geographical location:* To ensure that the search included evidence from a diverse range of political regimes, limits on the geographical scope were not set. This was done intentionally to ensure a varied range of evidence given that academia is dominated by English speaking democracies in the Global North.

- *Time:* The search results were limited to studies published from 2000 – 2021 because it was in 2000 that the Advanced Encryption Standard (AES) was first introduced as a much stronger option to replace the Data Encryption Standard (DES), which had become vulnerable to brute-force attacks. Presently, AES is widely used to encrypt data at rest (i.e. on devices) and data in transit such as in wireless communications. A good example of this would be communications via encrypted messaging apps like WhatsApp.

- Results with titles and abstracts that do not contain at least two search terms were excluded

- Results with titles and abstracts that do not answer two research questions were excluded.

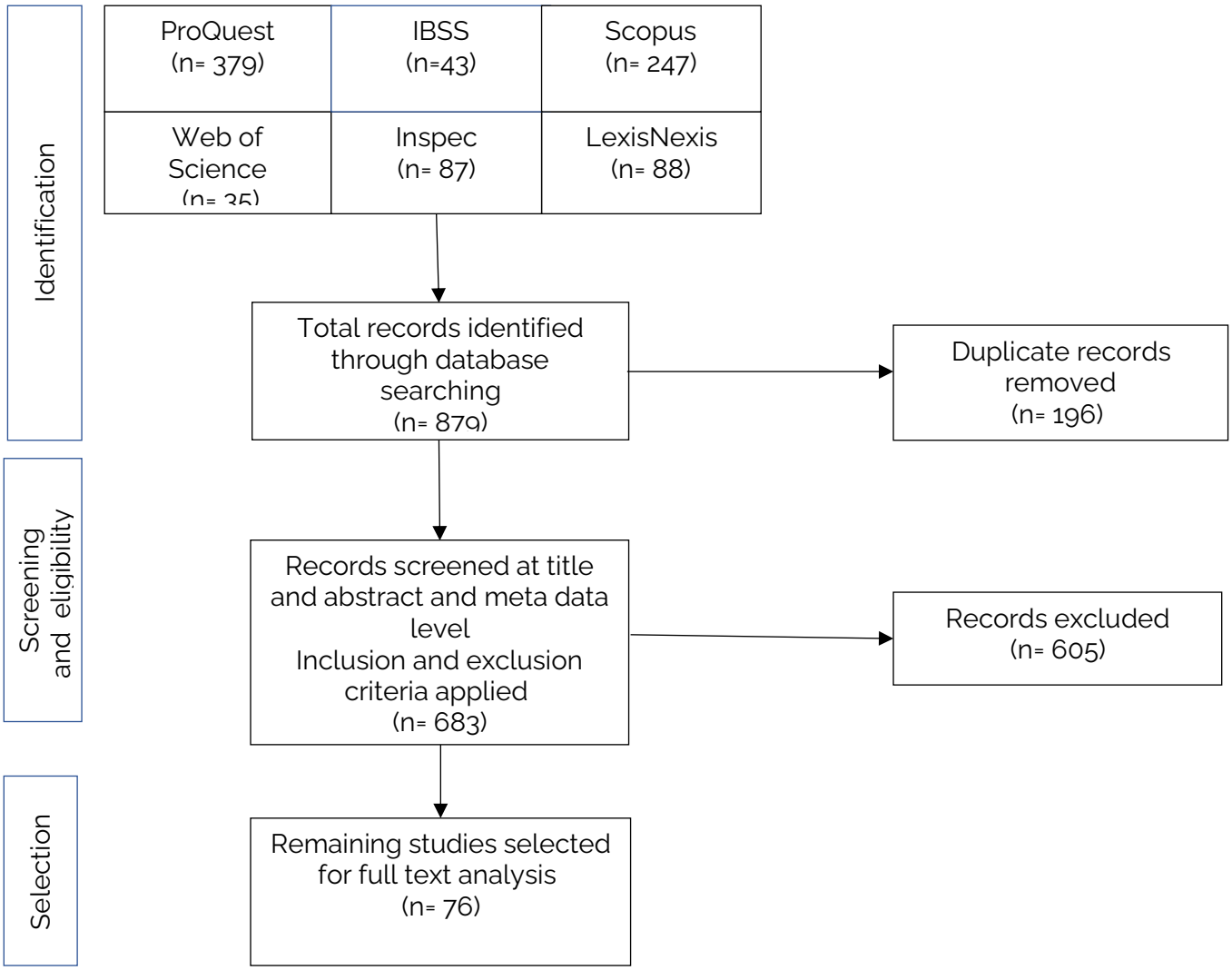
Literature management

- Zotero is the preferred reference manager as it a free open-source software thereby making it accessible to all team members. Zotero is also interoperable with all the academic databases selected and it is also able to detect duplicates within the same collection, therefore helpful in cleaning up and consolidating results from all the databases. Lastly, it allows for sharing of citations through shared folders, which enhances the transparency of the protocol and consequently the REA.

Selection of studies

- This review includes qualitative, quantitative, mixed methods and empirical studies.

Included Studies (PRISMA Framework)



76 studies were selected for full text analysis. However, only 28 articles were relevant in answering the research question and sub-research questions. 48 articles were therefore excluded as they did not contain any relevant information on encryption or did not answer the overarching research question and sub-research questions.

Strategy for data synthesis

The final articles 28 included in the REA were read and grouped according to the following questions:

- Which countries are studies focussed on?
- What are the means of weakening encryption?
- Identified impacts (risk and benefits) of weakening encryption, categorised by the economic and socio-political lens

- Who is affected by these policies and who is implementing these policies?
- What justifications are used for weakening encryption?

References of articles screened at full text for REA

1. Lin G, Hong H, Sun Z. A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing. IEEE Access 2017;5:9464–75.

2. Donahue JL. A comparative analysis of international encryption policies en route to a domestic solution. 2018;

3. Santos M, Faure A. Affordance is Power: Contradictions Between Communicational and Technical Dimensions of WhatsApp's End-to-End Encryption. Social Media + Society 2018;4(3):2056305118795876.

4. Wang S, Liang K, Liu JK, Chen J, Yu J, Xie W. Attribute-Based Data Sharing Scheme Revisited in Cloud Computing. IEEE Transactions on Information Forensics and Security 2016;11(8):1661–73.

5. Warren M, Leitch S. Data retention: an assessment of a proposed national scheme. Journal of Information, Communication & Ethics in Society 2019;17(1):98–112.

6. Lindsay JR. Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. Security Studies 2020;29(2):335–61.

7. Šepec M. Digital data encryption – aspects of criminal law and dilemmas in Slovenia | Digital Evidence and Electronic Signature Law Review. Digital Evidence and Electronic Signature Law Review 2014;10:147–54.

8. McGarrity N, Hardy K. Digital surveillance and access to encrypted communications in Australia. Common Law World Review 2020;49(3–4):160–81.

9. Voors MP. Encryption Regulation in the Wake of September 11, 2001: Must We Protect National Security at the Expense of the Economy? 2003;55:23.10.

10. Vandenberg DT. Encryption Served Three Ways: Disruptiveness as the Key to Exceptional Access. Berkeley Technology Law Journal 2017;32:531–62.

11. Chatterjee B. Fighting Child Pornography through UK Encryption Law: A Powerful Weapon in the Law's Armoury. Child & Fam L Q 2012;24(4):410–27.

12. Bellovin SM, Blaze M, Clark S, Landau S. Going Bright: Wiretapping without Weakening Communications Infrastructure. IEEE Security Privacy 2013;11(1):62–72.

13. Penney S, Gibbs D. Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter. mlj 2019;63(2):201–45.

14. Chatterjee BB. New but not improved: a critical examination of revisions to the Regulation of Investigatory Powers Act 2000 encryption provisions. International Journal of Law and Information Technology 2011;19(3):264–84.

15. Keith B. Official access to encrypted communications in New Zealand: Not more powers but more principle? Common Law World Review 2020;49(3–4):199–222.

16. Benson V, Turksen U. Privacy, security and politics: current issues and future prospects. Communications Law 2017;22(4):124–31.

17. Bharadwaj P, Pal H, Narwal B. Proposing a Key Escrow Mechanism for Real-Time access to End-to-End encryption systems in the Interest of Law Enforcement. In: 2018 3rd International Conference on Contemporary Computing and Informatics (IC3I). 2018. page 233–7.

18. Harkens A. "Rear Window Ethics" and Discrimination: The Darker Side of big Data. In: European Conference on e-Government. 2016. page 267–72.

19. Davies G. Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers. The Journal of Criminal Law 2020;84(5):407–26.

20. Murphy CC. State access to encrypted communications: A symposium. Common Law World Review 2020;49(3–4):153–9.

21. Keenan B. State access to encrypted data in the United Kingdom: The 'transparent' approach. Common Law World Review 2020;49(3–4):223–44.

22. Rozenshtein AZ. Surveillance Intermediaries. SLR 2018;70(1):99–189.

23. Murphy CC. The Crypto-Wars myth: The reality of state access to encrypted communications. Common Law World Review 2020;49(3–4):245–61.

24. Spinello RA. The ethical consequences of "going dark." Business Ethics: A European Review 2021;30(1):116–26.

25. Lear S. The Fight Over Encryption: Reasons Why Congress Must Block the Government from Compelling Technology Companies to Create Backdoors into Their Devices. CLEVELAND STATE LAW REVIEW 2018;66:35.

26. Savona EU, Mignone M. The Fox and the Hunters: How IC Technologies Change the Crime Race. 2004;24.

27. West L, Forcese C. Twisted into knots: Canada's challenges in lawful access to encrypted communications. Common Law World Review 2020;49(3–4):182–98.

28. Thanthry N, Pendse R, Namuduri K. Voice over IP security and law enforcement. In: Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology. 2005. page 246–50.

Appendix 2 Systematic Grey Literature Review Protocol

A systematic approach was taken to identify to review grey literature. However, as there is no prescribed standard for conducting a systematic grey literature search, a process similar to the REA was undertaken.

Research Question

What should policymakers be aware of and consider in their decisions concerning the weakening of encryption technologies?

Sub-research questions

- SRQ 1: What are the means of weakening encryption?
- SRQ 2: What are the justifications for weakening of encryption?
- SRQ 3: What are the impacts (risks and benefits) of weakening encryption?

Identifying sources of grey literature

Two approaches were taken to identifying relevant grey literature: 1) identifying organisations that work on the encryption-related issues and locate relevant publications on their websites 2) using existing grey literature databases to search

1. Identifying organisations that work on encryption-related issues

The members of the Global Encryption Coalition (GEC), which promotes and defends encryption in key countries and multilateral fora where it is under threat, provided a list of organisations whose work was closely tied to encryption. The comprehensive list of members was screened to exclude organisations and companies that did not have a working website in English and that did not publish research on encryption. Screened members were then categorised into the following five geographical categories:

- Global North (including Five Eyes countries)
- Pan Asia Pacific
- Pan Africa
- Pan Latin America (including Central American and Caribbean)
- General (where no country or region was specifically mentioned)
- N/A (where region or country is not relevant)

2. Grey literature databases
   i. Social Science Research Network: a platform for the dissemination of early-stage research prior to publication in academic journals.
   ii. OpenGrey: a multidisciplinary European database, covering science, technology, biomedical science, economics, social science and humanities.

Inclusion and exclusion criteria

The inclusion /exclusion criteria is as follows:

- *Types of information included were:*
  - Press releases
  - Consultation responses

- Position papers
- Open letters
- Committee reports
- Conference papers/ proceedings
- Working papers
- Gov report/ white papers
- Policy documents
- Research reports
- Technical reports

- *Range of research:* Qualitative, quantitative, empirical studies

- *Geographical location:* As the findings of the REA focussed largely on the Global North, there was a concerted effort to locate information from countries and regions that the REA did not cover. However, there were no set limits on the geographical scope.

- *Time:* The search results were limited to studies published from 2000 – 2021 because it was in 2000 that the Advanced Encryption Standard (AES) was first introduced as a much stronger option to replace the Data Encryption Standard (DES), which had become vulnerable to brute-force attacks. Presently, AES is widely used to encrypt data at rest (i.e. on devices) and data in transit such as in wireless communications. A good example of this would be communications via encrypted messaging apps like WhatsApp.

- Results that did not answer two research questions were excluded.

- Results that did not meet the Authority, Accuracy, Coverage, Objectivity, Date, Significance (ACCODS) framework that was adapted for this systematic search were excluded. The AACODs framework, developed by Jess Tyndall at the Flinders University, is used as a tool to critically appraise grey literature sources as grey literature sources may bypass a peer-review process which may result in varying quality. The AACODS framework was adapted as follows:

Authority	Associated with a reputable organisation? Is the organisation reputable? (e.g. UN)
Accuracy	Does the item have a clearly stated aim or brief? Is it representative of work in the field? If No, is it a valid counterbalance?
Coverage	Are any limits clearly stated?
	Eg: Country, stakeholders groups
Objectivity	Does the work seem to be balanced in presentation?
Date	2000 - present date
Significance	Does it enrich or add something unique to the research? Does it strengthen or refute a current position?

Literature management

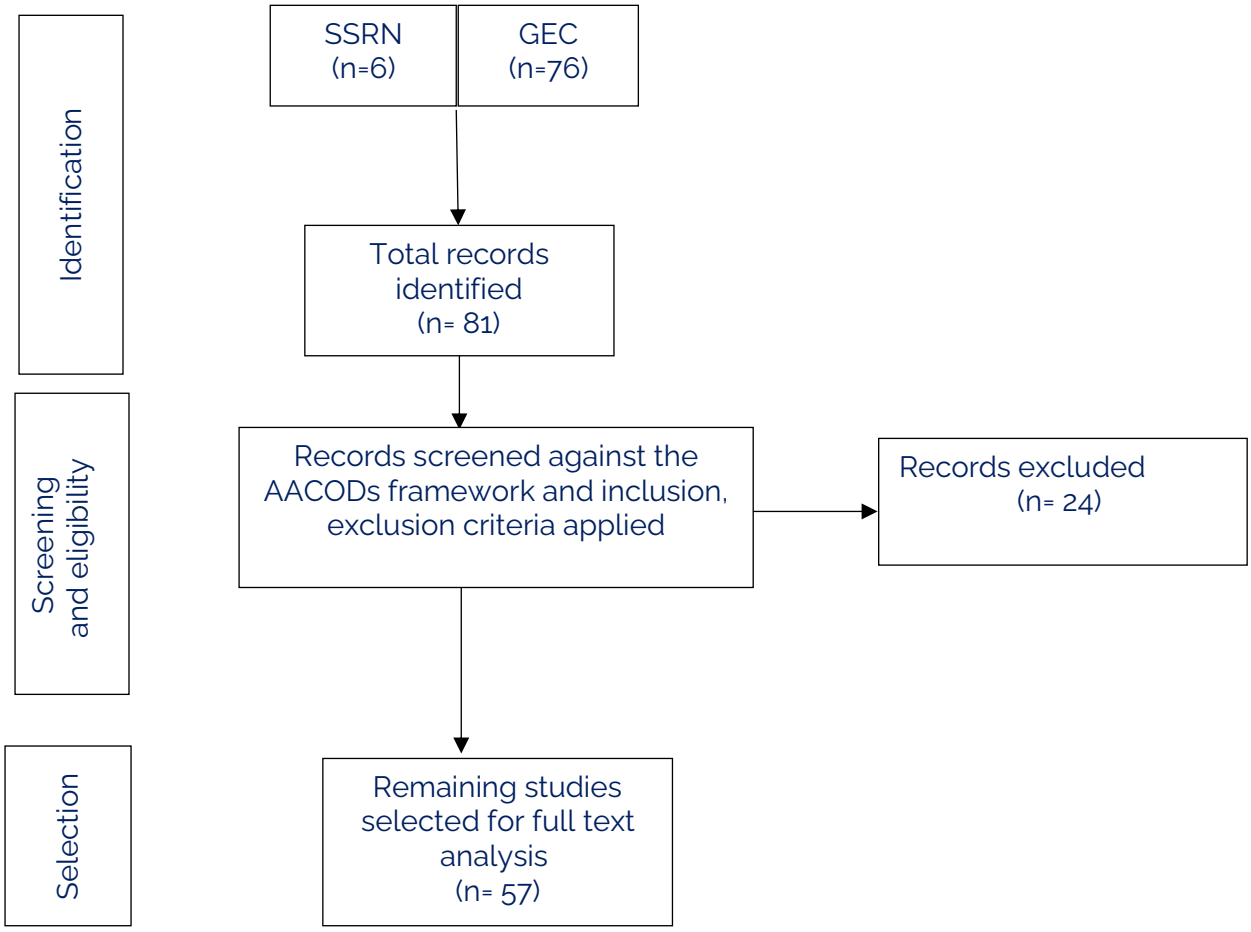
- Zotero is the preferred reference manager as it a free open-source software thereby making it accessible to all team members. With grey literature, it was easy to add links to specific publication sites through the web-browser plug-in.

The shared feature folders enable multiple team members to work on Zotero simultaneously.

Selection of studies

- This review includes qualitative, quantitative, mixed methods and empirical studies

Included Studies (PRISMA Framework)



Strategy for data synthesis

The final 57 articles included were read for the following questions:

- Is it for or against weakening encryption?
- Who are the winners and losers of weakening encryption?
- What lenses does it look at the issue from? Ie: Socio-political, economic, privacy, technical
- What are the justifications for weakening encryption?
- What are the impacts for weakening encryption?

References of articles read at full text for the systematic grey literature review

1. Herpig DS. A Framework for Government Hacking in Criminal Investigations [Internet]. 2018. Available from: https://www.stiftung-nv.de/sites/default/files/a_framework_for_government_hacking_in_criminal_investigations.pdf
2. Gillmor DK, Stanley J. A Little-Known Privacy Battle Is Being Waged Over Encrypting the Nuts and Bolts of the Internet [Internet]. American Civil Liberties Union2019 [cited 2021 Aug 9];Available from: https://www.aclu.org/news/privacy-technology/a-little-known-privacy-battle-is-being-waged-over-encrypting-the-nuts-and-bolts-of-the-internet/

3. ACLU. ACLU v. US Department of Justice [Internet]. American Civil Liberties Union2020 [cited 2021 Aug 9];Available from: https://www.aclu.org/cases/aclu-v-us-department-justice

4. Encryption Europe. An Introduction to Encryption Europe [Internet]. Position Paper2021 [cited 2021 Aug 10];Available from: https://encryptioneurope.eu/positionpaper/

5. Bhandari V, Bailey R, Rahman F. Backdoors to Encryption: Analysing an Intermediary's Duty to Provide "Technical Assistance" [Internet]. Rochester, NY: Social Science Research Network; 2021 [cited 2021 Aug 13]. Available from: https://papers.ssrn.com/abstract=3805980

6. Article 19. Blockchain and Freedom of Expression [Internet]. [cited 2021 Aug 13];Available from: https://www.article19.org/wp-content/uploads/2019/07/Blockchain-and-FOE-v4.pdf

7. Article 19. Brazil: WhatsApp services blocked nationwide in violation of freedom of expression [Internet]. ARTICLE 192016 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/brazil-whatsapp-services-blocked-nationwide-in-violation-of-freedom-of-expression/

8. The Citizen Lab. Canada's New and Irresponsible Encryption Policy: How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy [Internet]. The Citizen Lab2019 [cited 2021 Aug 10];Available from: https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/

9. Prostasia Foundation. Civil Society Coalition Letter: EARN-IT ACT [Internet]. [cited 2021 Aug 10];Available from: https://prostasia.org/wp-content/uploads/2020/09/Civil-Society-Coalition-Letter-EARN-IT-Act-9.15.20.pdf

10. Article 19. Coalition Letter to Ministers Responsible for the Five Eyes Security Community [Internet]. 2017 [cited 2021 Aug 10];Available from: https://www.article19.org/data/files/medialibrary/38820/Coalition-Letter-to-5eyes-Govs.pdf

11. Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)Canadian Internet Policy and Public Interest Clinic. Coalition Objects to Renewed Calls for Weaker Encryption Following "Five Eyes" Ottawa Meeting [Internet]. CIPPIC2017

[cited 2021 Aug 9];Available from: https://cippic.ca/en/news/coalition_objects_to_renewed_calls_for_weakened_encryption_following_5eyes_ottawa_meeting

12. Madsen W, Banisar D. Cryptography and Liberty 2000 [Internet]. Electronic Privacy Information Center2000 [cited 2021 Aug 10];Available from: https://epic.org/reports/crypto2000.html/

13. OECD. Digital Identity Management: Enabling Innovation and Trust in the Internet Economy [Internet]. OECD; 2011 [cited 2021 Aug 10]. Available from: https://www.oecd.org/sti/ieconomy/49338380.pdf

14. Open Rights Group. DNS Security: Getting it right. Recommendations for policy makers and technologists [Internet]. Open Rights Group2019 [cited 2021 Aug 10];Available from: https://www.openrightsgroup.org/app/uploads/2020/03/ORG_DNS_Security_Report_.pdf

15. Article 19. Egypt: Telecommunication Regulation Law Legal Analysis [Internet]. Egypt: Telecommunication Regulation Law2015 [cited 2021 Aug 10];Available from: https://www.article19.org/data/files/medialibrary/37966/Egypt-telecoms-report---English.pdf

16. Singh A. Encryption and anonymity in digital communications : new report by UN Special Rapporteur on freedom of expression David Kaye [Internet]. The Citizen Lab2015 [cited 2021 Aug 9];Available from: https://citizenlab.ca/2015/05/encryption-and-anonymity-in-digital-communications-new-report-by-un-special-rapporteur-on-freedom-of-expression-david-kaye/

17. LGBT Tech. Encryption Essential for the LGBTQ+ Community [Internet]. [cited 2021 Aug 10];Available from: https://docs.wixstatic.com/ugd/699ad7_d6ba4d9d03f649b8aba9035b8df88bde.pdf

18. CPJ. Encryption Letter to Obama [Internet]. 2015 [cited 2021 Aug 10];Available from: https://cpj.org/wp-content/uploads/2015/05/Encryption_Letter_to_Obama_final_0519155B15D-1.pdf

19. Article 19. EU: Civil society challenges EU plans to expand biometric mass surveillance [Internet]. ARTICLE 19 [cited 2021 Aug 13];Available from: https://www.article19.org/resources/civil-society-challenges-eu-plans-biometric-surveillance/

20. Article 19. EVENT: Surveillance State- What do Anonymity and Encryption mean for the UK? [Internet]. ARTICLE 192015 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/event-surveillance-state-what-do-anonymity-and-encryption-mean-for-the-uk/

21. Liguori C. Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate [Internet]. Rochester, NY: Social Science Research Network; 2020 [cited 2021 Aug 10]. Available from: https://papers.ssrn.com/abstract=3606601

22. Herpig S. Government Hacking: Computer Security vs. Investigative Powers [Internet]. 2017 [cited 2021 Mar 8]. Available from: https://www.stiftung-nv.de/sites/default/files/snv_tcf_government_hacking-problem_analysis_0.pdf

23. Herpig DS. Government Hacking: Global Challenges [Internet]. Stifung Neue Verantwortung; 2018 [cited 2021 Aug 10]. Available from: https://www.stiftung-nv.de/sites/default/files/government_hacking_akt.feb_.pdf

24. ACLU. Government Rescinds Gag on Secret Surveillance Order After ACLU Intervenes [Internet]. American Civil Liberties Union2016 [cited 2021 Aug 9];Available from: https://www.aclu.org/press-releases/government-rescinds-gag-secret-surveillance-order-after-aclu-intervenes

25. Stisa Granick J. In Latest Encryption Battle with Apple, Justice Department Still Wrong [Internet]. American Civil Liberties Union2020 [cited 2021 Aug 10];Available from: https://www.aclu.org/news/privacy-technology/in-latest-encryption-battle-with-apple-doj-still-wrong/

26. India: Tech firms should uphold privacy, free speech [Internet]. ARTICLE 19 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/india-tech-firms-should-uphold-privacy-free-speech/

27. Penney J. Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study [Internet]. Rochester, NY: Social Science Research Network; 2017 [cited 2021 Aug 18]. Available from: https://papers.ssrn.com/abstract=2959611

28. Article 19. Joint Civil Society Statement on Encyrption [Internet]. [cited 2021 Aug 10];Available from: https://www.article19.org/wp-content/uploads/2020/11/20201106-Joint-Civil-Society-Statement-on-Encryption.pdf

29. Civil Society Organisations, Technology Companies, Trade Associations, Security and Policy Experts. Joint letter to international governments to support encryption [Internet]. Open Rights Group2019 [cited 2021 Aug 11];Available from: https://www.openrightsgroup.org/publications/joint-letter-to-international-governments-to-support-encryption/

30. Dheri P, Cobey D. Lawful Access & Encryption in Canada: A Policy Framework Proposal [Internet]. Rochester, NY: Social Science Research Network; 2019 [cited 2021 Aug 10]. Available from: https://papers.ssrn.com/abstract=3470957

31. Myanmar: Scrap Cyber Security Draft Law and Restore Full Internet Connectivity [Internet]. ARTICLE 19 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/myanmar-scrap-cyber-security-draft-law-and-restore-full-internet-connectivity/

32. General CG-DD & Organizations Caution Policy Makers Against Encryption “Backdoors” [Internet]. lgbttech2019 [cited 2021 Aug 13];Available from: https://www.lgbttech.org/post/2019/12/10/organizations-caution-policy-makers-against-encryption-backdoors

33. Article 19. Pakistan: New Cybercrime Bill Threatens the Rights to Privacy and Free Expression Legal Analysis [Internet]. 2015 [cited 2021 Aug 10];Available from: https://www.article19.org/data/files/medialibrary/37932/Pakistan-Cybercrime-Joint-Analysis_20-April-2015.pdf

34. Wilson A, Park C. Privacy's Best Friend [Internet]. New America Open Technology Institute2020 [cited 2021 Aug 9];Available from: http://newamerica.org/oti/reports/privacys-best-friend/

35. CPJ. Re: Call for comments regarding the development of a report on the legal framework governing the relationship between freedom of expression and the use of encryption to secure transactions and communications, and other technologies to transact and communicate anonymously online [Internet]. 2015 [cited 2021 Aug 10];Available from: https://cpj.org/wp-content/uploads/2015/02/Letter-Encryption-02-10-15.pdf

36. Response to the call for inputs into a report on "Privacy: A Gender Perspective" by the United Nations Office of the Special Rapporteur on the Right to Privacy : A Gender Perspective [Internet]. IT for Change2019 [cited 2021 Aug 9];Available from: https://itforchange.net/sites/default/files/add/IT%20for%20Change%20-%20Privacy_%20A%20Gender%20Perspective.pdf

37. Article 19. Right to Online Anonymity [Internet]. Right to Online Anonymity2015 [cited 2021 Aug 10];Available from: https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf

38. Russia: 50+ NGOs urge UN to challenge restrictions to online expression and digital privacy [Internet]. ARTICLE 19 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/russia-ngos-call-on-un-to-challenge-restrictions-to-information-online-and-digital-privacy/

39. Article 19. Russia: Blocking Telegram is a serious violation of freedom of expression and privacy [Internet]. ARTICLE 192018 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/russia-blocking-telegram-serious-violation-freedom-expression-privacy/

40. Article 19. Russia: Telegram block leads to widespread assault on freedom of expression online [Internet]. ARTICLE 192018 [cited 2021 Aug 10];Available from: https://www.article19.org/resources/russia-telegram-block-leads-widespread-assault-freedom-expression-online/

41. Article 19. Rwanda: 2016 Law Governing Information and Communication Technologies Legal Analysis [Internet]. 2018 [cited 2021 Aug 10];Available from: https://www.article19.org/wp-content/uploads/2018/05/Analysis-Rwanda-ICT-Law-April-2018.pdf

42. Article 19. Senegal: Analysis of selected Internet regulation [Internet]. 2015 [cited 2021 Aug 10];Available from: https://www.article19.org/data/files/medialibrary/37908/Senegal-legal-analysis-EN.pdf

43. Gill L, Israel T, Parsons C. Shining a Light on the Encryption Debate: A Canadian Field Guide [Internet]. The Citizen Lab2018 [cited 2021 Aug 9];Available from: https://citizenlab.ca/2018/05/shining-light-on-encryption-debate-canadian-field-guide/

44. Moraes T. Sparkling Lights in the Going Dark: European Data Protection Law Review 2020;6(1):41–55.

45. ISOC Switzerland Chapter. Statement: ISOC Switzerland Chapter Concerned over Reports that EU Plans to Weaken Encryption - ISOC Switzerland ChapterISOC

Switzerland Chapter [Internet]. ISOC Switzerland Chapter2020 [cited 2021 Aug 10];Available from: https://www.isoc.ch/archives/4065

46. Henrique Atta P, Moraes T. Summary Report on the judgement of ADPF n° 403 and ADI n° 5.527: The WhatsApp Case [Internet]. LAPIN2020 [cited 2021 Aug 10];Available from: https://lapin.org.br/en-gb/2020/05/29/summary-report-on-the-judgement-of-adpf-no-403-and-adi-no-5-527-the-whatsapp-case/

47. Article 19. Thailand: Computer Crime Act Legal Analysis [Internet]. 2017 [cited 2021 Aug 10];Available from: https://www.article19.org/data/files/medialibrary/38615/Analysis-Thailand-Computer-Crime-Act-31-Jan-17.pdf

48. Callas J. The "Ghost User" Ploy to Break Encryption Won't Work [Internet]. American Civil Liberties Union2019 [cited 2021 Aug 9];Available from: https://www.aclu.org/blog/privacy-technology/ghost-user-ploy-break-encryption-wont-work

49. Ruane K. The EARN IT Act is a Disaster for Online Speech and Privacy, Especially for the LGBTQ and Sex Worker Communities [Internet]. American Civil Liberties Union2020 [cited 2021 Aug 9];Available from: https://www.aclu.org/news/free-speech/the-earn-it-act-is-a-disaster-for-online-speech-and-privacy-especially-for-the-lgbtq-and-sex-worker-communities/

50. Herpig S, Schuetze J. The Encryption Debate in Germany: 2021 Update [Internet]. Carnegie Endowment for International Peace; 2021 [cited 2021 Mar 8]. Available from: https://carnegieendowment.org/files/202104-Germany_Country_Brief.pdf

51. Demas A, Escobedo F. The FBI is Secretly Breaking Into Encrypted Devices. We're Suing. [Internet]. American Civil Liberties Union2020 [cited 2021 Aug 9];Available from: https://www.aclu.org/news/privacy-technology/the-fbi-is-secretly-breaking-into-encrypted-devices-were-suing/

52. Deeks A. The International Legal Dynamics of Encryption [Internet]. Rochester, NY: Social Science Research Network; 2020 [cited 2021 Aug 10]. Available from: https://papers.ssrn.com/abstract=3587438

53. Diab R. The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking-Bombs, and the Future of the Encryption Debate [Internet]. Rochester, NY: Social Science Research Network; 2019 [cited 2021 Aug 10]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3393172

54. O'Shea L, Thomas E. The Role of Encryption in Australia : A Memorandum [Internet]. Access Now; 2018 [cited 2021 Aug 9]. Available from: https://digitalrightswatch.org.au/wp-content/uploads/2018/01/Crypto-Australia-Memo.pdf

55. UN HRC: Protecting rights online requires States to address violence against women in digital contexts [Internet]. ARTICLE 19 [cited 2021 Aug 13];Available from: https://www.article19.org/resources/un-hrc-protecting-rights-online-requires-states-to-address-violence-against-women-in-digital-contexts/

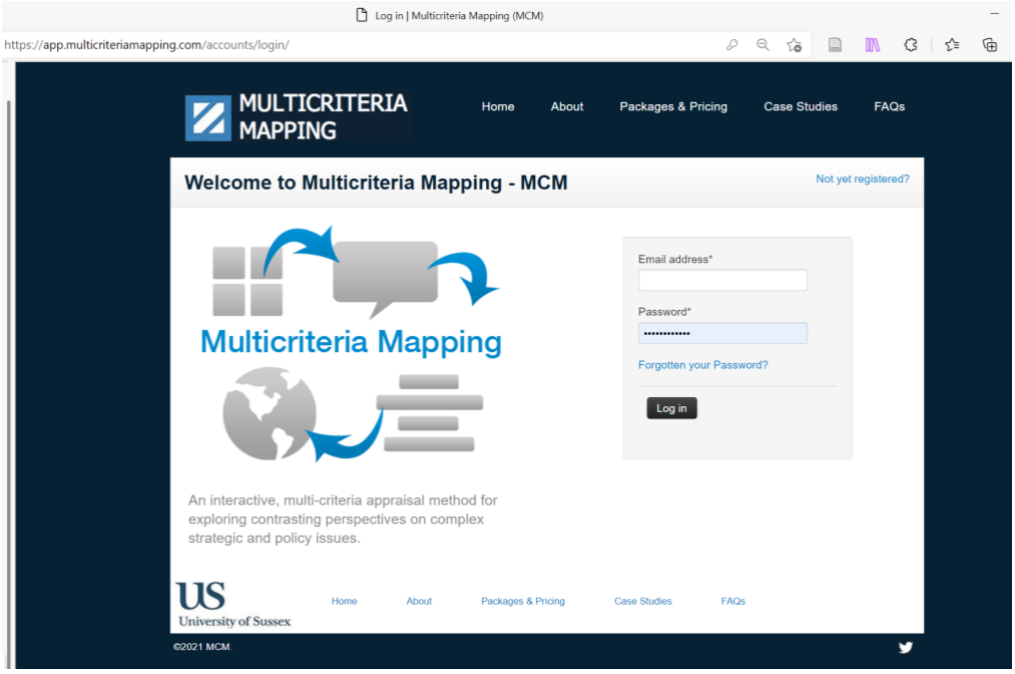
56. UN: To protect privacy in the digital age, world governments can and must do more [Internet]. ARTICLE 19 [cited 2021 Aug 9];Available from:

https://www.article19.org/resources/un-to-protect-privacy-in-the-digital-age-world-governments-can-and-must-do-more/

57. Gurumurthy A. WhatsApp Challenges Govt: Breaking End-to-End Encryption Will Lead to Security Issues but Timing of Petition Circumspect [Internet]. IT for Change2021 [cited 2021 Aug 9];Available from: https://itforchange.net/whatsapp-challenges-govt-breaking-end-to-end-encryption-will-lead-to-security-issues-but-timing-of

Appendix 3 MCM Tool and Interview Guide

Developed by the Science Policy Research Unit at the University of Sussex, MCM is an interactive, multicriteria decision analysis (MCDA) method for exploring contrasting perspectives on complex, uncertain and contested issues. It aims to help 'open up' technical assessment by systematically 'mapping' the practical implications of alternative options, knowledges, framings and values.[1]



About page of MCM tool website

Normalisation and Aggregation Procedures in MCM[2]

The MCM process uses a linear additive weighting aggregation model based on the simple weighted average of option performance. While *P* is the inputted performance score for a given option under a stated factor, *C* represents inputted performance scores across all options under the same stated factor.

$P_{ij}^{min}, P_{ij}^{max}$: nominal minimum/maximum performance score for option *i* under factor *j* (as keyed into MCM tool)

C_j^{min}, C_j^{max}: nominal minimum/maximum performance score across all options under factor *j* (as keyed into MCM tool)

n_j: nominal weighting for factor *j* (as keyed into MCM tool)

$C_j^{min} = \min\,(P_{1j}^{min}, P_{2j}^{min}, \ldots, P_{mj}^{min})$: minimum performance score *C* across all options *P* under factor *j* (determined by MCM tool)

[1] https://www.multicriteriamapping.com/about
[2] Adapted from: http://users.sussex.ac.uk/~prfh0/Rethinking%20Risk.pdf; http://users.sussex.ac.uk/~prfh0/MCM_Manual.pdf

$C_j^{max} = \max(P_{1j}^{max}, P_{2j}^{max}, \ldots, P_{mj}^{max})$: maximum performance score *C* across all options *P* under factor *j* (determined by MCM tool)

A. Normalisation of performance scores and weights

The scores and weights inputted in the MCM tool are normalised using the below equations.

1. $s_{ij} = P_{ij}^{normalised} = \frac{P_{ij} - C_j^{min}}{(C_j^{max} - C_j^{min})} (\min = 0, max = 1)$

2. $w_j = n_j^{normalised} = \frac{n_j}{\sum_j n_j} (sum = 1)$

Equation 1 means that the normalised performance score for the *i*th option under the *j*th appraisal factor (s_{ij}) is the ratio of the difference between the performance measure determined for that option (P_{ij}) and that for the lowest-performing option (C_j^{min}) with the difference between the performance measures determined for the highest (C_j^{max}) and lowest (C_j^{min}) performing options under that factor (i.e. *j*).

Equation 2 means that the normalised factor weights for the *j*th appraisal factor (w_j) is the ratio of the nominal weighting for factor *j* (n_j) with the summation of all n_j values across all options under that factor (i.e. *j*).

B. Aggregation of normalised performance scores using normalised weights

The normalised performance scores are then aggregated with the below equation. This equation means that the overall performance rank obtained for the *i*th choice option (r_i) is the sum of the performance scores determined for that option under the *j*th appraisal factor (s_{ij}) each multiplied by the importance weighting on that factor (i.e. w_j).

$$r_i = \sum_j w_j . s_{ij}$$

Calculation of MCM outputs (charts)

Equations behind this calculation of ranks from weights and normalised scores are outlined in the following steps (performed by MCM tool):

For each interviewee in the selected perspective and for each factor in the selected issue:

1. multiply pessimistic normalised scores by normalised weights; this is 'pessimistic (worst-case) subrank'.
2. multiply optimistic normalised scores by normalised weights; this is 'optimistic (best-case) subrank'.
3. subtract pessimistic subrank from optimistic subrank; this is 'delta'.
4. sum half delta with pessimistic subrank; this is 'median'.

Encryption Pros and Cons: Interview Guide

**This interview guide was sent to all interviewees via email before their interview.*

Purpose of research

This research aims to answer the overarching research question: *What should policymakers be aware of and consider in their decisions concerning the restricting of encryption technologies?*

Encryption is the process of scrambling data so that only those with the 'keys' can understand what is being shared. It is commonly used to protect 'data in transit'; the transmission of data across computer networks including the Internet, and 'data on a device '; the storage of data on computer systems. End-to-end encryption for example can protect data in transit, as it ensures the sender and the recipient of a piece of data are the only parties who can view it and no third parties can access the data.
Due to encryption's capabilities, this technology has become vital for the fabric of the Internet in ensuring security, confidentiality, and privacy in our online interactions. However, given its inherent features, it is prone to abuse by malicious actors, who avail themselves of the confidentiality encryption affords to conduct criminal behaviour.

Based on this malicious activity, there is a growing global regulatory trend pushing for the weakening ofthis technology through the introduction of so called 'back-doors', which would allow regulators and law enforcement to access encrypted communications. This would create a technological point of failure in encryption's infrastructure which could be exploited, jeopardising the protection that encryption provides to so many.

This project seeks to guide policy decision-makers in the encryption debate by producing:
- An Impact Assessment exploring the risks and benefits of restricting encryption.
- A Decision-making Framework that can guide policymakers in their decisions concerning the restriction of encryption technologies.

The Interview

The interview is semi-structured and the concepts discussed will be shaped by your own opinions and experiences you choose to discuss in the interview. Therefore, no prescriptive or close-ended questions will be asked. Instead, we aim for broader concepts to be discussed. These concepts include:

- Impacts of restricting encryption.
- Criteria that should be considered when making encryption-related policy decisions.

These impacts and criteria could be economic, social, political, legal or technical. This is by no means anexhaustive or prescriptive list, rather an indication of the breadth of impacts that we welcome to be discussed in this interview.

Multicriteria Mapping (MCM) questions

The running of the interview is inspired by the Multicriteria Mapping tool, created by the University of Sussex's Science Policy Research Unit (SPRU). The MCM process is depicted in Figure 1 below.

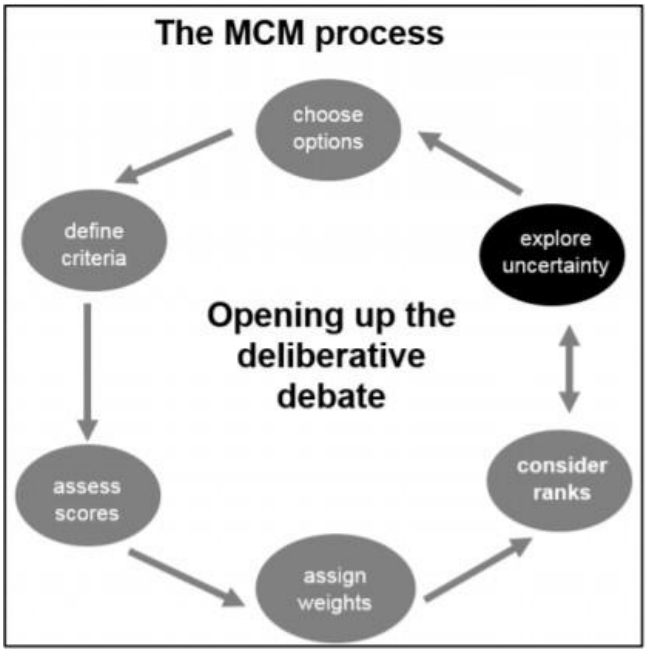


Figure 1 MCM Process

This interview will follow the MCM process of selecting and appraising different options and criteria concerning encryption-related policy decisions. You will be asked the following broad questions:

- Why is encryption and which aspects of encryption important to you?
- Concerning the work you do, at what point is encryption most relevant or important to you? I.e. at rest, in transit
- In your opinion, what are the main factors you consider when evaluating these options?
- What should decisionmakers consider before they decide on an option?
- Why is this factor important to consider?
- How would you score and weight these factors in your decisions about the encryptiondebate?
- What is your reason for this score or weight?

After these questions have been asked, you will have the opportunity to reflect on your choices and beable to edit anything you have said. More details about each stage of the process can be found below in the 'Multicriteria MappingInterview Guide'

Multicriteria Mapping Interview Guide

1. Reviewing Options

In this first step, you will be asked to review policy options concerning the restricting ofencryption technologies.

Core options are those that have been defined by the research team. You are asked to appraiseall the core options.

Core Option 1: Restrict encryption technologies through technical

Key features: Use technical tools to restrict encryption

Description: Entails overt or direct technical interference by state actors to decrypt encrypted data or communications. Examples include using a key escrow system whereby service providers or Internet intermediaries are required to store copies of decryption keys with state-appointed third parties. The possibility that encryption may be weakened in the future using new technologies like quantum computing is also noted.

Core Option 2: Restrict encryption through non-technical means

Key features: Use non-technical tools to restrict encryption

Description: Implies state actors employing indirect means to access encrypted data and communications. Examples include governments issuing mandates for compelled disclosure of decryption keys, warrants requiring technical assistance from service providers and fines if this assistance is not provided. Other non-technical means include import/export controls restrictions on encryption technologies.

Core Option 3: Do not restrict encryption

Key features: Encryption not to be restricted at all.

Description: No means; either technical or non-technical, should be employed to restrict encryption.

2. Defining Factors

You will now be asked to define factors. Factors are characteristics or aspects that influenceyour judgements over the performance of the encryption related options presented above.

Factors can be grouped in whatever way is meaningful to you. *For example, you could create amain factor group and call it 'Human rights factors', and within that group have sub-factors suchas 'Right to privacy and 'Freedom of expression'.* We recommend choosing a maximum of 4 factors

3. Assigning Scores

In this stage, you will be asked to assign scores to express your judgement about the level ofimpact that each factor would have under each option, taking into account both the most optimistic (best case scenario) and the most pessimistic conditions (worst case scenario). In each case, please indicate the main reasons for your judgement.

We recommend scoring ranges from 0 - 100, where lower scores indicate worse impact of thefactor under the option, and higher value scores indicate better impact.

One way to start scoring is to begin with a high score for whatever seems factor clearly has thebest impact, or a low score for whatever seems to clearly have the worst. Then you can fill in middle-performing options one by one.

If you are unsure what score to assign, please treat this as 'uncertainty' and let us know this sowe can make a note of it.

4. Assigning Weights

This is an opportunity for you to assign more subjective weightings to the factors according tohow much you considered these factors in the options earlier discussed.

Weighting will range from 0 – 100, where 0 indicates you did not consider this factor at all whenconsidering the options, and 100 indicates you only considered this factor when considering theoptions.

You can apply relative weights to your factors. Please make your weights express the sameproportions as fractions of 100 ie: the sum of all your weights should add up to 100.

End of MCM Interview Guide

This worksheet was developed using the guidance offered by the University of Sussex'sScience Policy Research Unit's Multicriteria Mapping Tool software.

Encryption Pros and Cons

Interviews

28th July 2021

Research team

Zoe Tilsiter

Project Manager

Adeola Akinla

Quality and Risk Officer

Kirthika Selvakumar

Communications Officer

Ayesha Gulley

Ethics Officer

Context

Encryption is a vital technology for the fabric of the Internet which ensures **security, confidentiality and privacy** in the interactions we have and transactions we conduct online. However, given its inherent features, it is prone to abuse by malicious actors, who avail themselves of the confidentiality encryption affords to break the law or commit otherwise objectionable conduct.

On account of encryption's negative flipside, there is a growing global regulatory trend pushing for the **weakening of this technology** through the introduction of so-called '**back-doors',** which would essentially allow regulators and law enforcers to have access to encrypted communications. This would create a **technological point of failure** which would eliminate the protection that encryption provides for all.

Research Objectives

Project Rationale

This project seeks to guide decision-makers in the encryption debate, by highlighting the impacts of weakening encryption would have on various stakeholders, including **law enforcement, industry, and civil society**. These stakeholders will benefit from it by becoming informed on the benefits and trade-offs to weakening encryption through various perspectives. These insights are intended to further guide policy deliberations on encryption.

Overarching Research Question :

What should policymakers be aware of and consider in their decisions concerning the restricting of encryption technologies?

Agenda

• Introduction and overview of research objectives	10 mins
• Review of options and generation of factors	20 mins
• Break	5 mins
• Scoring of options and weighting	45 mins
• Wrap up	5 mins

Multicriteria Mapping

Developed by the Science Policy Research Unit (Uni of Sussex), multi-criteria mapping aims to authentically represent a range of different appraisals to understand which factors different stakeholders would consider and prioritise in policy decisions concerning encryption.

1 **Options**

A set of core options has been defined for appraisal.

2 **Factors**

Define factors that influence your judgments over the performance of the Options. Please define a maximum of 4 factors.

3 **Scores**

Evaluate the relative impact of different options under each factors using a scale from 0-100 to 'score'.

4 **Weighting**

Assign more subjective weightings to the factors using a scale from 0-100.

Initial Questions

As a stakeholder:

- Why is encryption important to you?
- Which aspects of encryption are important to you?
- Concerning the work you do, at what point is encryption most relevant or important to you? i.e. at rest, in-transit.

Review Options

Option 1: Restrict encryption (technical)

Key features: Use technical means to restrict encryption

Description: Mainly concerns employing technical means to access encrypted data or communication. Examples of these means include using a key escrow system to store copies of decryption keys. There is also the future possibility of encryption being weakened by new technologies such as quantum computing.

Option 2: Restrict encryption (non-technical)

Key features: Use non-technical means to restrict encryption

Description: Mainly concerns governments issuing legislation or regulation to give law enforcement exceptional access to encrypted communications for reasons related to public safety. These mandates include compelled disclosure of decryption keys, issuing warrants intercept communications or mandating technical assistance from service providers and fining them if this assistance is not provided.

Option 3: Do not restrict encryption

Key features: Encryption not to be restricted at all.

Description: No means; either technical or non-technical, should be employed to restrict encryption

Options

- What are your thoughts on these options?
- Which is the option you would prefer governments adopt?
- Why this option? Why this option over the others?

Factors

- What are the main factors you consider when evaluating these options ?
- What are the key features and descriptions of this factor?
- Why is this factor important to consider?
- What should decision makers consider before they decide on an option?
- What are the impacts or considerations that you think would arise out of these options?
- What risks or benefits are involved?

Please define a maximum of 4 factors

5-minute break

Scores

- Scores express your judgement of the relative impact of each option under each factor taking into account both the most optimistic (best case scenario) and the most pessimistic conditions (worst case scenario).
- In each case, please indicate the main reasons for your judgment.
- Scoring ranges from 0 - 100,
  - 0 is an extremely negative impact of the option under the factor
  - 50 is a neutral impact of the option under the factor
  - 100 is an extremely positive impact of the option under the factor
- One way to start scoring is to begin with a high score for whatever seems clearly best, or a low score for whatever seems clearly worst. Then you can fill in middle-performing options one by one.
- If you are unsure what score to assign, please treat this as 'uncertainty' and let us know this so we can make a note of it.

Weights

- Assign more subjective weightings to the factors according to how much you considered these factors in your selection of options concerning restricting encryption.
- In your opinion, what is the relative importance of the factors in making these encryption-related decisions?
- Weighting will range from 0 – 100
    - 0 indicates you did not consider this factor at all when considering the options
    - 100 indicates you only considered this factor when considering the options.

- The sum of all your weights should add up to 100.

Thank you

steapp.encryption@ucl.ac.uk

Appendix 4 Coding Process

As discussed in the report, interviewees generated 66 factors that they deemed important to consider when making encryption-related policy decisions. These factors were qualitatively coded. Qualitative coding involves identifying general themes from data collected. The purpose of this coding is to assist with data analysis, by identifying themes, similarities, and points of difference across the data collected. The coding conducted was 'open coding', where the themes were constructed and grouped from the bottom-up, directly informed by the interviewees' responses. The coding was also done iteratively, moving between broader issues and more specific issues as more explicit themes emerged and as codes were refined.

This qualitative coding involved two steps. The first involved identifying the interviewees' 66 factors and initially grouping them into general emerging themes, known as factor codes. This can be seen in the figure below.

Human rights	Cybersecurity considerations	Economic	Trust in government/state actors	Public Safety	Impacts on different groups in society	Purpose/ specific use case of encryption	Nature of government	Impact on digital realm	Legal context	Systems operability
Free communication	New vulnerabilities	Business considerations	Abuse by state actors	Victim support	Protect vulnerable LGBT people	Necessity/ Proportionality	Precedent	Regressing technology	Legal landscape	System complexities
Fundamental Human rights	Critical Services	Commerce and competitiveness	Elevated LEA powers	Public safety	Safety of activists	Proportionality	System of government	Digital ecosystem	Legal	Ease of use
Human rights	System integrity	Consumer trust	Surveillance	Efficiency to solve crime	User safety	Purpose	Historical context	Lawless online spaces		
Human rights	Cybersecurity	Economic competitiveness	Role of government	Proactive scanning	Distributional impacts	Data retention	Political			
Human rights	Cybercrime and corruption	Economic liberalisation	Trust in LEA and governments	Security						
Individual rights	Cybersecurity (digital)	Innovation and choice	Trust in government							
Privacy	Data security	Trust in the platform	Trust in state actors							
Privacy	Fraud risk	Openness of the internet								
Privacy	Security									
Privacy										
Privacy (digital rights)										
Privacy (human rights)										
Privacy and anonymity										
Right to privacy										
Rights Protection										
Speech and expression										
Privacy context										
Digital rights										

Initial Grouping of Interviewee Factors into General Factor Codes

The second step involved further grouping these factors into factor subcodes within the identified general themes. This step resulted in 11 factors codes and 33 factor sub-codes being identified, which can be seen in Table 2 in Section 3.2.1 of the report.

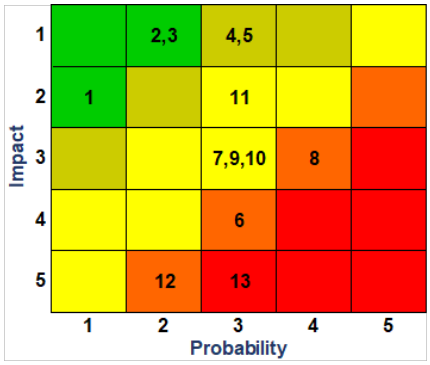
Appendix 5 Risk Management Table

Table 1: Project Risks Classification and Mitigation

Risk ID #	Task Area	Risk Description	Risk Category	Risk Source	Risk Type	Risk Rating	Project Phase	Status (Open/ Closed)	Mitigating Action(s)
1	Stakeholder engagement sessions (interviews and focus groups)	Stakeholders affected by COVID19 may be unable or unwilling to engage in research activities.	Resource	External	PMR	A	1,2	Open	• Engage participants in the early stages of the project and use digital collaboration tools to conduct interviews and focus group sessions. • Identify possible multiple participant groups which would provide redundancies if some groups become unavailable or inaccessible. • Timely escalation of constraints to Project Lead and Project Partner to avoid extended delays to the project.
2	Data collection, transcription, and storage	Participants' data may be unintentional ly leaked.	Operational	Internal	PMR	A	2,3	Open	• Ensure adherence to the team's data management protocol. • Encrypt collected data and store on UCL-managed infrastructure (OneDrive) and not on individual laptops.
3		Participants' identities may be inadvertently exposed or reassembled from leaked data.	Operational	External & Internal	PMR	A	2,3	Open	• Anonymise participants' data to avert identification. • Collected data shall not be matched across sources, profiled, or subjected to automated decision-making procedures.
4		Team members may selectively seek out and interpret evidence that agrees with or confirms their preconceptio ns about the encryption debate.	Bias	Internal	ACR	B	2, 3	Open	• Individually and collectively explore opposing arguments to preconceived ideas, and hypotheses. • Deliberately seek evidence which counters our preconceptions. • Rotate evidence review across the team to obtain broader and lateral interpretation of evidence.
5		Team members may overly rely on readily available information or evidence.	Bias	Internal	ACR	B	2,3	Open	• Seek out diverse stakeholder perspectives from external and internal sources. • Leverage our diversity in knowledge, experience and skills during data collection and analysis.
6		Project timelines for data collection may be extended due to delayed response from the UCL Ethics Committee.	Operational	Internal	PMR	D	2,3	Open	• Adopt purposive sampling in selecting participants. • Prioritise engaging with prospective participants within Partner's and the team's networks. • Conduct data analysis in parallel with collection activities.

Risk ID #	Task Area	Risk Description	Risk Category	Risk Source	Risk Type	Risk Rating	Project Phase	Status (Open/ Closed)	Mitigating Action(s)
7		Participants may be unavailable during the summer months.	Operational	External	PMR	C	2	Open	• Leverage Partner's network to negotiate workable timelines with participants. • Schedule participants with prior commitments for interviews/focus groups ahead of others.
8		Time zone conflicts may hinder certain groups of participants from engaging in the focus group sessions.	Operational	External	PMR	D	2	Open	• Coordinate participants into groups with similar time zones. Where this is not possible, we shall resort to conducting separate interviews with affected participants.
9		Participants may be led to provide responses that reflect their biases.	Bias	External	ACR	C	2	Open	• Frame questions in balanced language that does not overly promote or diminish prevailing narratives around the research topic. • Develop variant multicriteria mapping models that address multiple perspectives of our research problem.
10		Non-verbal cues from the participants may be missed as interviews and focus groups would be conducted virtually.	Operational	External	ACR	C	2	Open	• Limit focus group participants to 3-5 to enable live interactions and smooth moderation.
11	Team dynamics	Team members may become unavailable due to illness, personal circumstances etc.	Resource	Internal	PMR	C	1,2,3	Open	• Agreed team contract to ensure accountability from each team member. • Principles of communication to guide conflict management/resolution. • Each team member is assigned dual roles to act in the absence of the primary role owner. • All documentation (reports, minutes etc.) are maintained in a central location on MS Teams for easy access by team members. • Tracking of tasks/activities via project management tool (Notion) to keep team updated of due dates etc.
12	Project Partner engagements	Project Partner may step down from the project due to conflicting commitments.	Resource	External	PMR	D	1,2,3	Closed	Project Partner signed the project engagement contract on 26th May 2021.
13	Unknown risks	Risks yet to materialise	N/A	N/A	N/A	E	2,3	Open	• Assess impact of risk against project timelines and reprioritise tasks or activities if required. • Apply existing mitigating actions where applicable.

Note:
ACR – Analytic Component Related
PMR – Project Management Related



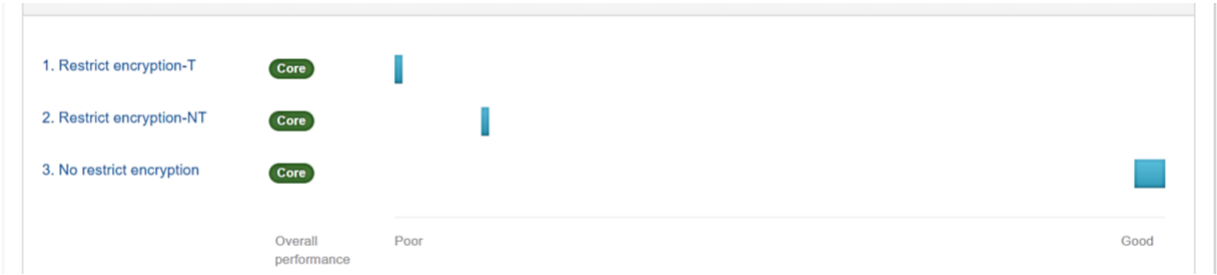
Legend

A	A	B	B	C	A: Very Low/Trivial
A	B	C	C	D	B: Low/Tolerable
B	C	C	D	E	C: Medium/Moderate
C	C	D	E	E	D: High/Substantial
C	D	E	E	E	E: Very High/Intolerable

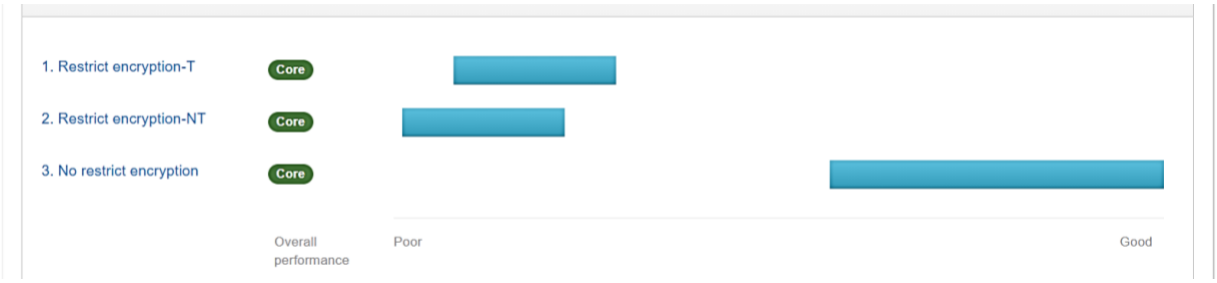
Appendix 6 Interviewee Comments

Longer bars indicate elements of uncertainty, variability or sensitivity (for which assumptions and/or contextual information was provided) in the interviewees' evaluation of the options, while shorter bars indicate less uncertainty, variability or sensitivity.

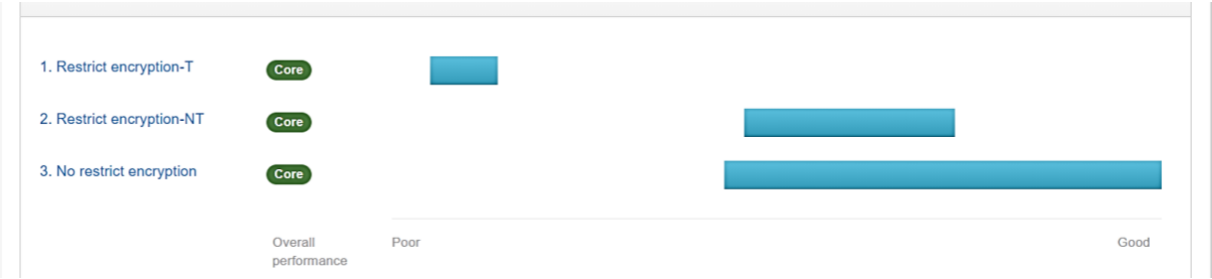
6.1.1 Individual Ranks Charts – Civil Society Perspective



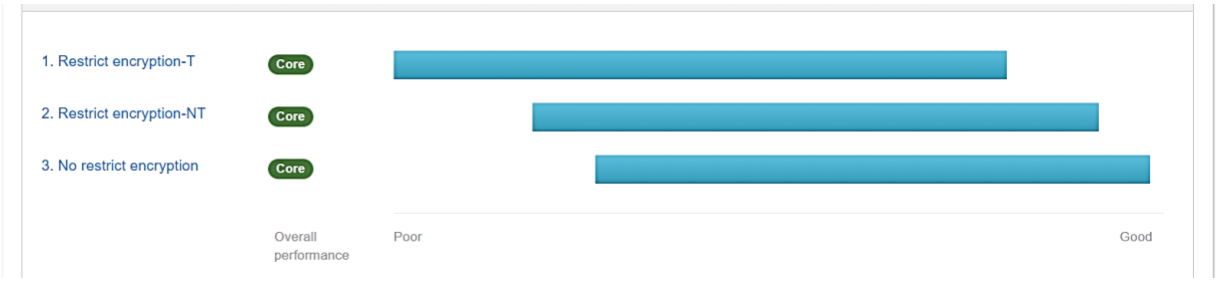
CS-Ranks chart 1: Access Now



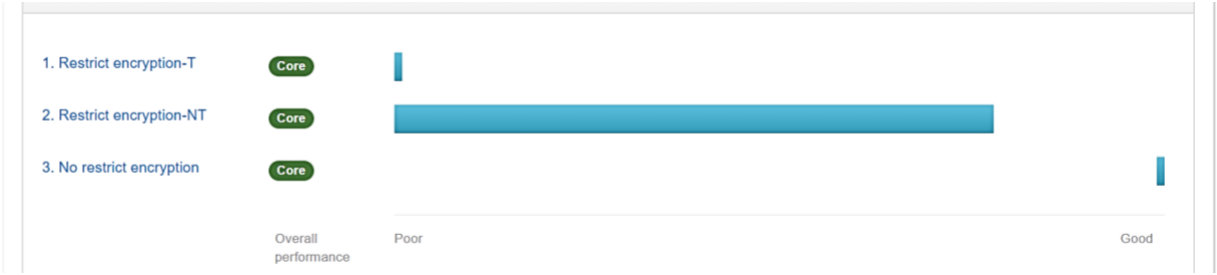
CS-Ranks chart 2: Anonymous Think Tank



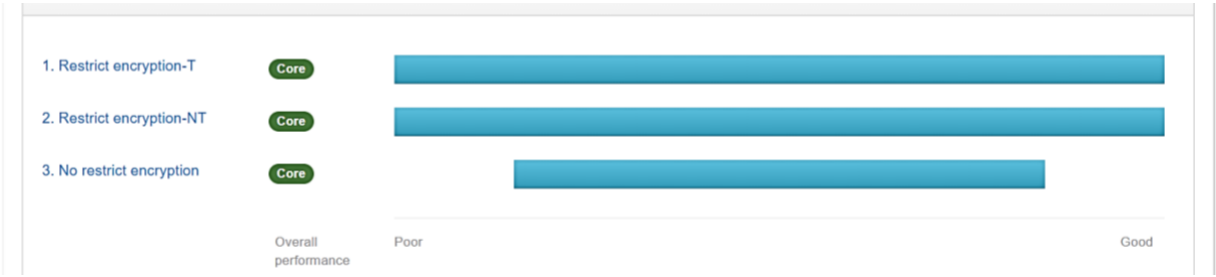
CS-Ranks chart 3: Collaboration on International ICT Policy for East and Southern Africa (CIPESA)



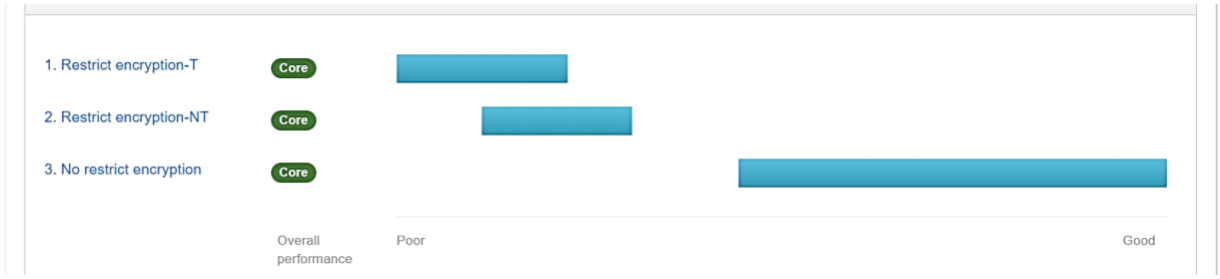
CS-Ranks chart 4: Digital Empowerment Foundation (DEF)



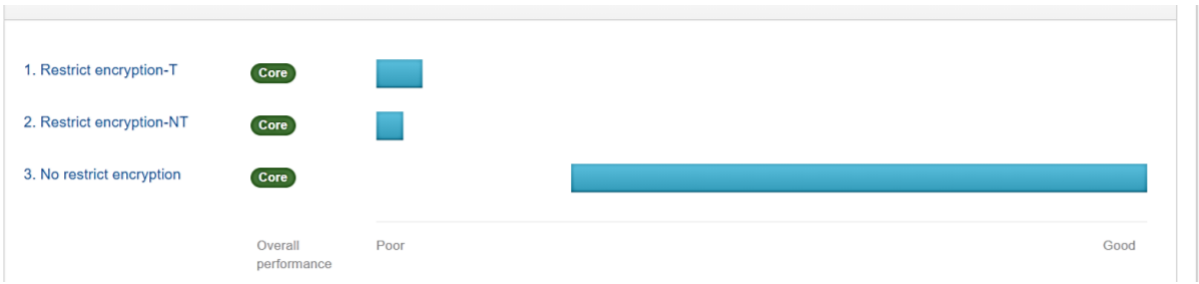
CS-Ranks chart 5: European Digital Rights (EDRi)



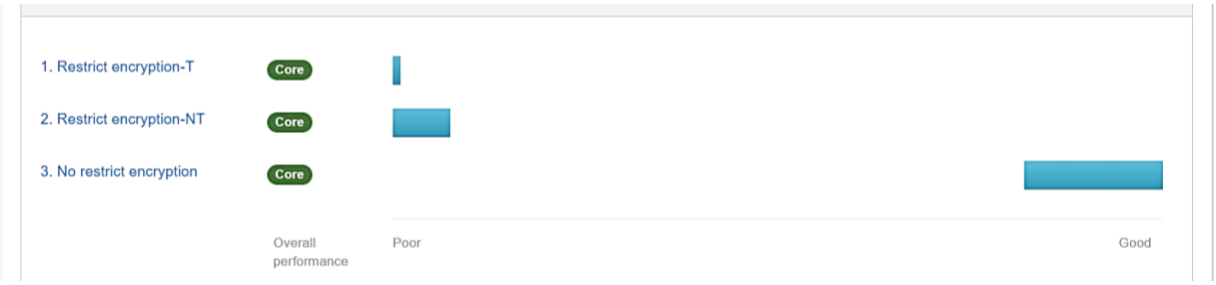
CS-Ranks chart 6: Future of Privacy Forum (FPF)



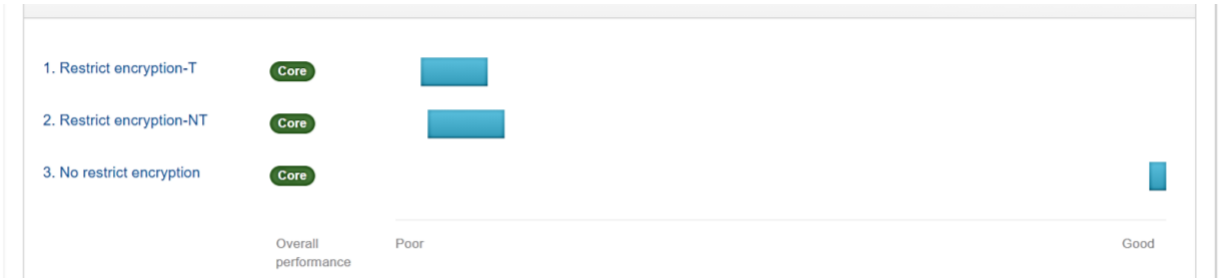
CS-Ranks chart 7: Anonymous Digital Rights Group 1



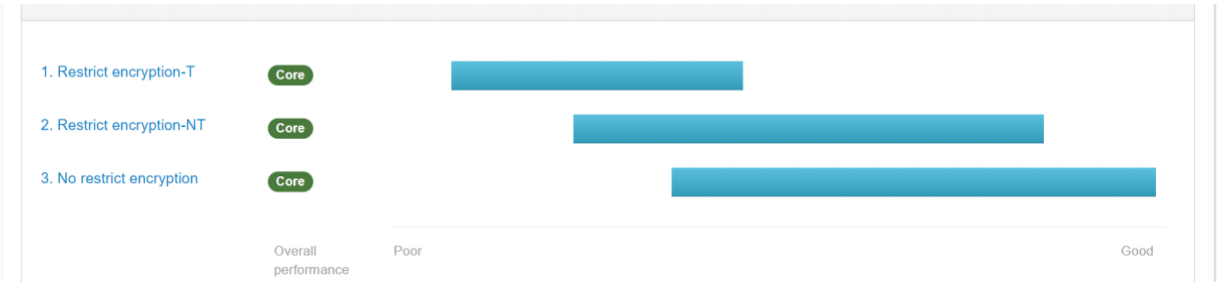
CS-Ranks chart 8: IT for Change



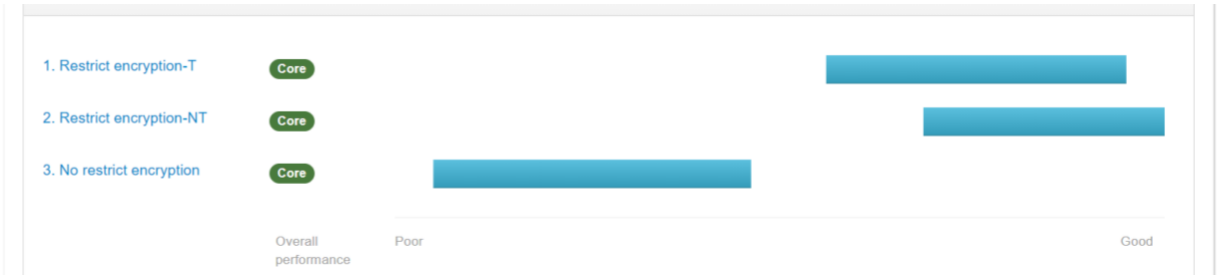
CS-Ranks chart 9: LGBT Tech



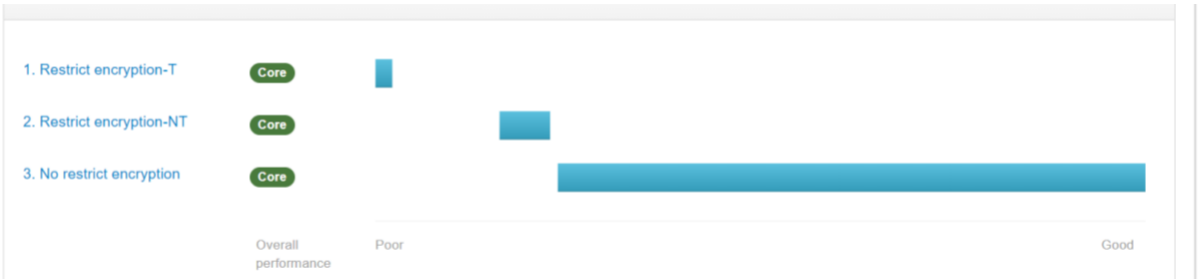
CS-Ranks chart 10: Open Rights Group (ORG)



CS-Ranks chart 11: Paradigm Initiative (PIN)

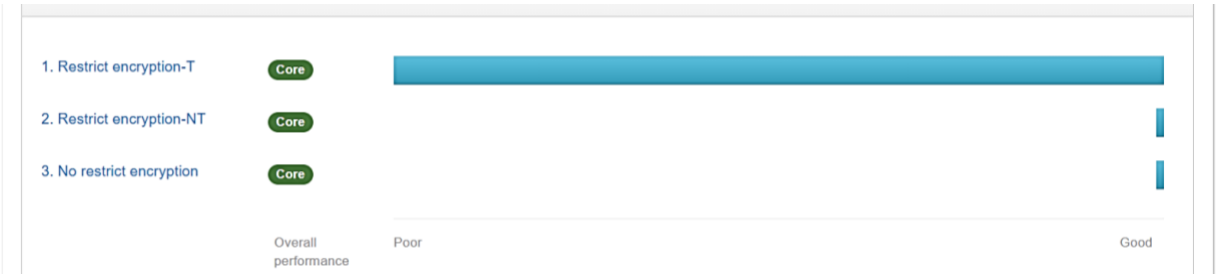


CS-Ranks chart 12: Anonymous Digital Rights Group 2

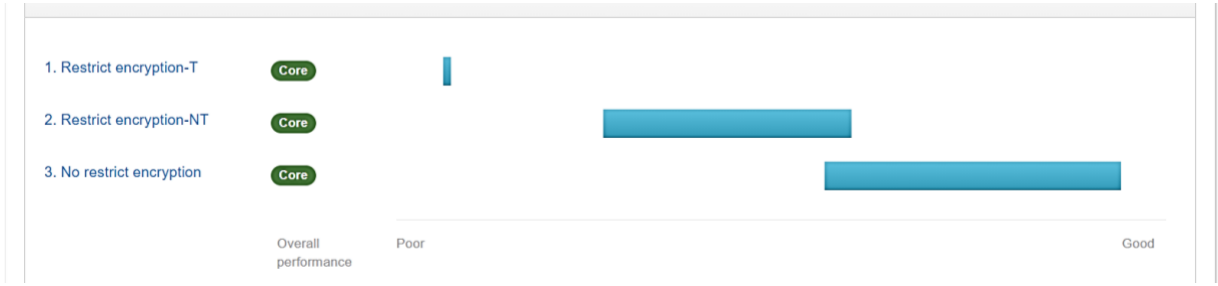


CS-Ranks chart 13: Software for Freedom Law Centre (SFLC)

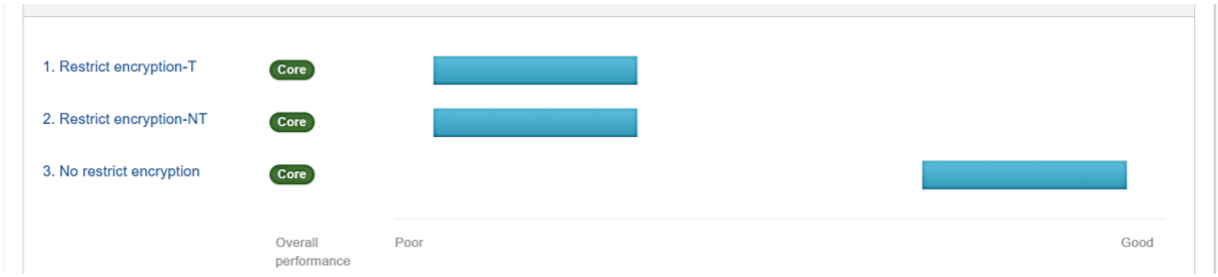
6.1.2 Individual Ranks Charts – Industry Perspective



Ind-Ranks chart 1: Anonymous Financial Services Provider

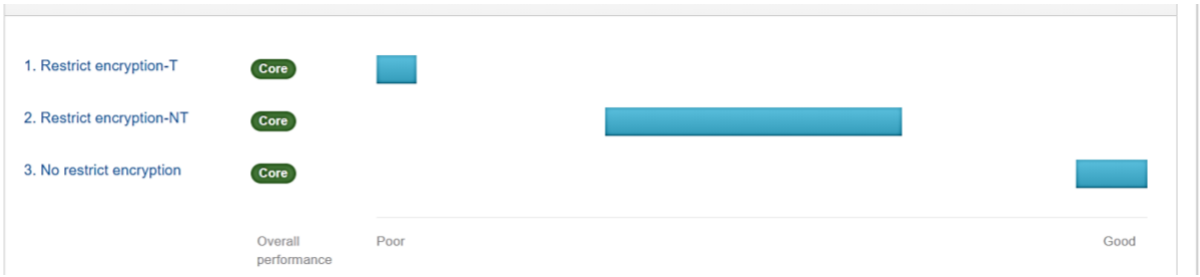


Ind-Ranks chart 2: ProtonMail



Ind-Ranks chart 3: Anonymous Encrypted Messaging Service

6.1.3 Individual Ranks Charts – Policymaker Perspective



PM-Ranks chart 1: Anonymous Policymaker

6.2.1 Rank-related comments – Civil Society Perspective

> If procedures are correctly implemented, less vulnerable to abuse by bad actors. Score is better than a technical means as if non-technical means were done properly there it is less likely to be abused.

> Hotline and law enforcement are trained to detect criminal activity. Would improve if they can access encrypted communications and identify criminals and bringthem to justice. Small chance that it is subject to abuse. There are other ways of manipulating the system.

Anonymous Digital Rights Group 2 – on Option 2 being preferred as it enables improved crime detection

> Non technical measures such as legal contractual or organizational measures supplement the technical measures as other ways to restrict encryption. Thus, there is no difference between using a nontechnical or technical means to restrict encryption, both are problematic.

> In the worst case, not restricting encryption creates a societal problem. This is due to not being able to push back on behaviors that are detrimental to our society, i.e., terrorism, cross-border crime, better policing (on an individual basis) --- state surveillance (from a societal perspective).

Future of Privacy Forum – on not seeing distinction between options 1 & 2

6.2.2 Rank-related comments – Industry Perspective

> Fundamental human right in democractic societies and entitled to disclose publicly what you would like to and that is only an option with strong encryption

> Any intrusion on privacy has to performed on the on user device and not on the 'technology' therefore private information is better protected. Metadata still exists, but its not as important for privacy (more of a risk to security than privacy)

ProtonMail – on benefit of encryption to privacy and how E2EE may be circumvented

> E2EE is fundamental to people's ability to communicate with a guarentee of privacy (acknowledging E2EE not a complete solution to privacy but a good effort)

Anonymous Encrypted Messaging Service – on E2EE not complete solution to privacy

> Encryption is primarily important to us because it secures customer transactions and enables us to comply with Financial Conduct Authority (FCA) regulations such as verifying customer identities during account management procedures.
>
> Compared to messaging services, we do not implement E2EE as a we run a ledger management system that encrypts data in transit and at storage. Customer transactions are encrypted on their devices and when in transit to our servers, thereby preventing interception by unauthorised parties (sniffing, man in the middle attacks etc). Although these data are also encrypted on our servers, our operations staff can access and view these data as required. As banking regulations apply to us, these data may also be disclosed as required. For example, if law enforcement agents (LEA) request banking or transaction information, we are required by FCA regulations to comply by surrendering the information.
>
> Distinguishes between how government interception may occur on messaging platform and on financial platforms. For messaging platforms, government may intercept messages in transit or require platforms to retain messages for longer duration so they can later access these messages with a retrospective order (essentially options 1 & 2). This does not apply to financial platforms as we do not have to peer to peer communications.
>
> Implies that we already implement a version of option 2 since financial transactions may be disclosed to LEA upon request (via a subpoena) during an investigation. In a sense, this version of option 2 is safeguarded by regulations and frameworks as specified in the FCA. However, is averse to deliberate weakening of encryption through technical backdoors or vulnerabilities to facilitate interception.

Anonymous Financial Services Provider – on position on encryption

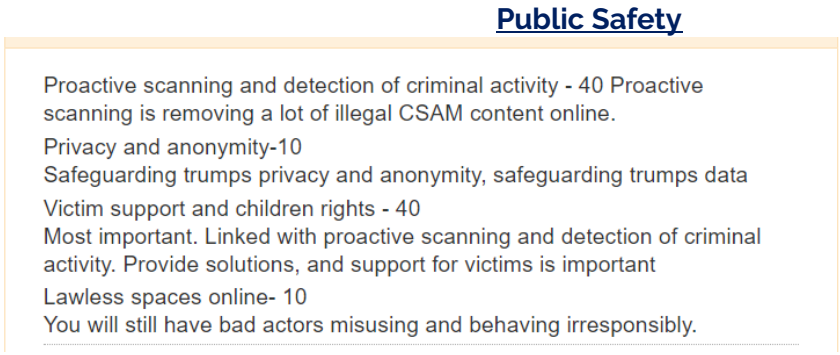
6.2.3 Rank-related comments – Policymaker Perspective

> Protecting encryption entrenches/strengthens the prominence, awareness and accountability of fundamental rights, society and markets.

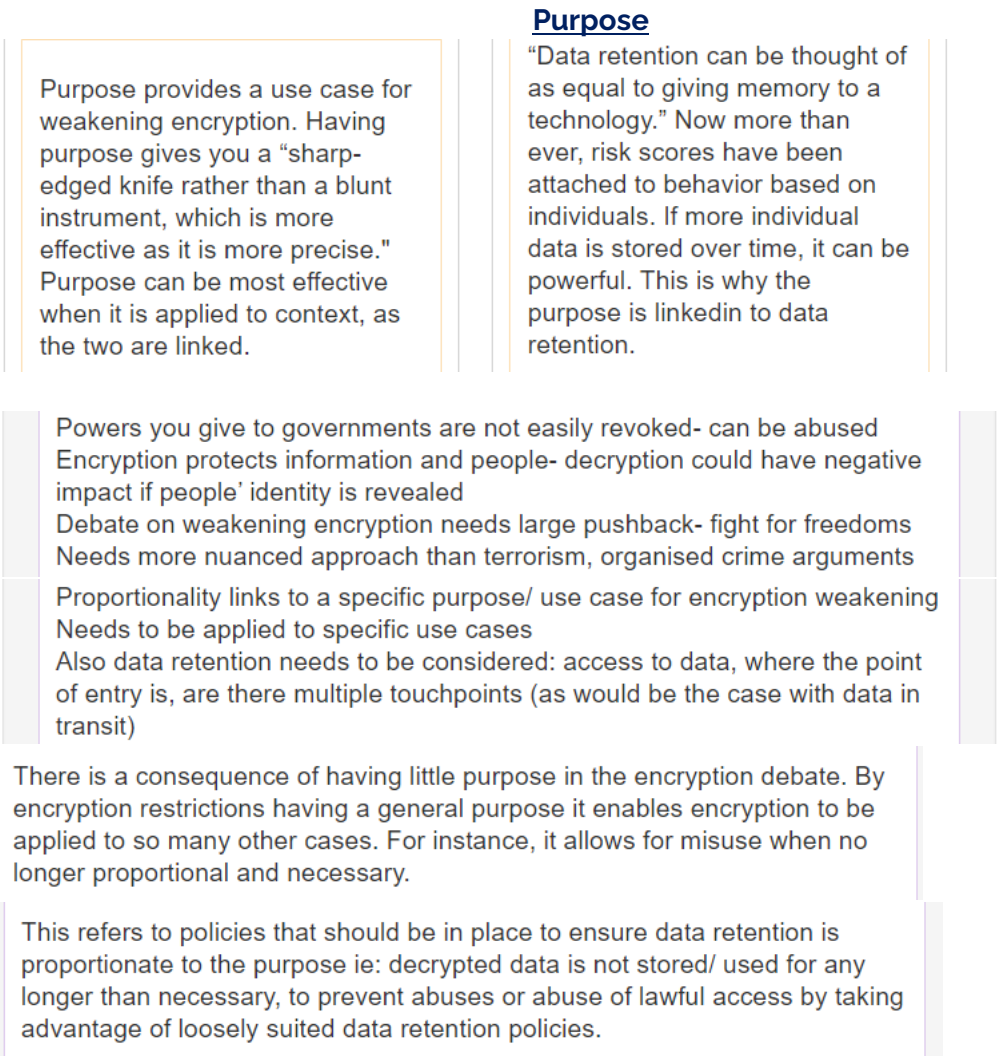
> Possibility of increased disinformation, escalating hate speech; lack of awareness of more systemic problems. May prompt need to redefine privacy and security in an online environment - especially when considering the range of services available to consumers.

Anonymous Policymaker – on rationale for option 3

6.3.1 Rationales for Weights – Civil Society Perspective



CS-Weights Rationales 1: Anonymous Digital Rights Group 2 – on public safety



CS-Weights Rationales 2: Future of Privacy Forum – on purpose of weakening encryption

Strong importance on proportionality and upholding fundamental rights. Without adhering to the Charter and passing the necessity and proportionality tests, an act is not legal. This would be a gross interference on the law.

CS-Weights Rationales 3: European Digital Rights (EDRi) – on purpose of weakening encryption

Human rights

Legal landscape- 25- laws define possibilities for defending oneself.

What laws exist to protect victims of abuse? What laws exist to hold the government accountable? Legal landscape indicates intended use of restricted encryption; if the legal landscape is more rights respecting than security focused, then they could endorse technical options.

CS-Weights Rationales 4: Paradigm Initiative – on prioritising legal landscape

Human rights: are critical to encryption, freedom of expression, privacy, assembly - role of gov and distributional impacts fall under this.

CS-Weights Rationales 5: Access Now

Human rights - 50:
Because we live increasingly digital lives, if individual and cybersecurity are undermined, society would be negatively impacted on a large scale because human rights would essentially be rendered useless.
User data is not private and secure and is prone to being accessed by state actors (privacy breaches, Freedom of Encryption, Freedom of Association, self-censorship).

As we become increasingly dependent on digital technologies, undermining encryption would create negative impacts on a range of human rights including the ones specified.

It is difficult to delineate between online and offline living; access to the Internet enables us to receive a range of services – healthcare, education, work – and if we cannot use the Internet safely due to undermined encryption we are put at risk. Denied access impacts both on and offline life.

An example of how this encroaches on human rights is during Internet shutdowns which have ripple economic and social effects. People are unable to access websites, or trade online and must resort to using workarounds like VPNs.

CS-Weights Rationales 6: Anonymous Digital Rights Group 2

Privacy, confidentiality and anonymity -30
Co-factors with trust; my privacy is not guaranteed on an untrustworthy platform.

CS-Weights Rationales 7: Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Individual rights (35). Highest. If you keep these the highest, then you will never be flouting policies and always meeting policies taking care of human rights. This is basis for creating a democracy

CS-Weights Rationales 8: Digital Empowerment Foundation (DEF)

Privacy - 50:
Fundamental human right enabled by encryption.

CS-Weights Rationales 9: IT for Change

50 - Privacy - is the biggest concern for LGBT

CS-Weights Rationales 10: LGBT Tech

Fundamental human rights - 20: There is a slight awareness of these rights on the individual level but this factor is more critical at the international level.

Added 3 weeks, 1 day ago

Digital Rights - 20: These can be subjective especially as a number of people are unaware of these rights until a problem arises.

CS-Weights Rationales 11: Open Rights Group (ORG)

Fundamental right to privacy : 40. Highest. If privacy in ensured, the freedom of speech and expression would be automatically safeguarded by the privacy of communications and systems. All other factors are co-related this factor.
Freedom of speech and expression - 20

CS-Weights Rationales 12: Software for Freedom Law Centre (SFLC)

Privacy is clearly important, as it is a fundamental right that needs safeguarding.

CS-Weights Rationales 13: Future of Privacy Forum

If you achieve necessary and proportionality principles privacy would be respected.

CS-Weights Rationales 14: European Digital Rights (EDRi)

Impacts on society groups

30 - Privacy and the protection of vulnerable communities is often lost in the encryption debate.

CS-Weights Rationales 15: LGBT Tech

10 - The lower score for distributional impacts is in part covered in the importance of human rights and part of it is because of tactical effectiveness being only so much of a defense.

CS-Weights Rationales 16: Access Now

Safety (security) of human rights defenders and activists - 10
CIPESA's programme areas are broad, so as much as safety and security of human rights defenders are important, there are other factors which are more important on a general scale, like privacy. Work with different actors, so considers the overall well-being of the Internet landscape.

Weights Rationales 17: Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Trust in government/state

Trust- 35- Trust is at core. Breach of trust is the basis of breaking encryption discussion.

CS-Weights Rationales 18: Paradigm Initiative (PIN)

Abuse by power by state actors -20
Several violations committed by state actors in the name of national security.

CS-Weights Rationales 19: Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Trust in state actors - 10:
Embedded in encryption (because trust is necessary for communications and transactions between people).

Added 3 weeks, 1 day ago

Elevated law enforcement - 5:
Access to encryption restricts opportunities for government overreach. Because privacy is already assumed as a fundamental right.

Added 3 weeks, 1 day ago

Surveillance - 5:
Access to encryption restricts opportunities for government surveillance. [LEA should not carry as much weight vs citizen rights]. Because privacy is already assumed as a fundamental right.

Added 3 weeks, 1 day ago

CS-Weights Rationales 20: IT for Change

6.3.2 Rationales for Weights – Industry Perspective

Human rights

> Privacy - 30
> Fundamental human right in democractic societies and entitled to disclose publicly what you would like to and that is only an option with strong encryption

Ind-Weights Rationales 1: ProtonMail

> Freedom of expression is the ability to communicate without concern that a user will be discovered by someone unintended.

Ind-Weights Rationales 2: Anonymous Encrypted Messaging Service

Cybersecurity concerns

> Encryption enables us to comply with FCA regulations. For instance, if a customer wants to change or alter their account information, we are required to verify that they are the legitimate account owner before processing this request. In addition, encryption helps us verify the legitimacy of transactions initiated by customers and prevents their requests from being intercepted by malicious actors.

Ind-Weights Rationales 3: Anonymous Financial Services Provider

> Cyber security (25). Service provider wants to minimise attack surfaces that could pose cybersecurity risks to us as a platform and therefore to users

Ind-Weights Rationales 4: Anonymous Encrypted Messaging Service

Economic

> Encryption for private messaging has become the expectation of private messaging. From a competitive perspective being able to offer a product that does this is essential to functioning of the company.

> Impact on broader integrity of system: Solutions proposed such as 'giving backdoor just to the good guys' is not possible as although intended for one purpose, can cause secondary effects and problems too. Second order impacts coming about as a result of weakening encryption for 'the bad guys'. Eg: 'build a key escrow system to access comms' but this is shown that this creates a problem for good guys too.

Ind-Weights Rationales 5: Anonymous Encrypted Messaging Service

All factors weighted 25: Fraud risk tampers with the integrity of consumer transactions which affects consumer trust that would in turn impact economic competitiveness.

Ind-Weights Rationales 6: Anonymous Financial Services Provider

Security - 32
Most important - is tied to protection of private info and also protects everything that is part of our daily life today, and anything online today. Eg: Banking information

Privacy - 27
Fundamental human right in democratic societies and entitled to disclose publicly what you would like to and that is only an option with strong encryption

Ind-Weights Rationales 7: ProtonMail

Public Safety

Public safety (10). But also important (not to same extent) are secondary societal effects. Broader set of societal impacts can happen on any platforms eg: misinformation, planning an attack. Both are very important but user safety comes first

Ind-Weights Rationales 8: Anonymous Encrypted Messaging Service

Efficiency to resolve crimes - 18
With globalised internet, criminality being without borders. Weak encryption (client side scanning) would provide us with more vision on what is happening in the criminal word and might lead to better outcomes. Though not likely, given the current ability of LEA which is not not well funded and better.

Large scale content surveillance - it could marginally improve detection of criminality. Improves detection of criminal activity. Does not mean the crimes will be solved.

Ind-Weights Rationales 9: ProtonMail

6.3.3 Rationales for Weights – Policymaker Perspective

Purpose

Minimal evidence on proportionality has been gathered and shared openly across EU member states. Minimal understanding of the issues at hand such as those highlighted under the legal factor (capacity and mutual agreements). There needs to a broader conversation of the actual problems beyond "hot topics" like terrorism and CSAM. A broader, all-encompassing view is required of the role encryption plays in criminality and fighting crime.

Human rights

Guided by the International Declaration of Human Rights. Fundamental rights are also enshrined in the EU's treaty. Encryption and its related issues like privacy and security are in the process of legislation in the EU. An example is the current e-privacy proposal that designates encryption as the gold standard for protecting privacy online. Security is also regarded as the backbone of EU cybersecurity initiatives framework. The need to protect encryption is a fundamental pillar of the EU's cybersecurity framework.

Legal context

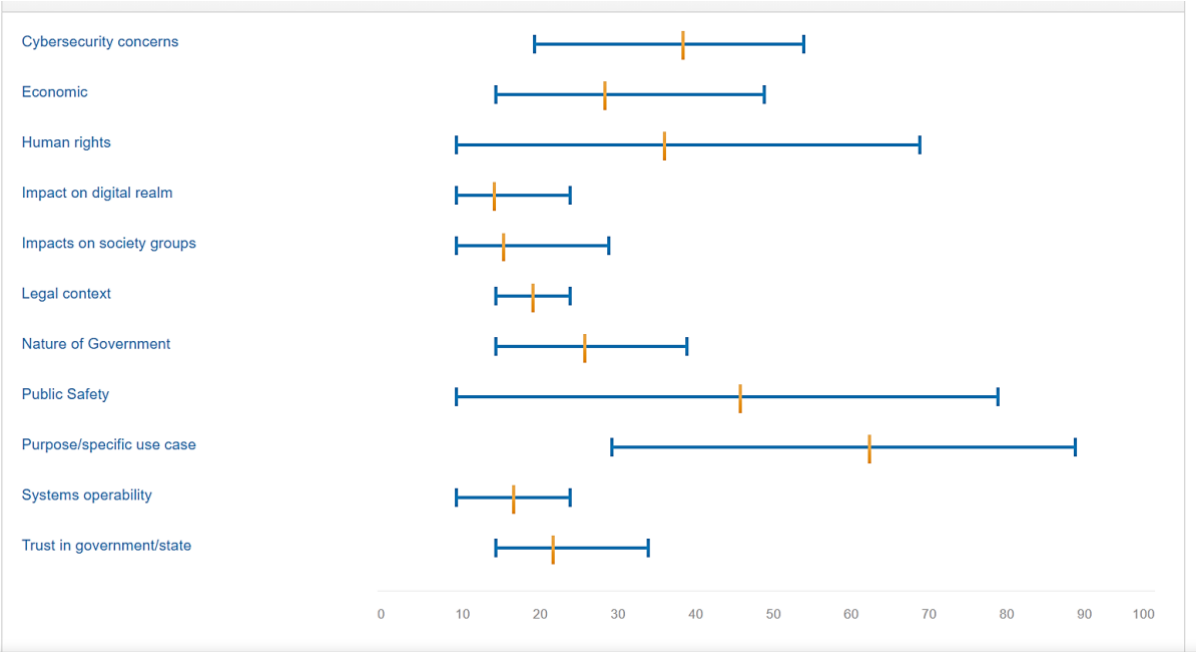
These problems are broadly classified as:
1) Staggering lack of capacity in LEA (police and intelligence authorities) across EU member states to work in an increasingly encrypted environment
2) Extremely weak mutual legal treaties across the EU member states. Challenges persist around sharing e-evidence and data retention in the EU. Legal frameworks apply differently and are currently not designed to resolve cross-border issues stemming from encryption.

Without mutual treaties or increased capacity to understand the implications of encryption legislation, it would be difficult for EU LEA to apply a consistent framework and enforce such legislation.

Nature of Government

There is a false dichotomy of political claims such as strong encryption vs keeping children safe, strong encryption vs organised crime or terrorism etc, which is problematic. The political calls need to be balanced with stronger political awareness, learning and sharing across the other stated factors (proportionality, fundamental rights and legal). Current debates are too entrenched in criminality and conflated with other criminal issues.

6.3.4 Weights graph across all Perspectives



Weights Graph 1: All Perspectives

6.4.1 Interviewee comments on Encryption

> It is important for the discussion around encryption to be more nuanced. There should be high-level principles to guide these discussions rather than the prevailing securitised narrative at play. Given the need to develop solutions that can solve societal problems arising from encryption-related discussions, nuance is necessary.

> It protects the confidentiality and integrity of information which is essential to privacy and supports safe and secure communications which leads people to express themselves freely. Encryption therefore enables people to 'access' these fundamental rights of freedom of expression/privacy by providing them the security that their communicate is secure and confidential. These affordances are essential to vulnerable groups in countries where legal safeguards such as democratic mechanisms or rule of law are lacking.
>
> From a human rights perspective, E2EE and data at rest and in transit are both important, even though it seems most people do not realise that encryption works at both points as they tend to assume their data is safe and secure. However, the rising tide of surveillance practices and general attempts to weaken encryption suggest this may be a wrong assumption. Pegasus is an example of how human rights activists, journalists were spied on despite having E2EE.

General comments on encryption 1: Anonymous Digital Rights Group 1

With how integrated the Internet is in our current society, disruptions to it can prevent citizens from accessing a wide range of regular and critical services including news, healthcare, food, social media etc. Especially important for urban populations in India. If encryption is restricted, there would be increased possibilities of unauthorised access to sensitive information like personal data and payment information. At a minimum, existing offline trust structures and relationships should be emulated in the online environment, and these can be aided by having adequate cryptographic or encryption technology in place.

Encryption also affords secure, secret and private communications between smaller groups of individuals, features that admittedly bad actors exploit to commit crime, and which has inspired calls by state actors (law enforcement agencies) to undermine its use. Nevertheless, the pros of encryption outweigh its cons, so rather than state actors attempt to weaken encryption under the assumption that most citizens exploit it for criminal activity, they should explore more creative means to gather evidence and investigate crime.
Rule of proportionality: cannot just assume that all citizens are suspected criminals and therefore should weaken the entire system. There are other means apart from weakening encryption. Additionally, undermining encryption would excessively tilt the balance of power in favour of state actors because they control internet infrastructure. Encryption provides the technical means for enabling citizens to enjoy the basic right to privacy.

General comments on encryption 2: IT for Change

Increasing need to secure online communications, many use the internet to invoke social change (freedom of assembly must be preserved). Privacy has been hampered with unsecure online communications, yet it is needed to fight social struggles.

General comments on encryption 3: European Digital Rights (EDRi)

In terms of the product we provide, it's a end to end encrypted messaging service platform.

Encryption is at the core to protecting user's privacy. The best way to ensure user privacy is for the company not to be part of user's communications at all, which is why E2EE works.

E2EE ensures only the sender and recipient can see message.

Important from privacy and cyber security perspective. You cannot hack into a message someone does not have. Therefore, if a service provider does not have these messages, they are more secure.

Also very important in terms of company values, protecting vulnerable populations such as LGBTQ, rights defenders, journalists and E2EE can help do this.

General comments on encryption 4: Anonymous Encrypted Messaging Service

> From a thinktank perspective, found the encryption debate straddled several issues spanning democracy, fundamental human rights and global technology for decades. Now from a multilateral perspective, coordinates the encryption debate among governments, institutions and civil society groups in the EU. Coordinating this debate is necessary because it remains very high-level intellectually on both the technical and political sides, with minimal shared understanding in between. If political debates continue along the trajectory of seeking to legislate use of encryption, this could prove detrimental to society in several ways that governments or the broader public does not realise.
>
> Considering current factors in the EU encryption debate, end to end encryption (E2EE) is most important. Believes the work should commence with resolving the issues around E2EE as it is more important.

General comments on encryption 5: Anonymous Policymaker

6.4.2 Interviewee comments on Citizen-State relationship

> Excessive government powers make the role of government increasingly problematic. With issues around data retention and their ability to use the data, data collection facilitates surveillance – violating necessary and proportionality standards (EU fundamental rights).

Citizen-State Relationship 1: Access Now

> Abuse will be present as state actors can easily compel service providers to give this information (state actors may not necessarily obtain legal notices before attempting to intercept encrypted information). Lack of judicial oversight and technical understanding by the judiciary to understand nature of the cybercrimes therefore judges may delay in issuing warrants, or might not issue warrants at all. [long timelines not helpful given high-rate of cyber-crime]

Citizen-State Relationship 2: Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

> The expectation that state actors would not undermine its social contract with citizens through unauthorised access to their private communications.
> Propensity of state to leverage its access to resources (Internet infrastructure, communications networks etc.) to indiscriminately target citizens under the guise of investigating crime.
> The state has existing mechanisms to more easily conduct mass surveillance online.

Citizen-State Relationship 3: IT for Change

> A system that strong encryption does have to rely on trust of a centralised authority. Also speaks about trust in governments and LEA and also of platforms.

Citizen-State Relationship 4: ProtonMail

> Because we live increasingly digital lives, if individual and cybersecurity are undermined, society would be negatively impacted on a large scale because human rights would essentially be rendered useless. User data is not private and secure and is prone to being accessed by state actors (privacy breaches, Freedom of Encryption, Freedom of Association, self-censorship).

Citizen-State Relationship 5: Anonymous Digital Rights Group 1

6.4.3 Interviewee comments on Appraisal of Options

There is no difference between option 1 and option 2 – they are deeply linked to one another. All non-technical legal measures require a technical measure (a technical implementation of it). Therefore, any intrusion upon encryption is a general alteration on how we secure communications. This often has unintended consequences.

Comments on appraisal options 1: Access Now

• Third option is preferred of not restricting encryption.
• Notes that the third option is absolute: it does not reflect the issues that governments are facing in terms of how to balance providing encryption while dealing with CSAM, national security threats like malicious actors who use encryption as tool.
• UK US and Australian government working hard to make encryption look like a criminals tool.
• Option 3 should be followed by government commitment and public education campaign that they are doing in LEA and intelligence community. Today that is super secret.

• Would like to note a fourth option: Unleash encryption and provide 2-way transparency [mutually assured disclosure]. The government needs to not only allow encryption so my bits can be protected. Also need to let you know when and where they might be tracking them, and who I am communicating with.
• I'm more willing to accept certain types of surveillance if I know where, how and why its happening. [Has parallels to algorithmic decision making and when these things are used]
• Eg: Stingray – mass surveillance is an issue, not targeted surveillance
• 50% of solution to tracking down online crime is in the meta data.

Comments on appraisal options 2: Anonymous Think Tank

• Options 1 & 2 geared towards concerns around addressing cyber-terrorism and child online protection for policy makers. Reviewing options 1 & 2 from a civil society perspective, in Uganda, where people are being arrested "unnecessarily", e.g. for "offensive communications", there could be laws backing LEA to access encrypted communications. However, these options would be abused by the state actors in a non-democratic society. The degree of abuse for Option 2 may be less than option 1 because legal procedures would be followed to access encrypted information
• She thinks LEA should have access to encrypted information when a particular crime has been committed subject to developing and following proper standards around accessing encrypted information. Explains her preference for Option 1/2.

Comments on appraisal options 3: Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

To him, Options 1 and 2 collapse into each other as technical means could be mandated by governments. Option 1 could be enabled by legislation too (like option 2 suggests). So to him there is little distinction.
In order to access the data in technical means, governments will still have to issue something to enable this. How the governments do this and whether they prescribe the means they want companies to do this in or not is up to government's discretion. This is the only distinction to him (whether the means are prescribed or whether companies can choose how they do it). But in either case, still telling the company to provide unencrypted data. The only difference would be that if gov prescribes it, companies have less flexibility they should do it.
Option 1 would have to say 'government has prescribed the means of weakening encryption ie: prescribe a backdoor access key', whilst Option 2 would just have to provide government with the data when they ask for it (gov not fussed how they do it, as long as they do it'. It would then be up to the service provider to build technical means eg: wiretapping
Therefore there could be a distinction between how specific technical means data will be accessed. But the company would still have to come up with technical means to do so even if forced to, so the distinction is minimal
So he'd pick option 2 if it did not prescribe companies to have to build in a backdoor to provide data and companies were open to choose how they wanted to provide the data to government. This would be marginally less bad than option 1 if option 1 was prescribing such technical backdoor options to be implemented
Crux of it: governments can say 'here's the outcome we want you figure out how to get there', but if way to get there is going to be problematic, then this is no different from legislating the problematic thing it in the first place

Comments on appraisal options 4: Anonymous Encrypted Messaging Service

Cannot have option 2 (non-technical means) without option 1 (technical means) as they work together. Sees no difference between the two. Eg: a law prescribing equipment interference is a non-technical and technical option at same time as it still mandates a technical action to be taken.
Strong opposition to option 2 - restricting from a non technical means. Abusive law enforcement could misuse their decryption capabilities. Views law enforcement as an actor we need to protect against rather than empower with ability to weaken encryption.
This option is not in the LGBTQ communities best interest. If the argument for this option is to only weaken encryption for criminals, this would not help LGBTQ community where in some countries being apart of LGBTQ is a crime. The means of weakening of encryption would be used on them on a 'lawful' basis! Option 2 as a precursor to option 1.
Option 3 is preferred. There is no way to weaken encryption in a safe way to protect rights.

Comments on appraisal options 5: LGBT Tech

> Technical solutions to encryption may transcend factors being deliberated in the EU, beyond things like sustainability, feasibility, security and privacy. Likewise, non-technical solutions can result in implications that governments may be unaware of. A more necessary approach is to create safeguards and legal frameworks for using encryption. In moving the current conversation forward and despite this being difficult, it is important to emphasise the black and white nature of encryption to politicians, security and police forces and that undermining encryption leads to several consequences, not least is increasing the surface area for malicious action by both criminal and government actors.

Comments on appraisal options 6: Anonymous Policymaker