TERRORIST USE OF E2EE: STATE OF PLAY, MISCONCEPTIONS, AND MITIGATION STRATEGIES

REPORT

tech against terrorism

tech against terrorism

PART 1

USE AND PERCEPTION OF E2EE: LANDSCAPE REVIEW

1. BACKGROUND AND SCOPE

This report aims to provide a comprehensive overview of the risks and mitigation strategies related to the use of end-to-end encryption (E2EE) technology – with a focus on the use of end-to-end encrypted communications and the risks of abuse by terrorists and violent extremists. This report is divided in four sections:

1. A landscape review of E2EE and associated risks: providing an overview of the current use of end-to-end encryption and an assessment of criminal use of online services offering E2EE.

- o *Part 1: Use and Perception of E2EE – Landscape Review*
- o *Part 2: Criminal Use of E2EE – Terrorists and Violent Extremists Focused Assessment*

2. Recommendations for risk mitigation: assessing the different risk mitigation and content moderation strategies that have been proposed with regard to E2EE, and outlining recommendations for governments and tech companies.

- o *Part 3: Criminal Use of E2EE – Strategies for risks mitigation*
- o *Part 4: E2EE, Criminal use and Risks Mitigation – Tech Against Terrorism's recommendations*

The report was commissioned by Facebook. All findings represent Tech Against Terrorism's independent analysis and research.

2. METHODOLOGY

For this report, Tech Against Terrorism consulted over 160 publicly available reports, articles, white papers, and pieces of legislation concerning the use of encryption, and of end-to-end encryption in particular, as well as the associated risks of criminal actors exploiting such technology. In addition, we consulted five encryption experts from the civil society and tech sectors

Open-source analysis was used to map out the use of E2EE by internet users, as well as the perception of encryption technologies amongst policymakers and the public. To ensure a broad overview and in-depth comprehension of E2EE, including its benefits and potential misuses by malevolent actors (especially terrorists and violent extremists), we supplemented this analysis with a series of interviews with E2EE experts. These interviews were focused on how they viewed policymakers' calls for so-called "safe" backdoors to encryption, and how they considered tech companies could support law enforcement investigations without compromising the online privacy and security provided by E2EE. Furthermore, a review of the prominent literature addressing the specificities both of encryption technology and of terrorist uses of the internet allowed us to build a detailed overview of the technical specificities of E2EE and of the content moderation challenges related to E2EE-protected content. Finally, open-source intelligence (OSINT) analysis was used to inform our understanding of the use of encrypted platforms by terrorists and violent extremists, including their preferred platforms and the reasons for those preferences.

3. USE AND PERCEPTION OF E2EE: KEY FINDINGS

Increased use of encryption and concerns for online privacy:

1. There are growing user concerns over online privacy and tech company misuse of personal data: 64% of users say they are worried about this.[1]

2. These concerns have motivated online services to turn to encryption, including E2EE, in particular for their communications offering. As of 2019, over 40% of private companies across all business sectors were using encrypted solutions.[2,3]

3. In certain countries and regions, including the US, UK, Russia, Germany, and Canada, almost 100% of internet traffic passing through Google is encrypted on the server-side.[4]

Messaging apps and end-to-end encryption:

4. Messaging apps represent the second most common online activity globally (after social media), with 87% of the world's population using such services.[5] WhatsApp, the world's most frequently used messaging app, delivers over a 100 billion end-to-end encrypted messages every day,[6] in an indication of the global popularity of E2EE messaging apps.

5. Four of the six most-used messaging apps globally offer E2EE as a default or opt-in. Most of them rely on asymmetric encryption.[7] Signal's protocol, based on Double Ratchet Algorithm and Diffie-Hellman public values, is open-source and the basis for encryption protocols used by many leading E2EE messaging apps, including WhatsApp, Line Messenger, Viber, and Wire.

Government and law enforcement calls for "backdoors" to encryption

6. With E2EE becoming more prominently used as a result of user demand, policymakers and law enforcement have raised concerns regarding how E2EE could be exploited by criminal actors, including terrorists and violent extremists. However, privacy advocates stress that there is no substantial evidence that the lack of access to encrypted communications significantly hinder the work of law enforcement, nor that the monitoring of criminal actors cannot be done without breaking encryption.

7. E2EE technical experts and digital rights advocates agree that there are no safe backdoors to encryption. Instead they argue that compelling tech platforms to create backdoors or remove E2EE protection would create more security risks, and for a greater number of persons, than it would resolve.

8. The majority of the literature consulted stresses that E2EE is the most secure form of encryption, and the security backbone of today's digital world.

[1] Gorman Doug (2020), The new privacy landscape, Global Web Index.
[2] This includes online communications services, financial services, and health-related services that rely on strong encryption to ensure the integrity of their data and to prevent security breaches.
[3] Statista, Enterprise-wide encryption solution usage worldwide 2012-2019.
[4] Google, HTTPS Encryption on the Web.
[5] Global Web Index (2020), Messaging Apps: Understanding the potential of messaging apps for marketers.
[6] Singh Manish(2020), WhatsApp is now delivering roughly 100 billion messages a day, TechCrunch
[7] A user sends a message encrypted with a public key, which is then decrypted by the recipient, using their matching private key. In this type, AES256 keys are the most commonly used, often alongside Double Ratchet Algorithm protocols for key management.

4. PUBLIC PERCEPTION OF E2EE: USER CONCERNS FOR PRIVACY AND SECURITY

The question of whether online users view positively the mainstream roll out of E2EE across online services is difficult to assess given the lack of global surveys on the subject. Until now, and with the exception of high-level public confrontation between tech platforms and the authorities over providing law enforcement with access to encrypted devices and communications,[8] the question of whether encryption should be viewed as a risk to security has remained mostly a discussion between policymakers, law enforcement, tech companies, and E2EE experts. However, the growing popularity of encrypted messaging apps (EMS), as well as the proportionate rise in users' concerns about online privacy and how their data can be (mis)used by private companies and governments, can inform us about public perceptions of E2EE and EMS.

4.a Weakened trust in tech companies

Both the Snowden revelations and the Cambridge Analytica scandal in 2018[9] heavily impacted users trust in internet technologies and online platforms.

The use of E2EE for online communications has been driven by the Snowden revelations in 2013,[10] on the US surveillance programs on its own citizens via the National Security Agency (NSA). The documents leaked by Snowden revealed the existence of PRISM, a program that allowed the NSA to compel tech platforms to respond to user data requests. The document also revealed that most telephone companies in the US had been providing users' phone records to the NSA.[11] These revelations "triggered a global wave of privacy concerns by revealing the extent of government mass surveillance programs",[12] and drove E2EE to become the norm for messaging apps. The same year, WhatsApp began to roll out encryption before partnering with the Open Whisper System – the group behind Signal, one of the first messaging app that fully integrated E2EE – to begin rolling out E2EE on its services in 2014. WhatsApp became fully encrypted with E2EE protocols in 2016.[13] Similarly, ProtonMail, the leading E2EE email service provider, launched in 2014 in direct response to the Snowden revelations and out of a desire to provide an easy and secure communication service to users.[14]

A Pew Research Centre study on "Americans' Privacy Strategies Post-Snowden", published in 2015, showed that 30% of individuals aware of the surveillance programs had changed their online habits and "taken at least one step to hide or shield their information from the government."[15] This distrust towards online surveillance further shifted to target tech companies following the Cambridge Analytica scandal, as the proportion of social media users believing that the sites they were using

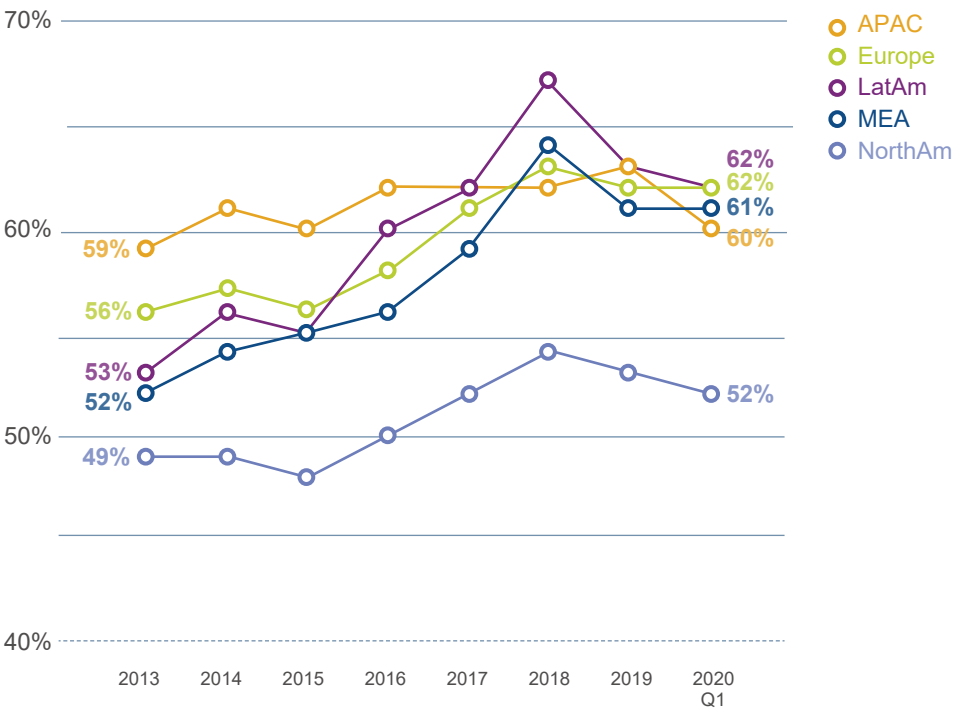
[8] *As was the case in the confrontation between Apple and the FBI around the San Bernardino case in 2015 and Pensacola in 2019, see: Part 2, Section on Suspected Use of E2EE in Terrorist Attacks and Its Impact on The Encryption Debate.*
[9] *In March 2018, The Guardian revealed that Cambridge Analytica, a political consulting firm based in the UK, had "harvested millions of Facebook profiles of US voters, in one of the tech giant's biggest ever data breaches", using the information collected to build a software program to predict and influence voters' political choices in the 2016 US elections.*
See: Cadwalladr Carole and Graham-Harrison Emma (2018), Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian.
[10] *Pelroth (2019).*
[11] *Franceschi-Bicchierai Lorenzo (2014), The 10 biggest revelations from Edward Snowden's Leaks, Mashable.*
[12] *Lomas (2016).*
[13] *Lomas (2016)*
[14] *Koch Richie (2020), Massive corporate databases become government tools of surveillance, ProtonMail Blog; ProtonMail About, We're building an internet that protects privacy, starting with email.*
[15] *Rainie Lee and Madden Mary (2015), Americans' Privacy Strategies Post-Snowden, Pew Research Centre.*
[16] *Mahlmann Ariel (2019), End-to-End Encryption Strategies Becoming the Norm for Social Media, Fornetix.*

were “trustworthy” fell to 9%.[16]

Other studies have shown that users’ concerns about their privacy online, and the potential misuse of data, are also common amongst the users of messaging apps. A 2016 Global Web Index (GWI) study focusing on WhatsApp, Line, and Facebook Messenger users showed that 58% of them were concerned about online privacy. The GWI thus underlined that companies’ introduction of E2EE was “very much in line with privacy concerns among their audiences.” The same study showed that over 60% of users are concerned about ISPs misusing their data.[17] A more recent study by the GWI highlights how online users’ concerns for privacy have continued to grow in recent years, showing that “64% of internet users say they’re concerned [about] how their private information online is being used by companies.” A concern shared worldwide with Europeans being least concerned, with 52% of users expressing privacy concerns in comparison to 60% or over in other regions of the world.[18]

PRIVACY CONCERNS HAVE INCREASED WORLDWIDE

% of internet in each region who say they are concerned about the internet eroding their personal privacy

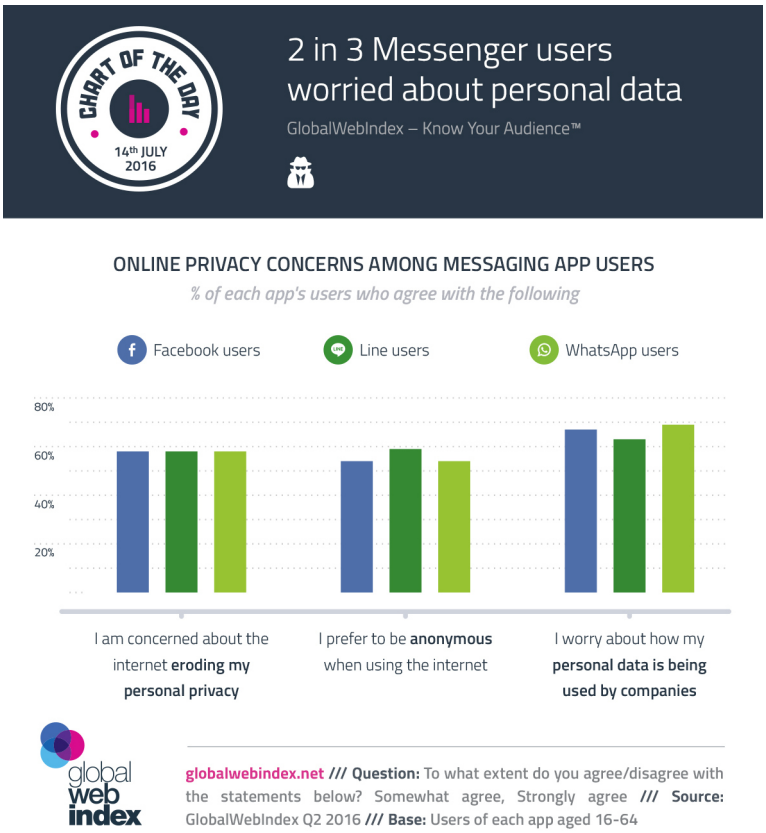


Question: Which of the following statements do you agree with? I am concerned about the internet eroding my personal privacy

Source: Global Web Index: The new privacy landscape.

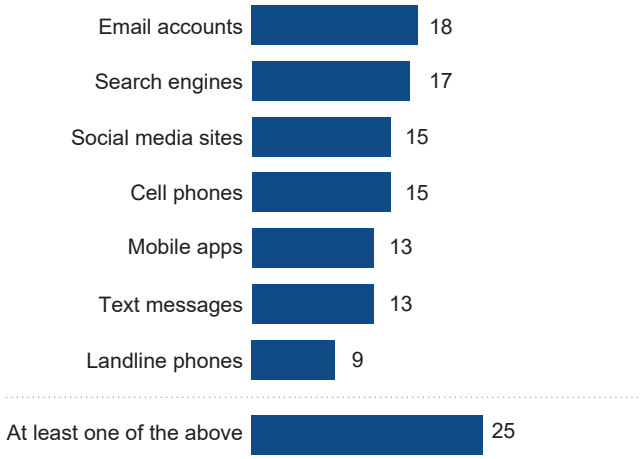
Base: All internet users

[17] *Buckle Chase (2016), 2 in 3 Messenger users worried about personal data, Global Web Index.*
[18] *Gorman Doug (2020), The new privacy landscape, Global Web Index.*



SURVEILLANCE PROGRAMS PROMPT SOME TO CHANGE THE WAY THEY USE TECHNOLOGY

Among the 87% of U.S. adults who have heard of the government surveillance programs, the percentage who have changed their use of... "a great deal" or "somewhat"



Source: Survey of 475 adults on GfK panel November 26, 2014 - January 3, 2015
PEW RESEARCH CENTER

Responding to users concerns: For platforms and apps whose main services are centred around encryption, the focus on user privacy and security has become an integral element of their offering and branding. These platforms brand themselves on the promise of entirely private communication, safe from government surveillance programmes and abuse by malevolent actors. With E2EE users can rest assured that no one has access to their private conversations and that their fundamental right to privacy online is safeguarded.

Source: Left, Global Web Index, 2 in 3 Messenger users worried about personal data;

Bottom, Pew Research Center, Americans' Privacy Strategies Post-Snowden.

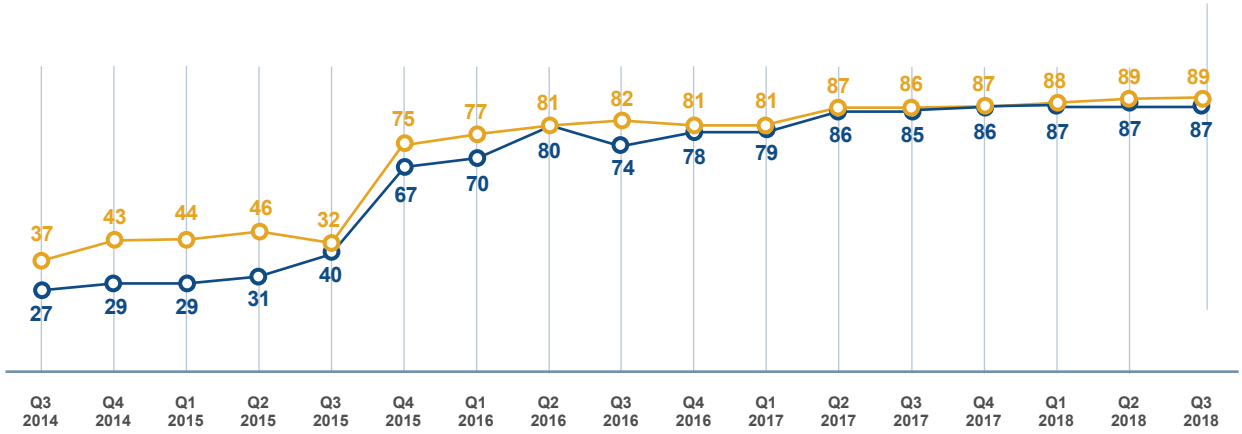
4.b Communications, user privacy and the rise of E2EE

The use of E2EE is particularly prevalent among online platforms and mobile applications used for communication purposes, such as messaging apps and email services.[19] The increased use of video-conferencing services during the Covid-19 crisis has also led the providers of such services to introduce end-to-end encryption to both reassure their user base that their communications are safe, and to respond to public concern that such services are insufficiently secure.[20] Some file-hosting services also offer E2EE.

Instant messaging apps: Whether they offer E2EE or not, messaging apps represent a substantial market share of today's social media landscape, with 87% of the world population using online messaging services at least once a month – a growth of 60% since 2014. This makes instant messaging "the second most common online activity after social media usage", as users are shifting their online conversations from social media to more private channels of communication.[21]

THE ONLINE MESSAGING LANDSCAPE

The growth of private messaging channels

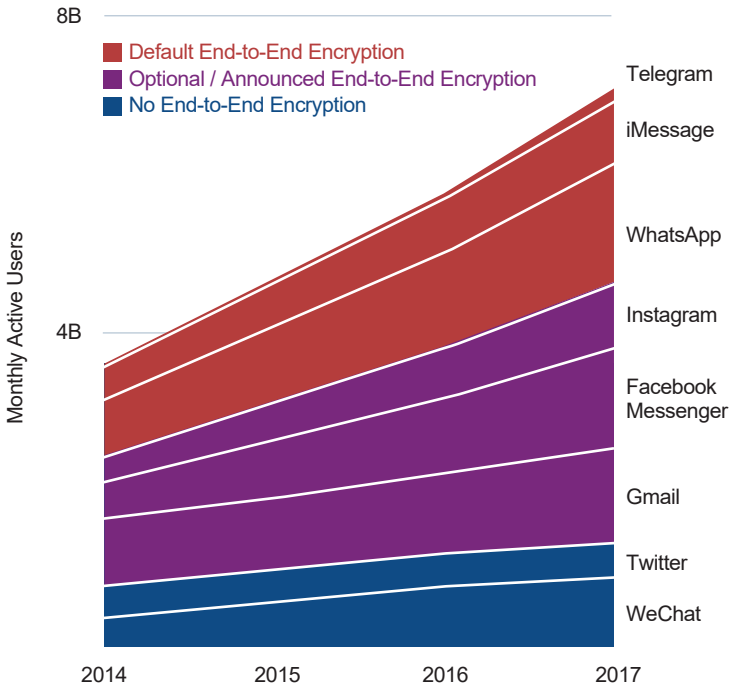


Source: Global Web Index, Messaging Apps: Understanding the potential of messaging apps for marketers.

[19] *Google announced in 2014 that it would roll out E2EE for Gmail, framing the move as part of its commitment to users' security. See: Google Security Blog (2014), Making end-to-end encryption easier to use.*
[20] *In 2020, video-conference platform Zoom responded to privacy concerns by announcing a four-phase plan for E2EE. Since this announcement, Zoom has introduced E2EE beta features. Jitsy Meet also introduced E2EE for its video-call and conferencing services. See: Jitsy (2020), This is what end-to-end encryption should look like!; Khron Max (2020), Zoom Rolling Out End-to-End Encryption Offering, Zoom Blog.*
[21] *Global Web Index (2020)*

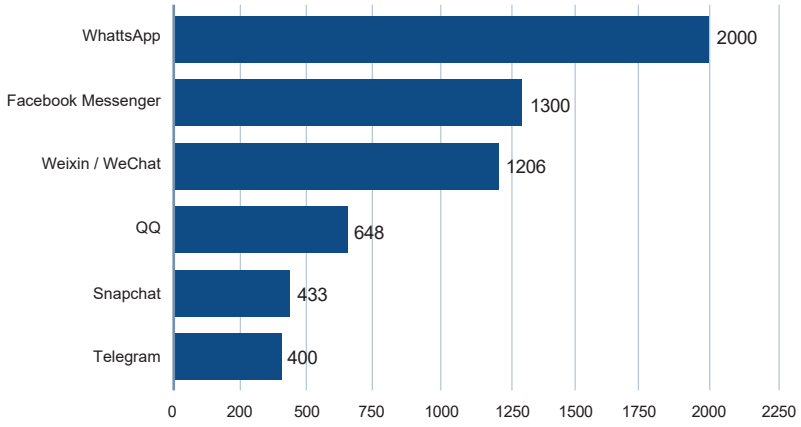
Encrypted messaging services (EMS): Amongst the most popular messaging apps in 2020, two thirds offer E2EE, either as a default or as an opt-in. The world's leading messaging app, WhatsApp, has been fully deploying E2EE since 2016.[22] For users concerned with safeguarding their online privacy and the risks of data misuse, E2EE offers an assurance that their conversations will remain private and that limited data can be harvested from their online communications. In comparison with other online services, those offering E2EE can guarantee their users that no one but the sender and recipient can access encrypted content, including files and messages.

SELECT MESSENGER MAUs



Source: BondCap Internet Trends 2019

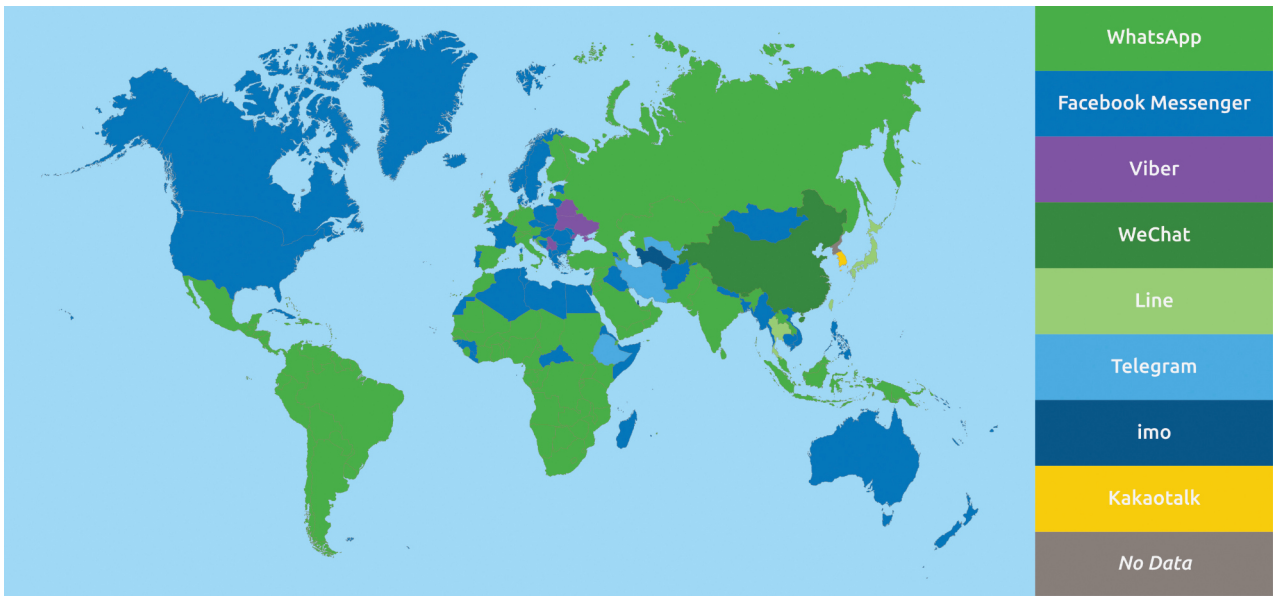
MOST POPULAR MOBILE MESSENGER APPS AS OF OCTOBER 2020, BASED ON NUMBER OF MONTHLY ACTIVE USERS (IN MILLIONS)



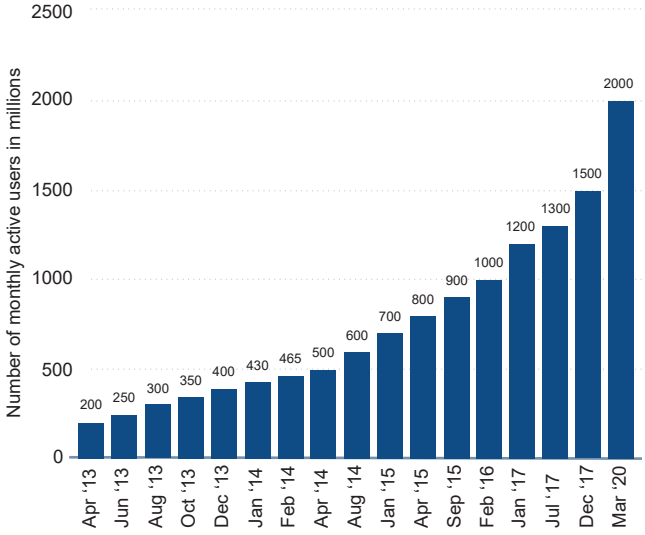
Source: Statista, Most popular global mobile messenger apps as of October 2020, based on number of monthly active users.

[22] Lomas Natasha (2016), "WhatsApp completes end-to-end encryption rollout", TechCrunch

TOP MESSAGING APPS BY COUNTRY



NUMBER OF MONTHLY WHATSAPP USERS



Source: Top, Bucher Birgit (2020), WhatsApp, WeChat and Facebook Messenger Apps – Global usage of Messaging Apps, Penetration and Statistics, MessengerPeople.

Bottom, Clement J. (2020), Number of monthly active WhatsApp users as of 2013-2020, Statista.

WhatsApp and public appreciation of E2EE

WhatsApp, the world's leading messaging app[23] with over 2 billion users,[24] demonstrates the popularity of EMS and the quantity of end-to-end encrypted communications shared across the world on a daily basis.[25] While we lack detailed statistics about the volume of E2EE web traffic in the world, the success of WhatsApp provides a clue. The app has grown constantly following the roll out of E2EE in 2014, going from 465 million monthly active users in February 2014 to 1 billion in 2016. In April 2020, WhatsApp was reported to have 2,000 million monthly active users; in October 2020, Marc Zuckerberg announced that the app was delivering around a 100 billion messages a day, all of which are encrypted.[26]

[23] When compared to social media platforms in general, WhatsApp ranks third as of October 2020. See: MessengerPeople, WhatsApp, WeChat and Facebook Messenger Apps – Global useage of Messaging Apps, Penetration and Statistics,
[24] Porter Jon (2020) WhatsApp now has 2 billion users, The Verge
[25] Bucher (2020)
[26] Singh (2020)

4.c The use of encryption by governments and public servants

Even though policymakers have been calling for access to E2EE platforms, several political figures as well as governmental and intergovernmental institutions have been known to use E2EE messaging services.

In the US, Jared Kushner, Senior Advisor to former President Donald Trump, used WhatsApp to conduct government business and discussions with foreign leaders, including Saudi Crown Prince Mohammed Bin Salman.[27] Close aids to US policymakers including to Presidents Donald Trump and Barack Obama, former Secretary of State Hillary Clinton, and Andrew Cuomo and Bill de Blasio, respectively Governor of New York and Mayor of New York City, are also known to have been using WhatsApp. The move to encrypted messaging in the US political landscape is likely to have been spurred by the Clinton emails leak, as underlined by one former Senior Aide to President Obama: "Everybody learned the lessons of the Clinton campaign when it came to communicating about sensitive issues over email".[28]

The UK Prime Minister, Boris Johnson, is also known to have used WhatsApp for communicating with high-level foreign officials, including the Saudi Crown Prince[29] and President Emmanuel Macron.[30] Besides the Prime Minister, British diplomats and Members of Parliament are also said to use WhatsApp to discuss sensitive policy topics.[31]

Australian Government

Australian politicians and members of the government are also known to have been using WhatsApp – for instance, Angus Taylor, Minister for Energy and Emissions Reduction, and Liberal Party Members of Parliament.[32]

"WhatsApp diplomacy": WhatsApp is not only used by world leaders, but by diplomats and public servants to communicate with colleagues and allies, as well as to organise meetings. The term for this phenomenon was coined by The Guardian, which suggested that diplomats could use the app to organise each other in groups sharing common interests and to communicate during meetings without having to leave the room.[33] Even when security concerns have been raised regarding politicians' and diplomats' use of WhatsApp, this has usually led to a change of encrypted messaging service rather than abandoning publicly available EMS – as demonstrated by the EU Commission and the UK Conservative parties switching to Signal.

[27] *Collier Kevin (2019), Jared Kushner's use of WhatsApp raises concerns among cybersecurity experts, CNN.*
[28] *Gay Mara (2017), Messaging App Has Bipartisan Support Amid Hacking Concerns, The Wall Street Journal; Mihindukulasuriya Regina (2019), Prying government eyes drive politicians, terrorists to WhatsApp, Telegram, Signal, The Print.*
[29] *Riley-Smith Ben and Hope Christopher (2020), Boris Johnson communicated with Saudi crown prince on WhatsApp, ex-UK officials say, The Telegraph;*
[30] *Gange David (2020), Boris Johnson and Emmanuel Macron's WhatsApp messages on quarantine-free travel blindsided officials, UK News Today.*
[31] *Wintour Patrick (2016), Internal report slams culture in UK Foreign Office, The Guardian.*
Kenber Billy and Parker Charlie (2020), Matt Hancock's neighbour won £30m deal to supply vials for Covid tests, The Times.
[31] *Davies Anne (2020), Angus Taylor v Clover Moore: WhatsApp messages reveal panic as minister's staff realised figures were wrong, The Guardian; Hutchens Gareth (2018), Leaked WhatsApp messages reveal Julie Bishop's leadership bid scuppered by colleagues, The Guardian.*
[33] *Borger Julian, Rankin Jennifer, Lyons Kate (2017), The rise and rise of international diplomacy by WhatsApp, The Guardian.*

The EU announced in early 2020 that it would recommend its staff to use Signal, in particular for "external communication between Commission staff and people outside the organization."[34] This change was prompted by the need to increase the security of the Commission's communications, given the series of high-profile hacks of EU diplomatic channels revealed in previous years.[35]

In France, the Inter-Ministerial Digital Directorate (Direction Interministérielle du Numérique, DINUM) has used Element's Riot Matrix Solution to develop its own encrypted communication tool, Tchap, for French civil servants.[36] However, French politicians are known to prefer publicly available EMS, including Telegram, used by President Macron and his aides, and WhatsApp in the case of former Prime Minister Edouard Philippe and his team. Other French politicians have been using Signal.[37]

In the UK, the Conservative Party switched from WhatsApp to Signal in 2019. Whilst some commentators have said that this was for reasons of security following WhatsApp leaks, a Conservative spokesperson has said that the move was to accommodate the number of members using the app, pointing out that WhatsApp only permits 256 members in a group chat.[38]

5. LANDSCAPE REVIEW: USE OF E2EE ACROSS THE INTERNET

In recent years, encryption has become a default option offered by most online communications services and functions as a token of security displayed by tech companies to reassure users about the safety of their data. This development has been driven by concerns for users' privacy and security, and data protection at large, especially in countries where data protection is regulated and in sectors where the protection of users' data and personally identifiable information (PII) is a core component of the services offered (for example, in online banking and finance or identity verification services). To provide a general overview of the use of encryption by ISPs, we have summarised below whether a given category of online services relies chiefly on E2EE or on server-side encryption.

[34] *Dussutour Chloe (2020a), European Commission to use open source messaging service Signal, JoinUp*
[35] *See: Cerulus Laurens (2020), EU Commission to staff: Switch to Signal messaging app, Politico; and Porter Jon (2020), Signal Becomes European Commission's messaging app of choice in security clampdown, The Verge.*
[36] *Dussutour Chloe (2020b), French government launches in-house developed messaging service, Tchap, JoinUp.*
More on Tchap: http://www.tchap.fr/
[37] *Hacot Valerie (2019), Messageries : plutôt WhatsApp à Matignon et Telegram à l'Elysée, Le Parisien.*
[38] *Waterson Jim (2019), Tories switch to messaging app Signal after WhatsApp leaks, The Guardian*

End-to-End Encryption (Client-side encryption, Zero Access/ Knowledge)

Messaging apps: Most leading messaging apps offer E2EE by default or as an opt-in – see below.

Emails: E2EE is also commonly offered by email providers. Outlook, for instance, offers E2EE features, and other platforms, such as ProtonMail and TutaNota, have been built on the promise of entirely private and secure emails.

File hosting: Certain file-hosting services also offer E2EE to their users, including Mega.Nz, Nextcloud, Sinc.com, and Pcloud.

Video conference: Following an exponential rise in the use of video conference platforms, users have increasingly been concerned with how private their calls are. This led certain platforms in the pursuit of a E2EE roll-out, including Zoom and Jitsy Meet which both started testing E2EE and now fully offer E2EE as an opt-in (as of August 2021).

Server-side encryption (TLS, AES, SSL)

WWW: Most online platforms and websites have server-side encryption by default, whether that be for data in transit or at rest. The “HTTPS” mark used by most websites has thus become a mark of a trustworthy website that most ISPs decide to opt for.

Emails: Most email services are using transport layer security (TLS) protocols to secure users’ communications.

Content sharing platforms: Most social media platforms, including blogger platforms, offer HTTPS by default or add-ons that users can opt for when setting up their accounts.

Banking, financial and health services: Business handling sensitive and personal information, such as health records and banking details, have turned to advanced encryption protocols to ensure the security of their users’ data.

5.a Overview of leading messaging apps offering E2EE

Please note that the below table only provides an overview of leading messaging apps offering E2EE as a default or opt-in, more detailed comparisons covering security features, content moderation, and cooperation with law enforcement can be found in relevant sections of the report.

	Apps' slogans reflecting the emphasis on security	Encryption protocol	Monthly active users	Fully E2E encrypted	"Secret chat" E2EE option
WhatsApp	"Simple. Secure. Reliable Messaging."	The Signal Protocol, designed by Open Whisper Systems, is the basis for WhatsApp's end-to-end encryption.[39] Encryption is based on the sender generating an AES256 Key, and on the HMAC-SHHA256 key (both are ephemeral).[40]	2 billion monthly active users (April 2020)		
Signal	"Speak Freely."	Powered by the open-source Signal Protocol.[41] This is mainly based on the Double Ratchet Algorithm and Diffie-Hellman public values.[42] The Signal Protocol, being open source, is used by a number of other platforms, including WhatsApp and Wire.[43]	1-5 million downloads (no specific metrics available);[44] User base estimated to be at least 2 million in 2016.[45]		
Line Messenger	N.A.	Letter Sealing protocol, using AES256 key for message encryption and SHA-256 for message hashing.[46]	84 million monthly active users (2020).[47]		
Viber	"Free and secure calls and messages to anyone, anywhere."	Viber's protocol uses the same concepts of the "double ratchet" protocol used in Open Whisper Systems Signal application. However, Viber's implementation was developed from scratch and does not share Signal's source code.[48] 1-1 chats have E2EE turned on by default, users can choose to turn it off. E2EE is limited to 1-1 chats and group chats under 50 participants	1,169 millions unique users IDs (March 2020).[49]		
Wire	"The most secure collaboration platform."	Proteus is Wire's main cryptographic protocol. It is an independent implementation of the Axolotl/Double Ratchet protocol, which is in turn derived from the Off-the-Record protocol, using a different ratchet[50]	Over 1,000,00 installs on Google Play.[51]		

[39] *WhatsApp (2020), Encryption Overview Technical White Paper.*
[40] *See Glossary for definition*
[41] *Signal Homepage;*
[42] *Signal, Technical information.*
[43] *Cohn-Gordon K., Cremer C., Dowling B., Garratt L., Stebila D., (2019), A Formal Security Analysis of the Signal Messaging Protocol.*
[44] *Lee Micah (2016), Battle Of The Secure Messaging Apps: How Signal Beats WhatsApp, The Intercept.*
[45] *Greenberg Andy (2020), Signal is Finally Bringing Its Secure Messaging to the Masses, Wired.*
[46] *LINE (2016), Encryption Overview Technical White Paper*
[47] *Statista (2020), LINE – Statistics & facts.*
[48] *Viber Encryption Overview*
[49] *Clement J. (2020a), Viber: number of registered user IDs 2011-2020, Statista.*
[50] *Wire Security White Paper*
[51] *https://play.google.com/store/apps/details?id=com.wire&hl=en_GB&gl=US*

	Apps' slogans reflecting the emphasis on security	Encryption protocol	Monthly active users	Fully E2E encrypted	"Secret chat" E2EE option
Wickr me	"Privacy made easy with Wickr"	Wickr Secure Messaging Protocol: "Each Wickr device node creates and refreshes a pool of asymmetric key pairs to be used for Diffie-Hellman key exchange when receiving messages, referred to as KEn and PKEn. The public components of these key pairs are signed by the originating device's Node Identity Private Key. This signature, SKn(PKEn), is uploaded to Wickr servers along with PKEn and a unique identifier for the key, IDken."[52]	Over 5,000,000 installs on Google Play[53]		
Threema	"The messenger that puts security and privacy first."	Threema communicates with three different types of servers. To access the directory and to download/ upload encrypted media files, HTTPS is used. To transport the actual chat messages, a custom protocol built on TCP is used.[54]	Over 8 million users (including 2 millions for Threema Work)[55]		
Element (formerly Riot.im)	"Own your conversations"	Matrix Protocol.[56]	Over 100,00 installs on Google Play[57]		
IMessage:	"Privacy is built from the beginning"	For encryption, there is an encryption RSA 1280-bit key as well as an encryption EC 256-bit key on the NIST P-256 curve. For signatures, ECDSA 256-bit signing keys are used. The private keys are saved in the device's Keychain and only available after first unlock. The public keys are sent to Apple Identity Service (IDS) where they are associated with the user's phone number or email address, along with the device's APNs address.[58]	Estimate of 1.3B active users (2019)[59]		
Rocket.chat	"Rocket.chat is the best messaging solution to protect your data."	On login the client auto-generates the encryption password and asks the user to save it. This password is used to generate a secure 256-bit AES-CBC encryption key, called "Master Key". More information on Rocket.chat E2E included here.[60]	Over 100,000 installs on Google Play[61]		
Telegram	"Telegram messages are heavily encrypted and can self-destruct."	Relies on the MTProto Mobile Protocol for server-client encryption, and offers E2EE for secret-chats.[62]	400 million monthly active users (October 2020)[63]		

[52] *Wickr (2017), Wickr Messaging Protocol Technical Paper.*
[53] *https://play.google.com/store/apps/details?id=com.mywickr.wickr2&hl=en_GB&gl=US*
[54] *Threema. Cryptography Whitepaper*
[55] *Threema (2020), Cryptography Whitepaper.*
[56] *Element Homepage*
[57] *https://play.google.com/store/apps/details?id=im.vector.app&hl=en_GB&gl=US*
[58] *Apple Platform Security: iMessage overview*
[59] *99Firms (2019), Most Popular Messaging Apps.*
[60] *Rocket.Chat Security*
[61] *Googe Play: Rocketchat*
[62] *Georgina Petcu Alina (2020), Is Telegram Secure? What You Need to Know Before Downloading the App, Heimdal Security.*
[63] *Iqbal Mansoor (2020), WhatsApp Revenue and Usage Statistics (2020), Business of App.*

	Apps' slogans reflecting the emphasis on security	Encryption protocol	Monthly active users	Fully E2E encrypted	"Secret chat" E2EE option
Conversations	N.A	XMPP federated protocol for the user to choose which servers to connect to when using the app. All communications are TLS encrypted.[64] For enabling E2EE, users can choose OMEMO,[65] a multi-end-to-multi-end encryption method based on Double Ratchet, or OpenPGP.[66]	Over 100,000 installs on Google Play.[67]		
Kakaotalk	N.A	Secret chat mode.[68]	45 million active users in South Korea (2020)[69]		
Snapchat	N.A	SnapChat allows messages to be encrypted in transit; however, according to the tech-based site, Recode, Snapchat messages are encrypted while at rest on Snapchat's servers (though the company has the encryption key if needed). Snaps are deleted from the servers as soon as they're opened by the intended recipients, and Snapchat claims these delivered messages "typically cannot be retrieved from Snapchat's servers by anyone, for any reason."[70]	249 million daily active users (2020)[71]		
Session	"Send Messages Not Metadata."	Session is an open source, public key-based secure messaging application which uses a set of de-centralised storage servers and an onion routing protocol to send end-to-end encrypted messages with minimal exposure of user metadata.[72]	Over 100,000 installs on Google Play (December 2020)[73]		
Fortknoxster	"Military grade encryption"	When a user registers on FortKnoxster.com - four sets of RSA key-pairs are generated, two sets of elliptic curve (EC) key-pairs and 6 Key Protector(s) (one per private key) in the client's browser. These encryption and identity key-pairs are used for different services and protocols. Unlike other known encryption protocols, each of FortKnoxster's services or protocols needs two sets of key-pairs, one for encryption and decryption and one for signing and verification. The key protector is used to encrypt/wrap each private key which is only known to the user. The user's personal password is used to compute derived keys in the client, the account password, and root keys.[74]	Over 100,000 installs on Google Play (December 2020)[75]		
Hoop Messenger	"Hoop connects you to the world with unparalleled freedom & privacy"	Hoop Messenger allows the user to encrypt files within the Vault (patent pending). All content in the Vault is secured using long AES256 keys mapped with PBKDF2, therefore no one can access the content in the Vault without the correct password.[76]	Over 500,000 installs on Google Play (December 2020)[77]		 Via the "Vault"

[64] Conversations' homepage.
[65] Conversations, OMEMO Multi-End Message and Object Encryption.
[66] Conversations' homepage.
[67] Conversations page on Google Play
[68] South Korea's Kakao Talk Adds 'Secret Mode', Wall Street Journal
[69] Waldeck Yasmin (2020), Number of monthly active users of KakaoTalk in South Korea 2015-2020, Statista
[70] 5 Popular Messaging Apps and the Ecnryption Behind them, Lumen
[71] Clement J. (2020a), Daily active users of Snapchat 2014-2020, Statista.
[72] https://getsession.org/wp-content/uploads/2020/02/Session-Whitepaper.pdf
[73] https://play.google.com/store/apps/details?id=network.loki.messenger&hl=en&gl=US
[74] https://fortknoxster.com/FortKnoxster_Whitepaper_English.pdf
[75] https://play.google.com/store/apps/details?id=com.fortknoxster&hl=en&gl=US
[76] https://hoopmessenger.com
[77] https://play.google.com/store/apps/details?id=com.magnificus.hoop&hl=en&gl=US

5.b Privacy by design at the core

For some messaging and email providers, privacy via E2EE has become an intrinsic component of their services, with E2EE presented as the main reason why a user should opt for one app rather than another – providers often compare their services to those of major companies that either do not offer E2EE or offer fewer privacy features. Signal's homepage demonstrates this by featuring quotes from Edward Snowden and Jack Dorsey, Twitter's CEO, stating their use of Signal and their trust in the security of the app.

"I Use Signal every day".
Edward Snowden
Whistleblower and privacy advocate

"I trust Signal becuase it's well built, but more importantly, becuase of how it's built: open source, peer reviewed, and funded entirely by grants and donations. A refreshing model for how critical srvices should be built".
Jack Dorsey
CEO of Twitter and Square

Source: Signal's homepage.

Privacy branding

Platforms that have placed privacy at the heart of their product offering, such as Signal and Element, as seen above, have increasingly focused their branding on user privacy and security, and to this end they showcase the different privacy and security features they have implemented. This type of privacy branding includes encryption but also the ability to delete messages or create accounts without the need to provide a phone number or an email address – for a more complete overview of privacy and security features offered, see the table below.

Protonmail, for instance, brands itself with "Swiss Privacy – Data Security and Neutrality", E2EE, and "Anonymous Email" and does not require personal information to create an account. Threema, also a Switzerland-based messaging app and one of the few with a download fee, uses the following slogan as a key marketing argument: Your private life is valuable. Don't Pay with Your Data.[78] However, this branding can risk attracting terrorists and violent extremists to an app, especially when an app explicitly states that it will not share users' data with government as with the case of Telegram – See Telegram case study in: Part 2, Section 11.c Terrorist and violent extremist use of E2EE: Telegram case study.

Encryption white papers: The use of white papers detailing security and encryption processes has become a common practice amongst tech companies deploying advanced encryption protocols, including E2EE, on their services. WhatsApp, Line Messenger, Signal, Wire, ProtonMail, Zoom and Google have all published white papers or other programmatic documents outlining their encryption protocols as a means of informing their users of the steps taken to protect their data and communications. A list of relevant whitepapers can be found in the bibliography.

[78] *In Germany, Threema is the 7th most popular messaging app, with 6.0 million daily active users as of November 2019. See: Bucher (2020),*

5.c E2EE apps - overview of privacy and security features offering

Note: *Empty cells mean that no information is available*

	Decentralised server network	Delete sent messages / Disappearing Messages[79]	Password / Lock	"Private" or "hidden" chats[80]	Phone number visibility for non-address book contacts	File-storage[81]	Additional security features
WhatsApp		✓ Delete & disappearing: Users have the ability to delete messages (both senders and recipients) and o send a message which disappears after seven days.[82] Disappearing messages can also be set as the default for chats. Since August 2021 WhatsApp also allows users to send photos and videos that disappear once opened.[83]	✓		✓		
Signal		✓ Users are able to delete messages sent or received within the past 3 hours , and to send a message which disappears after a set period has elapsed (anywhere from 5 seconds to 1 week).	✓		✓		

[79] *Also known as: self-destruct or timed messages.*
[80] *This category is used to designate the possibility to pin-protect certain chats within the app, or to hide them from the general chats list.*
[81] *Certain EMS offer users the possibility to store files directly within the app, for instance via the app's cloud-storage in the case of Telegram.*
[82] *In April 2021, WhatsApp began to test the possibility for users to send 24h disappearing messages: Business Standard (2021), WhatsApp tests 24-hour time limit for its disappearing messages feature.*
[83] *WhatsApp (2021), View Once Photos and Videos on WhatsApp.*

	Decentralised server network	Delete sent messages / Disappearing Messages	Password / Lock	"Private" or "hidden" chats	Phone number visibility for non-address book contacts	File-storage	Additional security features
Line Messenger		✓ Delete & disappearing: Users are able to to delete messages sent or received within 24 hours , and to send a disappearing message using 'Hidden Chats' where messages are only displayed for a pre-set amount of time (2, 5, or 10 seconds; 1 minute; 1 hour; 1 day; 1 week) after the recipient has clicked on it		✓ "Hidden chats":[84] Separate chat rooms, when a message is received it appears as a "hidden" message that the recipient needs to tap to display. "Hidden" messages can only be displayed for a set amount of time before self-destructing.			
Viber	✗	✓ Delete & disappearing: Users are able to delete messages sent or received, and to send a message timed to self-destruct(at 10 or 30 seconds, 1 minute, 1 hour)	✓	✓	✓ Hidden chats": Separatechat rooms from the general chat list with pin protection. Notifications do not display a preview of the message [85]		Proxy connection available
Wire		✓ Delete & disappearing: Users are able to to delete messages sent or received and to send messages timed to self-destruct	✓				

[84] http://official-blog.line.me/en/archives/1006361166.html#:~:text=Open a 1-to-1,Hidden Chat room as usual.
[85] https://help.viber.com/en/article/hidden-chats

	Decentralised server network	Delete sent messages / Disappearing Messages	Password / Lock	"Private" or "hidden" chats	Phone number visibility for non-address book contacts	File-storage	Additional security features
Wickr Me		✓ Delete & disappearing: Users are able to delete messages sent or received(also for recipients), and to send self-destructible messages (either using the 'expiration' option or 'burn-on-read' options)	✓				Screen overlay protection; Functionalities to resist forensic enquiry
Threema		✓ Delete Users are able to delete messages sent or receivedthat are older than the specified amount of time, 1 week to 1 year,	Session passwords to use Threema Web are available on application	✓ "Private chats": Users can pin-protect certain chats, which are hidden from the general chats list and for which notifications do not include a preview of the message.[86]			Threema uses open source NaCl cryptography library for encryption
Element/Riot	✓						A user can see every device that has joined an encrypted conversation. If a new and unexpected device joins, the user can use device verification to check that it is really someone they trust

[86] https://threema.ch/en/faq/private_chats

	Decentralised server network	Delete sent messages / Disappearing Messages	Password / Lock	"Private" or "hidden" chats	Phone number visibility for non-address book contacts	File-storage	Additional security features
Rocket Chat	✓	✓ Delete: Users are able to delete sent messages (not specified whether for sender only or also for receiver)					
Telegram		✓ Delete & disappearing: Users are able to delete messages sent or received, and to enable auto-delete messages (to be set to delete either 24 hours or 7 days after sending)	✓				Usera able to set-up a proxy server ("Anti-Censorship tool")
Session	✓					Secure attachments: Share voice snippets, photos, and files with Session's secure encryption and privacy protections	No metadata logging: "Session doesn't store, track, or log your messaging metadata" IP address protection: "Device IP addresses are never exposed to the person you're talking to or the servers holding your data"
FortKnoxster	✓	✓ Disappearing: Users are able to send self-destruct messages (time-limit is not specified)	✓			Encrypted and decentralised cloud storage	
Hoop Messenger		✓ Disappearing: Users are able to send timed messages (time-limit is not specified)	✓	✓	N/A	✓	Third party audit by CNLABS (Switzerland) VPN Browsing: "Multiple aliases which cannot be traced to master account"
Conversations	Lack of publicly available information						

6. E2EE: CHALLENGES FOR CONTENT MODERATION

In contrast to server-side encryption, E2EE poses significant challenges in both content moderation (COMO) and in obtaining lawful access to content by investigative public bodies. These challenges both result from the intrinsic characteristic of E2EE, but despite their common origin, the two must be distinguished.[87] When they are conflated, the encryption debate loses relevance, and the competing arguments lose their salience.

The principal impediments to moderating user-generated content on E2EE services, and to countering their abuse for criminal purposes, can be summarised as follows:

- Content that cannot be seen or accessed cannot be moderated.
- Content cannot be moderated without compromising either the security of user data or their overall privacy when using the services.
- Content cannot be moderated if it cannot be correctly identified and reported.
- Malevolent users, including terrorist and violent extremist actors, cannot be identified and excluded from the service.

Despite service providers not being able to view content, experts in computer science and encryption argue that "forms of content moderation may be compatible with end-to-end encrypted messaging, without compromising important security principles or undermining policy values." User reporting, for instance, can be fully compatible with E2EE, with little to no technical challenge. Policymakers and technical experts have proposed other solutions for moderating E2EE content with a view to identifying and reporting illegal and harmful content shared via EMS, as in the case of the leaked EU report on identifying child sexual abuse (CSA) content on encrypted platforms – see section 7 on Challenges For Law Enforcement Access.

More on technical solutions to counter criminal user of E2EE services, in Part 3 of this report: Criminal Use of E2EE – Strategies for risks mitigation.

6.a E2EE Messaging Apps – Overview of content moderation capacities

The table below provides an overview of the policies and enforcement capacities for countering illegal and in particular terrorist use of services in the case of the leading messaging apps offering end-to-end encryption. This overview is based on information publicly available on the different apps' websites: the absence of information in the table thus does not denote that an app does not act against malevolent use of its services, but rather that such information is not publicly available. This suggests either a lack of policy regarding illegal and criminal use, or a lack of transparency.

[87] *Ibid.*

	Terms of Service (ToS) prohibiting certain content / behaviours	Explicit prohibition of terrorism	Act against CSA content (publicly mentioned on website)	Pro-active monitoring for illegal content and/or use (publicly mentioned on website)	Possibility to ban accounts
WhatsApp	✓	✓	✓	✓ CSAM material via PhotoDNA (unencrypted information only)[88]	✓ In violation of ToS, user reporting does not necessarily lead to bans
Signal					
Line Messenger	✓		✓		✓
Viber	✓			✓ "This may include URLs included in messages, which were reported as SPAM by other users"	✓
Wire[89]	✓		✓		✓
Wickr Me[90]	✓				✓
Threema[91]	Not for Threema Messenger				
Element/Riot[92]	✓ For Matrix services in general				✓ For Matrix services in general
Rocket chat[93]	✓	✓			✓

[88] *WhatsApp (2021), How WhatsApp Helps Fight Child Exploitation.*
[89] *See: https://support.wire.com/hc/en-us/articles/202857164-How-does-Wire-handle-reports-of-misuse-; https://support.wire.com/hc/en-us/articles/203122400-How-do-I-block-or-unblock-someone-;*
[90] *https://support.wickr.com/hc/en-us/articles/115005136708-Block-Unblock-a-Contact; https://wickr.com/terms/; https://wickr.com/privacy/*
[91] *https://threema.ch/en/support; https://threema.ch/en/faq/unwanted;*
[92] *https://matrix.org/legal/terms-and-conditions*
[93] *https://desk.rocket.chat/portal/en/kb/articles/where-do-the-reported-messages-go; https://docs.rocket.chat/legal/terms; https://docs.rocket.chat/legal/privacy';*

	Terms of Service (ToS) prohibiting certain content / behaviours	Explicit prohibition of terrorism	Act against CSA content (publicly mentioned on website)	Pro-active monitoring for illegal content and/or use (publicly mentioned on website)	Possibility to ban accounts
Telegram[94]	✓	✓		✓ "To improve the security of your account, as well as to prevent spam, abuse, and other violations of our Terms of Service, we may collect metadata such as your IP address, devices and Telegram apps you've used, history of username changes, etc. If collected, this metadata can be kept for 12 months maximum."	✓
Session[95]	✓				✓
FortKnoxster	✓				✓
Hoop Messenger[96]	✓				✓
Conversations	Lack of publicly available information				

[94] https://telegram.org/tos; https://www.technobezz.com/how-to-report-someone-on-telegram/; https://telegram.org/faq; https://www.purevpn.com/how-to-block/telegram; https://telegram.org/privacy;
[95] https://getsession.org/terms-of-service/.;
[96] https://hoopmessenger.com/legal/

7. CHALLENGES FOR LAW ENFORCEMENT ACCESS

The complete protection from third party access afforded to end-to-end encrypted content also poses significant challenges for law enforcement and security agencies. The challenge arises both in monitoring the communications of criminal actors using E2EE services and in the collection of digital evidence.

The challenges for law enforcement access, when compliant with established procedure and and entrenched in the rule of law, can be summarised as follows:

- ISPs cannot disclose past messages at the request of law enforcement.
- ISPs cannot intercept and monitor live conversations at the request of law enforcement.

Beside those two questions relating to what can be provided by tech companies to law enforcement, there is also the question of law enforcement's need to access encrypted content foro two distinct purposes:

- Access to encrypted communications for monitoring purposes: to track and disrupt activities of criminal actors, or collect evidence for ongoing investigations into certain criminal networks.
- Collection of e-evidence following a particular event, for instance a terrorist attack, during which an encrypted messaging app was known to have been used by the perpetrators.[97]

Service providers offering E2EE do not have the technical ability to provide law enforcement with the content of the messages in a readable and decrypted format. There are only three solutions: to not implement E2EE, to implement it "incorrectly" such as by creating a backdoor, or to compromise the endpoints. An example of compromised endpoints was seen in the case of the NSO Group using vulnerabilities in encrypted messaging services to plant Pegasus spyware targeted devices.[98]

COMO vs. law enforcement access: Law enforcement and policymakers have conflated the two in assuming that "content moderation is fundamentally incompatible with end-to-end encrypted messaging" and, thus, E2EE poses important risks to national security.[99] The national security risk argument is often based on the fact that child sexual abuse and terrorist offenders can use E2EE to communicate and share illegal content without law enforcement being able to intercept it, nor tech companies being able to detect and remove this content shared via E2EE. The conflation of the two problems is also reflected in certain policymakers' calls for tech companies to ensure that CSA content can be identified on services offering E2EE.[100] The leaked EU report on technical solutions to detect child sexual abuse in E2EE communication focuses on such monitoring and moderation of E2EE content[101] – See Section 8 on Policymakers Calls For Access To And Traceability E2EE.

[97] *As was the case in the opposition between Apple and the FBI around the San Bernardino case inn 2015 and Pensacola in 2019*
[98] *Agraval Aditi (2020), Encryption and issues related to Terrorism and Communications, Medianama.*
[99] *Mayer Jonathan (2019), "Content Moderation for End-to-End Encrypted Messaging", Princeton University.*
[100] *Mayer (2019)*
[101] *EU Commission (2020a), Leaked report on technical solutions to detect child sexual abuse in end-to-end encrypted communications.*

7.a Overview of E2EE messaging apps: Approaches to criminal use and cooperation with law enforcement

	Information sharing with Third party including law enforcement	Legal framework for illegal content, reporting	App ownership	Governing law	Servers location
WhatsApp	✓	✓	Facebook	EU: Ireland Otherwise: State of California	Facebook servers worldwide
Signal	✓	✓ Legal and acceptable use detailed in ToS[102]	Signal Messenger LLC	State of California	Not mentioned
Viber	✓	✓ Legal and acceptable use detailed in ToS	Rakuten	worldwide	State of New York
Wire	✓ Transparency report	✓	Wire	"Outside the US: Switzerland (Zug Canton) US: US Law and State of California"	Switzerland, Germany and Ireland
Wick Me	✓	✓	Wickr	State of Delaware, US	Not mentioned
Threema	✓ Small transparency report[103]	✗	Independent	Switzerland	Zurich, Switzerland
Element/Riot	✓	✓	Matrix.org Foundation (maintained by)	England and Wales	Not mentioned
Rocket Chat	✓	✓ Legal and acceptable use detailed in ToS	Rocket.Chat	Not mentioned	Worldwide

[102] https://signal.org/legal/
[103] https://threema.ch/en/transparencyreport

	Information sharing with Third party including law enforcement	Legal framework for illegal content, reporting	App ownership	Governing law	Servers location
Telegram	✓	✓	Telegram	Canada[104]	Worldwide
Session	✓ Small Transparency report.[105]	✓ Legal and acceptable use detailed in ToS	Loki Foundation	Not mentioned	State of Victoria, Australia
FortKnoxster	✗ ✓ "Any authority must direct a request to the relevant authorities, which may then possibly contact us, following the protocol that the relevant legislation stipulates. We will not comply with demands from any authorities to a higher extent than the law demands."	✓	FortKnoxster Ltd	Gibraltar	Not mentioned
Hoop Messenger	✓	✓	Magnificus Software Inc	Canada	Not mentioned
Conversations	Lack of publicly available information				

[104] https://itelegram.com/telegram/tos.asp
[105] https://loki.foundation/transparency/

8. POLICYMAKERS CALLS FOR ACCESS TO AND TRACEABILITY OF E2EE

As encryption technology has become more developed and secure, and with E2EE now a common feature of messaging apps, governments and heads of law enforcement and security agencies have increasingly been calling for lawful access to encrypted communication. This has led to new legislation being passed or discussed to ensure law enforcement access, and in certain instances to compel service providers to answer requests for technical assistance to do so.

Legislative and other proposals for regulating online content have also directly and indirectly targeted the use of EMS. This has been the case in Brazil and India which have been significantly impacted by misinformation shared on messaging apps, as well as in Singapore which in 2019 introduced new legislation on "online falsehoods" applying to both social media platforms and messaging apps.[106]

In general, legislation impacting encryption can be divided into three categories:

1) Legislation aimed at facilitating and ensuring access to E2EE communications for law enforcement.
2) Legislation focusing on the detection and moderation of illegal content, mainly CSA material.
3) Legislation creating traceability requirements for messages shared on social media and/or messaging apps.

Monitoring vs. backdoor access: Whilst both online child sexual abuse and terrorist use of the internet have been central to policymakers' criticisms of E2EE as a potential criminal safe space, the two phenomena have each elicited different solutions:

- **CSA and the monitoring of content:** CSA has most often led to calls for tech companies to monitor content shared on E2EE services.
- **Counterterrorism and backdoors access:** In contrast, the counterterrorism argument has led to law enforcement asking for direct access to E2EE communication – in other words, for backdoors to be created. This is often done under the guise of improved technical collaboration, or assistance, between law enforcement and tech companies.[107]

This division is reflected in the divergent positions of EU bodies on E2EE:

- A report mandated by the EU Commission, the EU's executive branch, reviewed different technical solutions for monitoring CSA material on E2EE platforms.[108]
- A resolution from the European Council, the EU's collegiate body, on "Security through encryption and security despite encryption" – broadly covering terrorism and other illegal activities – called for law enforcement access to E2EE communications.[109]

[106] Even though Singapore's POFMA also covers encrypted messaging services, we are yet to see how this effectively applies to such services.
See: Tech Against Terrorism (2021a), The Online Regulation Series Handbook.
[107] This is notably the case in Australia and the United Kingdom, see the overview of legislation impacting E2EE below.
[108] EU Commission (2020a), Leaked report on technical solutions to detect child sexual abuse in end-to-end encrypted communications.
[109] Council of the EU (2020), Draft Council Resolution on Encryption - Security through encryption and security despite encryption.

1) Ensuring law enforcement access to E2EE communication and decrypted content: Such regulations are introduced with the explicit goal of providing a legal framework for law enforcement and security agencies to access E2EE communication, or a decrypted version of the communication content.

a) This is often framed as the basis for expedited cooperation between ISPs and law enforcement by requiring collaboration and, in some instances, the provision of technical assistance to grant law enforcement access to encrypted channels of communication and/or decrypted content.

b) Most of the legislation and proposals directly targeting encryption, emphasise in their drafting the importance of the right to privacy and the desirability of a secure and safe online environment for all. The EU draft resolution on encryption, for instance, states: "Competent authorities must be able to access data in a lawful and targeted manner, in full respect of fundamental rights and the data protection regime, while upholding cybersecurity." Similarly, the Australian government in its presentation of the Assistance and Access Act stresses "nothing in this legislation can require industry to break encryption."[110]

Most of the existing and proposed legal frameworks for law enforcement access have been criticised by technical and digital rights experts for effectively calls for "backdoors" to E2EE. Criticism is mainly directed at the lack of specificity in these regulations concerning what technical assistance may be requested from platforms, and in what instances access might be provided (including for which type of content). According to E2EE advocates, this could risk being used as a legal basis to compel services providers to create backdoors or remove E2EE altogether.

2) Scanning and monitoring encrypted content for illegal material: In both the EU and the US, 2020 saw much regulatory discussion about how to ensure that tech companies could act against CSA taking place on their services. This was notably the case of the EU Strategy For a More Effective Fight Against Child Sexual Abuse, published in July 2020, and of the original EARN IT Act proposed in the US in March 2020. [111]

a) Rather than calling for a backdoor access to encrypted communication, or to decrypted content, such proposals typically require tech companies to systematically scan all content shared by users for CSA material, thus directly infringing on users' fundamental right to privacy.

b) The conflict between the scanning of content for CSA content and the fundamental right to privacy is demonstrated by the EU requests for a temporary derogation to certain provisions of its ePrivacy Directive – which protects users privacy and communication content online.

[110] Australian Department of Home Affairs, The Assistance and Access Act 2018.
[111] On its introduction in early 2020, the EARNT IT Act was considered by digital rights advocates as the most serious threat to encryption, despite not directly and explicitly targeting it. It has since been amended to ensure that tech companies could not be held liable because they offer E2EE or other encryption services. However, the impact of EARN IT Act on E2EE in the long term is unknown – see Regulations with an ambivalent or unknow impact on encryption.

3) Traceability requirements: India and Brazil, two countries that have been significantly impacted by misinformation shared on WhatsApp, introduced legislative proposals in 2020 to compel encrypted messaging services to be able to trace back messages.

a) These typically require EMS to keep logs of messages shared on their services, as well as to store data domestically to ensure easy access by law enforcement.
b) These requirements are mostly linked to the possibility of analysing messages' metadata rather than on accessing the content itself.
c) Experts have questioned the implications for EMS that do not store metadata of users, or do so in a limited fashion. Traceability requirements will put significant pressure on EMS to develop the technical capacity to comply if they wish to continue operating in these jurisdictions.
d) Traceability requirements do not grant law enforcement access to the content of the messages. However, by compelling companies to keep logs of metadata of forwarded messages (which are the main targets of these proposals), one can in theory confirm whether a message concerns a specific topic by assessing whether another an identical (forwarded) message was sent. The ability to either positively or negatively confirm the content of a message, depending on whether it is identical to another one or not, has been criticised by digital rights advocates for weakening the confidentiality and privacy of E2EE communications.[112]
e) Critics argue that any traceability requirement would be detrimental to encryption by requiring platforms to "keep massive amounts of metadata", or by being, in effect, a breach of encryption to access the "payload" of an encrypted message.[113]

[112] *Rodriguez Katitza and Schoen Sean (2020), FAQ: Why Brazil's Plan to Mandate Traceability in Private Messaging Apps Will Break User's Expectation of Privacy and Security.*
[113] *Tsavkko Garcia Raphael (2020), Brazil's "fake news" bill won't solve its misinformation problem, MIT Technology Review; Rodriguez Katitza and Schoen Seth (2020), FAQ: Why Brazil's Plan to Mandate Traceability in Private Messaging Apps Will Break User's Expectation of Privacy and Security, Electronic Frontier Foundation; Rai Saritha (2020), 400 Million Social Media Users Are Set to Lose Their Anonymity in India, Bloomberg; Newton Casey (2020), India's proposed internet regulations could threaten privacy everywhere, The Verge; PYMNTS.com (2020), India's New Social Media Rules Would Strip Anonymity — When Asked — From Accounts.*

8.a Overview of key legislations impacting E2EE

Country / Region	Legislation / Proposal	Stage	Direct/Indirect impact on E2EE	Key points
United Kingdom	Investigatory Powers Act 2016 The Act was completed by five codes of practices in 2018 via the Investigatory Powers (Codes of Practices) Regulations 2018. These include the "Interception of Communications" code of practice.	Passed	Direct	● The Act governs and oversees the use of investigatory powers by law enforcement, security and intelligence agencies in the UK. ● The Act grants new powers to these agencies to access large volumes of data, and includes key provisions on tech companies removing encryption protection from messages and content shared by their users. To assist law enforcement, tech companies can be asked to remove encryption when presented with an interception warrant.[114] ● The code of practice on "Interception of Communications" sets out the procedure to be followed for obtaining data from the interception of communications, including guidelines related to encryption and its removal to comply with a legal request. ● A "Technical capability" explanatory note was drafted to provide details on the obligation related to the technical capability notice that can be handed with an interception warrant. ● In response to the tech sector's concerns about the risks posed to privacy in the country,[115] the government "softened" its language on the possibility of platforms having to break encryption by offering "a pragmatic approach" which specified that tech companies won't be compelled to remove encryption if not "technically feasible".[116] However, no more precise definition of "technically feasible" was supplied.[117]
Australia	The Assistance and Access Act 2018	Passed	Direct	● The Act allows law enforcement and intelligence agencies to request technical assistance from ISPs, and requires ISPs to develop new technical capability to provide this assistance if needed. ● Under Schedule 1 of the act: o Law enforcement can request voluntary assistance from providers via "a technical assistance request" or via "a technical assistance notice" where the provider is already capable of giving the required assistance. o The Attorney-General and Minister for Communications can jointly require a provider to develop a new capability via a "technical capability notice".[118] ● Signal announced that it would not comply with the new requirements.[119]

[114] *Pickworth Jonathan and Hickman Tim (2016), Investigatory Powers Act 2016 becomes law, White & Case.*
[115] *Hern Alex (2015), Tech firms warn snooper's charter could end strong encryption in Britain, The Guardian.*
[116] *Critics of the bills have responded to this amendment by calling it a "cosmetic tweaks" — Erik King, Don't Spy on Us Coalition" and saying that it "barely pays lip service to the concerns raised" – Jim Killock, Open Right Groups.*
See: Hern Alex (2016), Technology firms' hopes dashed by 'cosmetic tweaks' to snooper's charter, The Guardian.
[117] *Hern (2016).*
[118] *See: Australian Department of Home Affairs, Assistance and Access: Overview; The Assistance and Access Act 2018.*
[119] *Signal (2018), Setback in the Outback.*

Country / Region	Legislation / Proposal	Stage	Direct/Indirect impact on E2EE	Key points
US	Lawful Access to Encrypted Data Act (LEADA) of 2019, introduced by Senate Judiciary Committee Chairman Lindsey Graham, Senators Tom Cotton and Marsha Blackburn.[120]	Proposal / In discussion	Direct	● Aimed at countering "warrant-proof" encryption, LEADA is similar to the UK and Australian legislation in creating a framework for tech companies to assist law enforcement to access encrypted data, whether at rest or in transit, when presented with a court order. ● However, LEADA differs from other "technical assistance"-focused legislation by introducing additional requirements for service providers, and by creating incentives for technical solutions to be developed to ensure law enforcement access: o The US Attorney General would have the authority to issue directives to service providers requesting them to report on their ability to comply with court orders and the timeline of their compliance. o Service providers would be compensated by the government for costs incurred when complying with a directive. o A prize competition would be organised to encourage the development of "lawful access solutions that operate in encrypted environments while maximizing privacy and security". ● In addition, LEADA would also fund a programme for digital evidence training for law enforcement, and set up a "call center for advice and assistance during investigations" for law enforcement agents.
Brazil	Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, The Brazilian Internet Freedom, Responsibility and Transparency Act, or Law PLS2630/2020 Passed by the Senate in 2020, yet to be signed into a law by President Bolsonaro.[121]	Proposal / last phase	Direct	● This law would compel ISPs that offer instant messaging services to ensure the traceability of messages shared on their services, and to retain information of "viral messages" (shared by 5 persons and reaching at least a 1000 recipients) for 3 months.[122]
Singapore	The Protection of Online Falsehood Bill (POFMA), 2019	Passed	Direct	● The POFMA bill was the world's first online content regulation framework also applying to E2EE services, therefore setting a precedent for the regulation of such platforms. However, the legislation has yet to be effectively applied to E2EE platforms.[123]

[120] On LEADA, see: Covington and Burling LLP (2020), Lawful Access to Encrypted Data Act Introduced, Lexicology; McCullough Patrick (2021), EARN IT and LAEDA: How Private Is Too Private?, Reporter Magazine.
President Bolsonaro is expected to hold a public consultation about the law, and ultimately veto it. See: Boadle Anthony (2020), Brazil's Bolsonaro would veto bill regulating fake news in current form, Reuters; and Tulio dos Santos Diogo (2021), Brazil, democracy, and the "fake news" bill, Global Americans.
[122] Tech Against Terrorism (2021a).
[123] See: Asia Internet Coalition (2020), Toolkit: Addressing Online Misinformation Through Legislation; Amnesty International (2020), Singapore: Social media companies forced to cooperate with abusive fake news law; Chen Siyuan and Chia Chen Wei (2019), Singapore's latest efforts at regulating online hate speech, Institutional Knowledge at Singapore University.

Country / Region	Legislation / Proposal	Stage	Direct/Indirect impact on E2EE	Key points
India	Intermediary Guidelines and Digital Media Ethics Code Passed by the Indian Government in February 2021.	Passed	Direct	● The Intermediary Guidelines require online platforms mainly providing messaging services to ensure that the original sender of an online message can be identified, introducing a de facto traceability requirement that would weaken encryption by requiring EMS to hold large amounts of metadata.[124] ● If traceability is not compatible with the design of the EMS, the latest update will be required to modify its design to ensure compliance with the guidelines. ● The guidelines incorporate different provisions for regulating social media and EMS in India that had been discussed in the country since 2018 and were to be introduced in 2020, including certain provisions previously discussed in the Framework and Guidelines for Social Media Regulations.
France	2016 Amendment to the Code of Criminal Procedure, in relation to the countering of terrorism and organised crime. Adopted in 2016.	Passed	Direct	● France's regulatory framework on E2EE is not a backdoor mandate, nor a technical assistance requirement per se. However, laws related to legal hacking and to access to encrypt content have been passed to ensure law enforcement access to encrypted content, and cooperation from service providers when necessary.[125] ● The 2016 Amendment notably criminalises the refusal to hand over decryption keys when available.
European Union	Security through encryption and security despite encryption Draft council resolution on encryption, November 2020	Proposal / last phase	Direct	● This resolution calls on EU institutions to propose a legislative framework for legal law enforcement access to encrypted communications – mainly to counter terrorism and CSAM – and for facilitated cooperation with service providers.

[124] *See: Internet Freedom India (2021), Latest Draft Intermediary Rules: Fixing big tech, by breaking our digital rights?; and Robertson Adi (2021), India sets stricter rules for social media giants, The Verge.*
[125] *Schulman Ross and Bankston Kevin (2017), Deciphering the European Encryption Debate: France, New America.*

Country / Region	Legislation / Proposal	Stage	Direct/Indirect impact on E2EE	Key points
European Union	EU strategy for a more effective fight against child sexual abuse Published in July 2020.[126]	Passed	Direct	● The EU Strategy lays out 8 initiatives meant at providing a framework for "implement[ing] and develop[ing] the right legal framework, strengthen[ing] the law enforcement response and catalyse a coordinated multi-stakeholder action in relation to prevention, investigation and assistance to victims". ● The introduction to the strategy underlines the risks of criminal use of E2EE, and singles out Facebook's plan to roll out E2EE on all its messaging services as a risk to the efficient detection of CSAM online. ● The 7th Initiative, "Galvanise industry efforts to ensure the protection of children in their products" specifically focuses on the question of monitoring online communications for CSAM, and task the EU Internet Forum (EUIF) in assessing technical solutions to detect CSAM on E2EE services.[127]

Regulations with an ambivalent or unknown impact on encryption

Beside the legislation and regulations outlined above, which all risk jeopardising the use and security of encryption, other regulations recently passed or being discussed could also have an uncertain impact on the future of encryption. Whether these regulations will offer a framework for encouraging security and privacy online or will instead further pressure services providers to weaken or even renounce encryption is unknown at present.

[126] In February 2021, the EU launched a public consultation to inform the preparation of the different initiatives laid out in the Strategy.
[127] This process resulted in the presentation of a report on identifying CSA content on encrypted platforms at the EUIF in January 2021. However, the report had been leaked earlier in September 2020 raising concerns amongst digital rights advocates, tech companies and cryptography experts. For more information and analysis of the solutions presented in the report, please see Part 3 of this report on Criminal Use of E2EE – Strategies for risk mitigation.

Country / Region	Legislation / Proposal	Stage	Direct/Indirect impact on E2EE	Key points
UK	Draft Online Safety Bill The draft bill follows the Online Harms White Paper and the Full government response to the consultation. The White Paper was published in April 2019, and followed by a Public Consultation Process to which the UK Government responded in December 2020.	Proposal / In discussion The draft laws are expected to be introduced in Parliament in 2021	Indirect	● The Online Safety Bill, including the duty of care requirements and obligations to limit it the dissemination of illegal content, including terrorist content and CSAM, will also apply to both public-facing social media platforms and private messaging services. Mandating platforms to limit the dissemination of illegal and other harmful content will, in practice, compromise end-to-end encryption. ● This has led civil society and digital rights organisations to raise concerns about the duty of care applying to encrypted services.[128] In particular with regard to the "use of automated technologies".[129]
European Union	ePrivacy Rules 2021	Passed	Indirect	● In early 2021, the Council of the EU released new ePrivacy rules for online communications, prohibiting any interference, including screening, of online communication and related metadata. The regulation notes exemptions to the rules, including for national security reasons and criminal investigations. However, how that applies to detecting terrorist use of E2EE services remains unclear. ● Unlike other laws presented above, the ePrivacy rules do not negatively impact encryption. On the contrary, they request online service providers to do what E2EE guarantees: that online communications cannot be interfered with. ● However, whilst the EU has agreed on these rules it continues to pressure service providers to monitor CSA content and to call for law enforcement access in response to concerns over terrorist use. Thus. and despite the commitment to online privacy these rules indicate, they should not be seen as the end of EU pressure for access to and monitoring of E2EE communications.
European Union	Proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC. Proposed by the European Commission in September 2020, the final version was adopted by the European Parliament in July 2021.[130]	Passed		● Anticipating the impact the new EU ePrivacy Rules could have on the possibility to detect CSA online, the EU Commission proposed a temporary derogation from certain of the provisions of the ePrivacy Rules, while ensuring that tech companies' elective practices to detect CSA can continue. ● The EU Data Protection Officers underlined that the derogation would significantly impact EU citizens' fundamental right to privacy – see below.

[128] *Burns Heather (2021), Encryption in the Online Safety Bill, Open Rights Group.*
[129] *Barber Ian (2020), The UK Government's Full Response To The Online Harms White Paper: Initial Thoughts, Global Partners Digital; and Wingfield Richard (2020), The UK's Online Harms Bill: Potential Implications for the Right to Privacy, The GNI Blog.*
[130] *Bertuzzi Luca (2021), New EU law allows screening of online messages to detect child abuse, Euractiv.*

Country / Region	Legislation / Proposal	Stage	Direct/Indirect impact on E2EE	Key points
US	EARN IT Act, The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2019.[131]	Proposal / In discussion	Indirect	● The amended EARN IT Act,[132] approved by the US Senate Judiciary Committee in July 2020, creates a "carve-out" from Section 230's protection from legal liability for platforms that "advertise, promote; present, distribute or solicit CSAM."[133] ● Whilst Senator Leahy's Amendment to the Act offers E2EE services providers a defence against liability because they offer encryption, how this legislation might impact E2EE is unclear and will take time to determine. The reason for this is that the amended act delegates many issues to State law: "we won't know whether or not offering end-to-end encryption would be seen as violating state laws until long and costly cases go through their lengthy process."[134] ● According to commentators, the amended bill could thus incentivise platforms either to encrypt everything (as they could not be held liable for doing so), or to collect more personal information from users.

[131] On the EARN IT Act, see: Mullin Joe (2020) The New EARN IT Bill Still Threatens Encryption and Free Speech, Electronic Frontier Foundation; Makena Kelly (2020), A weakened version of the EARN IT Act advances out of committee, The Verge.
[132] The original proposed bill stipulated that tech companies would have to "earn" Section 230 immunity based on their content moderation practices, rather than being granted immunity by default. Offering E2EE, and thus not being able to monitor conversation would have meant tech companies risked losing Section 230 immunity. Thus forcing platforms to choose between encryption and Section 230 protection
[133] Masnick Mike (2020), New EARN IT Act Creates An Insane New Dilemma: Either Encrypt All Or Spy On All, TechDirt.
[134] Masnick (2020)

Measures interfering with E2EE should be specific, respect private life, proportionate and necessary to meet the stated objectives: In an opinion on the EU Proposal for temporary derogations from Directive 2002/58/EC – the EU's ePrivacy Directive[135] – for the purpose of combatting child sexual abuse online, the European Data Protection Supervisor laid out the requirements that should be met by any measure interfering with "the fundamental rights to respect for private life and data protection of all users of very popular electronic communications services, such as instant messaging platforms and applications". In so doing, the Data Protection Supervisor underlined the following:

- "Confidentiality of communications is a cornerstone of the fundamental rights to respect for private and family life and [the] protection of personal data", however, measures envisaged in the proposal on countering CSA material would interfere with such rights.
- Interference is possible, however, it should be provided for in law, respectful of "the essence of data protection and privacy', proportionate and necessary with regard to the "objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".
- Any legislation must be clear and precise with regard to the scope and application of the measures, and should include safeguards against the risk of abuse.[136]

A similar opinion was issued in a Substitute Impact Assessment on the Proposal for temporary derogations, published by the European Parliament Research Services in January 2021. The Assessment recognised the competence of the EU to make such derogations, but stressed that the impact on human and fundamental rights "has not been adequately addressed", with particular reference to the need to provide clear legal guidelines and ensure redress mechanisms. The opinion also assessed different practices to detect CSA content currently undertaken voluntarily by tech companies, including Facebook. It concluded that, except for Microsoft's PhotoDNA, existing mechanisms, including Facebook's algorithms, did not meet the requirements laid out in Article 3 of the EU's proposed regulations regarding the processing of data.[137]

[135] *The Directive can be found here: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058*
[136] *European Data Protection Supervisor (2020), Opinion on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online.*
[137] *"Article 3 of the proposed regulation requires processing of data to be conducted by technologies that are: "well-established" and "regularly in use" (Article 3(a)); "sufficiently reliable" and "least privacy intrusive" (Article 3(b)); and limited to the use of "relevant key indicators" (Article 3(c))."*
See: European Parliament Research Services (2021), Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse – Targeted Substitute Impact Assessment.

9. KEY ARGUMENTS AGAINST THE CREATION OF BACKDOORS

Technical experts, digital rights advocates, and tech platforms implementing E2EE have all warned that proposals for safe back doors and automated identification of illegal content carry significant risks of weakening or even breaching encryption. They argue that the requirements of technical assistance, especially in the form of developing new technical capacities, are not only not technically feasible but beyond that open the door to further security risks, and for more people, than they would resolve. Most experts agree that there is no such thing as a safe backdoor to encryption: all attempts to provide decryption keys for anyone other than the sender and recipient would ultimately result in a safety breach.

The main arguments advanced against backdoors and other technical requirements for tech companies to provide data in a readable format can be summarised as follow:[138]

- **Risk of exposure by weakening E2EE protocols:** Any backdoor, any provision of the smallest point of access would **weaken the entirety of the E2EE system**, creating technical weak points that could be further exploited and exposing all E2EE users – individuals, public, and private organisations alike – to the risk of security breaches. Backdoors would thus **expose the data and communication of billions of innocent users for the sake of monitoring a minority of criminal users**.

- **Displacing the threat instead of combating it:** An overall ban on encryption, or any regulation compelling tech companies to provide law enforcement with general access to encrypted communications **would push criminals to migrate to other services and devices**. Two EMS representatives interviewed for this report stressed that they had cooperated with law enforcement when required to do so, provided this would not weaken encryption. Both said that a ban on encryption or backdoor provisions would only risk criminals turning to services unwilling to cooperate with law enforcement, or designed solely for criminal use – Encrochat was one such service (see: Part 2, Section on Monitoring Of Encrypted Platforms By Law Enforcement Agencies).

- **Jurisdiction:** Backdoors also raise the question of **jurisdictional limits** and who would be trusted with escrow keys, if they were to be created. Experts have also raised concerns about criminals turning to services located in uncooperative jurisdictions, as well as about non-democratic countries using as a model for their own regulations the backdoors and bans implemented in democratic ones.[139]

[138] See: Cohn Cindy (2018), Resisting Law Enforcement's Siren Song: A Call for Cryptographers to Improve Trust and Security, Lawfare; Ruiz (2018); Cohn (2020); Polk (2020); Abelson H., Anderson R., Bellovin S., Benaloh J., Blaze M., Diffie W., Gilmore J., Green M., Landeau S., Neumann P., Rivest R, Schiller J., Schneier B., Specter M., Weitzner D. (2015), Key under doormats: mandating insecurity by requiring government access to all data and communications.

[139] ess democratic governments copying online regulations created and implemented in Western democracies is already the case for the regulation of online speech and content. See: Tech Against Terrorism (2021a).

● **Risks of exploitation by foreign governments:** There are no guarantees that hostile foreign governments won't gain access to newly created backdoors and use them to target governments and citizens in countries that have mandated backdoors.[140]

● **Thinking beyond the short term: 'We don't know what comes next'** is also an argument that has been made by digital rights and privacy advocates against backdoors, **arguing that we cannot be guaranteed of what will happen to our data and personal information in the years to come.** A long-term security vision is required both in the interest of national security (in relation to the sophistication of cyberattacks), and for the protection of citizens from their own governments. It is worth noting that the creation of a digital database of citizens' biometric data in France was criticised on similar grounds by the Commission Nationale de L'informatique et des Libertés (National Commission on Computer Technology and Freedom) and the Conseil National du Numérique (National Digital Council), which argued that the rise of populism in Europe make "these bets on the future unreasonable" regarding the end use of the database.[141] Similarly, there is no guarantee that in the future a government won't use access to E2EE beyond the purpose stated at the time the legislation was passed.

Beside the different risks presented above, E2EE advocates have also argued that there is little to no evidence that E2EE significantly hinders law enforcement investigations, or that access to it might be necessary:

● **No proof that access to E2EE would benefit investigations:** E2EE advocates stress that they are yet to be given proof that access to E2EE content would significantly benefit law enforcement investigations. More specifically, E2EE advocates assert that there is no evidence that intelligence needed for law enforcement purposes could not be obtained by other investigation techniques, including passive monitoring[142] of EMS, human intelligence or other open-source intelligence techniques.

● **Lack of evidence that E2EE prevents investigations:** E2EE advocates have argued that there is in fact no significant evidence that lack of access to E2EE communications hinders law enforcement's capacity to successfully lead investigations. The Washington Post has revealed that the FBI and US Department of Justice, in calling for backdoors, had exaggerated the number of investigations allegedly hindered by E2EE as just under 7,000.[143] FBI Director Christopher Wray had, in 2018, stated to the Congress and the Public that the FBI had been locked out of nearly 7,800 devices, when the actual number was 880.[144]

[140] See: Pelroth (2019); Hayden Michael (2019), Encryption Backdoors Won't Stop Crime But Will Hurt U.S. Tech, Bloomberg Opinion.
[141] Untersinger Martin, (2016), Que reproche-t-on au TES, le "mégafichier" des 60 Millions de Français ?, Le Monde.
[142] Passive monitoring in this instance refers to online investigations that do not engage or otherwise communicate with terrorists.
[143] See: Croker Andrew (2019), DOJ And FBI show no signs of correcting past untruths in their new attacks on encryption, Electronic Frontier Foundation; and Bershidsky Leonid (2019), End-to-end encryption isn't as safe as you think, Bloomberg opinion
[144] Bett Devlin (2018) , FBI repeatedly overstated encryption threat figures to Congress, public, The Washington Post.

tech against terrorism

PART 2

ASSESSING TERRORIST AND VIOLENT EXTREMIST USE OF E2EE

KEY FINDINGS

10. TERRORIST AND VIOLENT EXTREMIST USE OF E2EE

1. E2EE services are used for multiple operational and strategic purposes by terrorists and violent extremists. The security and privacy that E2EE offers makes it a preferred feature for operational purposes, including internal communications and logistical coordination, as well as the sharing of material for online training. The inability to moderate the content of communications means that E2EE messaging apps are also used by terrorists and violent extremists to spread propaganda externally. E2EE messaging apps are also used as "beacons" to redirect supporters to content hosted elsewhere.

2. Terrorists and violent extremists do not only consider the availability of E2EE when choosing a platform. Audience reach, usability, file storage capacity, security features such as self-destruct messages and password protection, as well as an app's wider branding on matters such as privacy and security are also taken into account.

3. Apps that combine E2EE as well as the above features tend to be preferred by terrorists and violent extremists. We assess that this is the main reason why Telegram, which is not fully E2EE, has been the favoured messaging app for Islamist terrorists and far-right violent extremists in the past few years.

4. There are no publicly known instances of law enforcement breaking E2EE in transit. However, there are some reported cases in which law enforcement have managed to access encrypted content via several other tactics including use of sock puppets, targeted malware, wiretapping, and log-in hacking.

ASSESSMENT

11. TERRORIST AND VIOLENT EXTREMIST USE OF E2EE

Calls for law enforcement access to E2EE content, and for such content to be capable of moderation, are often based on the argument that E2EE platforms create safe spaces for terrorists, violent extremists, and other criminal networks to communicate without surveillance or interruption. Below we review terrorist and violent extremist (T/VE) use of encryption to assess this argument, and provide an overview of known instances where law enforcement have managed to monitor T/VE activities on encrypted platforms to date.

✓ Extensive known use by terrorists or violent extremists for this purpose

✓ Some known use by terrorists or violent extremists for this purpose

⊘ No known use by terrorists or violent extremists for this purpose

Overview of E2EE Platforms Used by Terrorists and Violent Extremists

	Propaganda dissemination	Internal communication	Individual recruitment	Fundraising	Link sharing
Conversations	✓ Conversations account promoted on al-Qaeda-affiliated "Gnews" RocketChat server; similar accounts promoted regularly by pro-IS networks on Hoop, Rocketchat and Telegram.	✓	⊘	⊘	✓
Element	✓ Resilient networks of IS supporters which migrated to Element following Europol operation on Telegram in November 2019.	✓	⊘	⊘	✓ Frequent use of outlinks by IS and al-Qaeda supporters to third-party paste sites and messaging platforms.
Hoop	✓ First exploited by IS and its supporters as an alternative to Telegram following Europol operation in 2019.	✓	⊘	⊘	✓ Out links shared frequently on IS-affiliated Hoop channels, including to file sharing sites, Hoop channels and channels on third-party messaging platforms.
iMessage	⊘	✓ Recommended by pro-IS online operational security guide, cited in San Bernardino attack case.[145]	⊘	⊘	⊘

[145] https://www.wired.com/wp-content/uploads/2015/11/ISIS-OPSEC-Guide.pdf

	Propaganda dissemination	Internal communication	Individual recruitment	Fundraising	Link sharing
Line	⊘	⊘	⊘	⊘	⊘
Minds	✓ Moderate exploitation by violent Islamists for propaganda purposes; extent of use of encrypted messaging feature unknown.	⊘	⊘	⊘	✓ Violent Islamist accounts on Minds monitored by Tech Against Terrorism in November 2020 frequently distributed long lists of outlinks to content on third-party platforms.
Protonmail	⊘	⊘ Recommended by IS supporters in an operational security guide originally created by Cyberkov, a Kuwaiti security company.[146]	✓ Protonmail addresses frequently cited as point of contact by violent far-right and Islamist terrorist groups online	⊘	✓ Some IS-affiliated propaganda groups have asked supporters to contact them via Protonmail for links to messaging channels
Rocketchat	✓ Dedicated servers for propaganda dissemination for both Islamic State and al-Qaeda	✓ Extensive networks of IS supporters on Rocketchat; users typically contactable by private message.	⊘	✓ Fundraising mentioned infrequently in IS-affiliated Tech Haven server monitored by Tech Against Terrorism.	✓ Outlinks used frequently in both IS-affiliated Tech Haven and al-Qaeda-affiliated GeoNews servers on RocketChat, including third-party messaging platforms and paste sites.
Signal	⊘	✓ Recommended on Telegram by OpSecGoy, a prominent online neo-Nazi operational security advisory group; used by members of "Triple K Mafia", a successor to National Action in the UK.[147]	⊘	⊘	⊘

[146] *Ibid.*
[147] *https://www.thelondoneconomic.com/news/two-men-teenager-in-court-accused-of-being-members-of-national-action-in-rebranded-group-called-triple-k-mafia/11/09/*

	Propaganda dissemination	Internal communication	Individual recruitment	Fundraising	Link sharing
Telegram	 Widely used for propaganda by both far-right and violent Islamist terrorists; dissemination primarily occurs on channels that are not E2E encrypted		 Telegram used extensively by Middle East-based IS "handlers" or "virtual entrepreneurs" in terrorist attacks in the West since 2015.[148]	 Used by IS supporters to raise funds for women in al-Hol refugee camp in north-eastern Syria; Bitcoin addresses often posted by far-right fundraisers.	 Some terrorist or violent extremist channels dedicated almost entirely to "join links" for other channels
Threema	 Accounts promoted regularly by both IS- and al-Qaeda-affiliated groups online. Cited in pro-IS operational security guide.[149]	 Reportedly used by a terrorist handler prior to a IS-claimed attack against Western tourists in Tajikistan in July 2018.[150]			
Tutanota			 Offered as point of contact by Feuerkrieg Division, a European far-right terrorist group, and National Socialist Order, a US-based neo-Nazi organisation. Also often recommended by violent far-right Telegram channels.		

[148] *Meleagrou-Hitchens Alexander and Hughes Seamus (2017), The threat to the United States from the Islamic State's virtual entrepreneurs, CTC Sentinel.*
[149] *https://www.wired.com/wp-content/uploads/2015/11/ISIS-OPSEC-Guide.pdf*
[150] *https://twitter.com/rcallimachi/status/1142994698782400512?s=20, Rukmini Callimachi (2017), How a couple's dream trip ended in tragedy at the hands of ISIS, Independent.*

	Propaganda dissemination	Internal communication	Individual recruitment	Fundraising	Link sharing
WeChat	 Reportedly used by IS supporters to circulate propaganda.[151]				
WhatsApp	 Some use of WhatsApp for propaganda dissemination by IS and al-Qaeda; larger files shared via outlinks				 WhatsApp phone number offered as contact to obtain access to TechHaven, a prominent IS-affiliated Rocketchat server.
Wire		 Account on Wire promoted by National Socialist Order in early 2021; group requires authentication to access	 Wire group promoted by National Socialist Order in early 2021		

[151] *Yaila Ahmet S. and Speckhard Anne (2017), Telegram: The Mighty Application That ISIS Loves – Part I, Vox-Pol.*

11.a Why turn to E2EE?

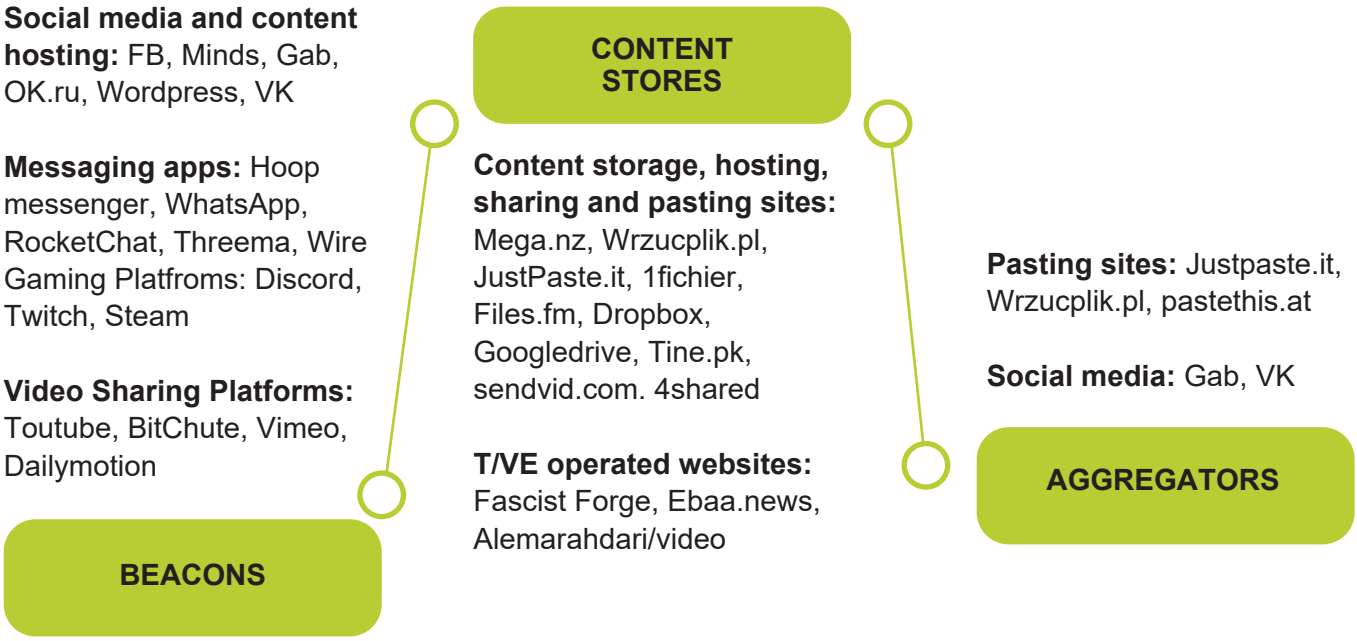
Terrorist and violent extremists exploit the entire tech eco-system of online platforms to achieve their strategic and operational aims. Inevitably, this includes encrypted platforms and services. Terrorists increasingly rely on encryption technology,[152] including E2EE, for internal communication and operational purposes, a phenomenon known as "going dark" or "dark social" in reference to new security features that render the tracking and retrieving of content particularly difficult.[153]

Aside from their propaganda output, terrorist groups and violent extremist networks are by definition clandestine, and so require the ability to communicate privately and securely, particularly when operating internationally or across wide geographical areas. Encryption provides them with a means through which to communicate online without fear of their communications being monitored or intercepted in transit by state agencies or law enforcement. E2EE apps can also serve more general strategic purposes and be used by terrorists and violent extremists as a stable platform on which to more reliably disseminate their content to their core non-operational support base.

- **Online security and operational purposes: Exploitation of internet technologies for operational purposes serves several aims including fundraising, online training as well as planning and coordinating attacks.** Terrorist use of the internet reflects a dual existence online structured around external and internal communication. In this context, closed online spaces are preferred for operational purposes, in particular for coordination between actors.

- **Diffusion of messages saved from content moderation:** Beside operational purposes, E2EE platforms can also be used for strategic purposes, namely propaganda, recruitment, and radicalisation-related activities. In these instances, group chats in E2EE messaging apps are used as "beacons" by terrorist and violent extremists, acting as a lighthouse/signpost to where the content can be found, without risks of being deplatformed by tech platform moderation teams. This is typically the case when a group chat is used to share links to where the content can be found (platforms serving a content storage or aggregator role for the diffusion of content as shown below).

[152] Encryption technologies, in particular E2EE messaging apps, are widely used by online users across the world, with no connection whatsoever with terrorist and violent extremist or criminal use. With internet users increasingly wary of privacy and security when using online platforms, many have turned to E2EE messaging for daily communications with friends, family, and colleagues, and the most commonly used messaging apps globally have rolled out, or are planning to roll out, E2EE encryption. The fact that WhatsApp is the world leading messaging app demonstrates this mainstream use of E2EE, as does the number of "secure and private" messaging apps such as Signal, Wire, or Wickr. Countering terrorist use of encrypted platforms is a difficult exercise, and particularly at risk of adversarial shifts if malevolent actors were to gain access in the encryption systems.
See: Butcher Birgit (2020), "WhatsApp, WeChat and Facebook Messenger Apps – Global Messenger Usage, Penetration and Statistics", Messenger People; and C. John (2020), "Most secure messaging apps on the market in 2020", AtlasVPN
[153] Conway, McNair, and Scrivens (2019); Graham Robert (2016), "How terrorists use encryption", in CTC Sentinel, Vol.9, Issue 6



To further comprehend how E2EE apps are used for both operational and strategic purposes, the table below summarises how some prominent E2EE services are used by terrorists and violent extremists. In general, platforms that can serve both strategic and operational purposes (for instance E2EE chats and large file-storage capacity to share content), are preferred by terrorists and violent extremists, as demonstrated by the exploitation of Telegram – see Section below.

11.b Beyond E2EE: what makes a platform attractive to terrorists and violent extremists

Whilst E2EE apps are preferred for operational purposes, other online platforms and services are used for more strategic purposes, including propaganda (recruitment, radicalisation, incitement to attacks), and the intimidation of perceived enemies. This also includes financing, such as calls for financial support by supporters of Islamic State on social media.[154] For terrorists, the exploitation of social media constitutes the main medium to get their message across to the widest audience possible, thanks to widespread use of social media globally and its public nature.[155]

[154] *Islamist terrorist groups have been known to exploit both Facebook and Instagram to do so. See: Farivar Cyrus (2020), "Feds announce largest seizure of cryptocurrency connected to terrorism", NBC News; Speckhard Anne and Ellenberg Molly (2020), "Inside the Sisterhood Springing Jihadis From Jail", The Daily Beast.*

[155] *Speckhard and Bodo (2018); Bertram (2016); Kavanagh, Carr, Bosco and Hadley (2017); Rudner (2017); and Berger J.M and Perez Heather (2016), "The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters", GW Program on Extremism*

In light of this, E2EE is far from being the only feature terrorists and violent extremists look for when exploiting online platforms and apps. Experts have shown that terrorists and violent extremists search for three main categories of features in an online platform or app: security, stability, and audience reach.[156] To these three categories, Tech Against Terrorism has added a fourth: usability.[157] In general, terrorists will try to establish themselves on a platform possessing all these features, although improvements in the content moderation capabilities of online platforms means that they typically have to balance these characteristics when selecting a platform. We summarise below the qualities that terrorists typically look for in an online platform.[158]:

- **Security:** Enhanced security and privacy features, such as E2EE.
- **Stability:** Limited capacity, or in some cases a limited willingness, to remove content or ban accounts, resulting in a more stable online presence for terrorist accounts or groups. Open-source software is also appealing as it offers terrorists the opportunity to develop their own platforms.
- **Audience reach:** Features that increase their ability to reach a wide audience, such as large-capacity groups or channels with unlimited audience.
- **Usability:** Encompassing the different features that make an app user-friendly, usability includes those that make the platform attractive to a wider audience and prove useful for organisational and idea-sharing purposes.

To better understand how these different sets of features apply to different messaging services offering E2EE, the below table compares WhatsApp, Telegram, Element (formerly Riot) and Signal according to the features and characteristics identified in this report as being particularly appealing for terrorists and violent extremists online.

[165] Conway, McNair, and Scrivens (2019); Clifford Bennet and Powell Helen (2019), Encrypted Extremism Inside the English-speaking Islamic State Ecosystem on Telegram, George Washington Programme on Extremism; Hayden Michel (2019b), "Far-Right Extremists Are Calling for Terrorism on the Messaging App Telegram", Southern Poverty Law Center; and Tech Against Terrorism (2019a), "Insights from Europol's 2019 European Counter Terrorism Centre Advisory Network Conference"

[157] Tech Against Terrorism (2019b), "ISIS use of smaller platforms and the DWeb to share terrorist content"

[158] The use of Telegram by terrorists and violent extremists of all persuasions exemplifies this. The messenger app offers both large audience-capacity through unlimited-size channels that can be searched by keywords, closed groups and encrypted discussions, as well as large file-storage capacity – to name of a few of the features that render it attractive for malevolent actors. Telegram's public commitment not to share data with governments and refusal to be a part of "politically motivated censorship" further adds to its integration for terrorists and violent extremists.
See: Squire Megan (2020), "Alt-tech & the radical right, part 3: why do hate groups and terrorists love Telegram?", Centre for Analysis of the Radical Right; Owen Tess (2019), "How telegram became White Nationalists' go-to messaging platform", Vice News; Mazzoni Valerio (2019), "Far Right extremism on Telegram: A brief overview", European Eye on Radicalization; Hayden (2019b).

	WhatsApp	Telegram	element	Signal
Audience reach – Public channels?	No public channels feature, making it difficult for terrorist and violent extremist groups to recruit or exert influence beyond their core support base.	Choice between public and private channels, as well as E2EE secret chats or client-server encrypted public channels and groups, enables terrorist messaging to reach a large audience whilst also allowing for secure internal communication.	Public terrorist channels and groups are searchable within the application's "explore" function.	Public terrorist channels and groups are searchable within the application's "explore" function. No public channels, making it difficult for terrorist groups to recruit or exert influence beyond their core support base.
Audience reach – How are groups accessed?	Groups can be accessed only via an invite link. There is no in-app search function for groups.	Search function enables easy discovery of and access (via link) to public terrorist groups and channels.	Private terrorist groups and channels accessible with an invite link.	No in-app search function for groups; possible to access groups via join links as well as QR codes. Ability to control inward flow of users to a group with admin approval feature.
Audience reach – Group size limit?	Group chat size is limited, with a maximum of up to 256 group members.	Terrorist groups and channels can reach a wide audience, with a supergroup member limit of 200,000 users, and a theoretically unlimited viewership for channels.	Element describes its group size limit as "huge", without giving a number.	Relatively large group size limit of 1,000 members.
Usability – File size limit?	A relatively small file size limit of 100mb inhibits terrorists' ability to store files within WhatsApp chats, instead forcing them to rely on outlinks to third-party platforms.	A 2gb file size limit allows terrorists and violent extremists to share and store large files such as high-resolution propaganda videos within the app.	Not known.	300kb MMS file size limit, making sharing of high-resolution videos or other multimedia difficult.
Security – Proxy server feature?	Terrorists must rely on a VPN, as WhatsApp does not have a built-in proxy server feature.	Built-in proxy server feature enables terrorists and violent extremists to hide their IP location.	Based on the decentralised Matrix network.	Built-in proxy feature enables access in countries where the app is banned.
Security – Personally identifiable information required?	Phone numbers are required for registration and are visible in group chats, potentially assisting authorities with the identification of terrorist offenders using the platform.	Phone numbers required for registration, but Telegram gives the option of hiding a user's number from their public profile.	Only username and password required for registration; email address optional addition for account recovery.	Telephone number required for registration, telephone numbers visible in group chats.

11.c Terrorist and violent extremist use of E2EE: Telegram case study

Despite its close similarities to WhatsApp in terms of product offering, Telegram has been more widely exploited by terrorists and violent extremists in recent years.[159]

Telegram offers a broader range of features that provide terrorists and violent extremists with an app that is easy to use, both secure and more stable than other platforms, and allows users to reach a wider audience. WhatsApp features secure encryption in all chats, but it offers a more limited range of other features, inhibiting the ability of terrorist and violent extremist organisations and networks to achieve their key online aims. The below graphic compares some of Telegram's key differences to WhatsApp, to illustrate why Telegram has been more widely exploited by terrorists in recent years.

A not so encrypted platform

Media reporting and public commentary around such use has often focused on Telegram's encryption, conveying the impression that this is the app's primary attraction for nefarious actors. Contrary to popular perception, however, not all messages sent on Telegram are protected by E2EE, with the majority being supported only by client-server encryption. While terrorists certainly view encryption as a positive feature, this is not the only feature that is seen as important for terrorists online. Below, we develop on the key features of Telegram that have proven attractive to terrorist and violent extremists. In addition to the platform's features, Telegram has continuously demonstrated a commitment to data protection and privacy and refused to share user data with governments.[160] The platform brands itself as an app that refuses to engage in "politically motivated censorship".[161] Whilst this implicitly refers to countries where criticism of the government is illegal, anti-censorship branding is an appealing one for violent extremists facing persistent moderation efforts from online platforms, as is the assurance that a given platform is unlikely to pass on their personal information to the authorities.[162]

[159] *"Europol and Telegram take on terrorist content online', Europol Press Release, 25 November 2019, available at: https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online; Rebecca Tan, 'Terrorists' love for Telegram, explained, Vox, 30 June 2017, available at: https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter, Will Bedingfield, 'How Telegram became a safe haven for pro-terror Nazis, Wired, 1 March 2020, available at:https://www.wired.co.uk/article/hope-not-hate-telegram-nazis, Jakob Guhl and Jacob Davey, 'A Safe Space to Hate: White Supremacist Mobilisation on Telegram', Institute for Strategic Dialogue, 26 June 2020, available at: https://www.isdglobal.org/wp-content/uploads/2020/06/A-Safe-Space-to-Hate.pdf.*

[160] *Hope Not Hate, (2020), "The Terrorgram network: a spiral towards bloodshed" in 2020 State of Hate Report; and Owen Tess (2019), How telegram became White Nationalists' go-to messaging platform, Vice News.*

[161] *Telegram, "Frequently Asked Questions"*

[162] *It should be noted that this 'non-censorship' appeal of Telegram is not set in stone. Indeed, after having been labelled as an online safe haven for the Islamic State, Telegram took action against the terrorist group use of its platform in November 2019, in coordination with Europol's internet referral unit. The medium- and long-term impacts of Telegram's first major removal of terrorist content and channels on its platform, remain to be compressively monitored and analysed. Including whether it will have an impact on far-right violent extremists' perception of the platform.*

TELEGRAM: ANALYSIS OF FEATURES

AUDIENCE REACH

• Public groups and channels are searchable within Telegram and are openly accessible to all users.

• Private groups and channels that are not searchable can be accessed via a join link, which can be promoted on public channels and third-party platforms.

• Supergroups can include as many as 200,000 members

• Channels can broadcast to a theoretically unlimited number of users

SECURITY

• Secret chats are protected by client-client end-to-end encryption. Content and messages shared can only be accessed on the device of origin or destination. Secret chats include a self-destruct feature.

• Public and private groups and channels are protected by client-server/server-client encryption.

• Telegram is founded on principles that emphasise user privacy. It states on its website that “protecting your private conversations from snooping third parties such as officials” is an essential foundation of the platform.

STABILITY

• Channels, and the messages and multimedia content contained within, often remain available after channel administrator accounts are suspended

• Terms of Service only explicitly prohibit the promotion of violence on “publicly viewable Telegram channels”. This means that private channels and groups do not seem to be targeted by content moderation.

• Telegram cloud servers are placed in several countries across the world, to avoid any specific state from having sole jurisdiction. The company is based in Dubai, but says that it is “ready to relocate again” if local regulations change.

USABILITY

• Accounts can be set up using only a telephone number, which can be changed at any stage.

• Large 2GB file size limit, allowing for sharing of large files including feature-length videos.

• Cloud-based storage with seamless sync. Messages are accessible from several devices simultaneously, and users can share an unlimited number of files. If users do not want data stored on their device, they can keep it in Telegram’s cloud.

• Multimedia history of channels and groups viewable in a separate tab.

• Channel feature allows administrators to control the flow of information. Only they can post, permitting for a unidirectional flow of curated content.

11.d Terrorist and violent extremist perceptions of E2EE platforms

Terrorists and violent extremists greatly value encryption. The media output of the several online groups dedicated to operational security for violent extremists illustrates this, particularly that of the prominent IS-linked Electronic Horizons Foundation and the extreme far-right OpSecGoy. Both have referred frequently to strong encryption in the past couple of years as a positive and essential tool through which terrorists can and should communicate. In addition, they have warned against the use of certain applications on the basis that their encryption software is insufficiently secure, and that their communications may be compromised.

Encrypted messaging services recommended by the IS-affiliated EHF	
Telegram	● The EHF identifies Telegram as a "social network" that has been used "intensely" by IS supporters, relying on it to publish 'news' and videos. ● It highlights that content can be made accessible through other social networks and via search engines. ● EHF cites the 'false propaganda' about Telegram's safety and encryption. ● It warns that users are 'forced' to use Telegram's servers, unless in a secret chat. ● It also flagged a change in Telegram's privacy policy in a post to its website in March 2020, warning that the platform will 'hand over the data of terrorists' if requested to do so by governments.
WhatsApp	● The EHF describes WhatsApp as a secure option, protected by E2EE. ● The EHF shared an article on RocketChat in February 2020 warning that WhatsApp join links that had been posted online were being indexed by Google, meaning that they were - at least in theory - publicly available.
Element Messenger	● The EHF highlights that Element supports encrypting messages and conversations by default. ● The EHF had its own channel on Element at the time of writing. ● It has pointed out that Element can be hosted on dozens of decentralised servers, making it more stable than centralised platforms. ● It can be used on most operating systems, including Tor. ● It advises against using only the Matrix.org server, as this is prone to content moderation. ● It suggests the use of a VPN with Element if not accessing via a Tor browser.
Conversations.im	● The EHF identifies Conversations as 'one of the best' encrypted apps for the Android system. ● It highlights the OMEMO protocol used by Conversations as more secure than OTR and OPENPGP. ● The EHF points out the benefits of XMPP server selection, allowing users to select servers to send and receive messages. It says this makes it impossible for "an attacker" to intercept metadata from messages. ● The EHF advises the use of automatic message deletion.
Hoop Messenger	● EHF described Hoop Messenger in June 2020 as having "similar features in the publication of the Telegram platform", including E2EE within the store feature only. ● It highlights the ability to create different accounts with a single phone number and email. ● It also highlights the internal browser that includes a VPN proxy to change the IP address while browsing websites. EHF advice to users: ● It warns that conversations and public channels are not encrypted, and are stored on the company's server. E2E is available within the store's feature only. ● It advises the use of Hoop Messenger for propaganda only, and not to send or store sensitive or personal data.

12. SUSPECTED USE OF E2EE IN TERRORIST ATTACKS AND ITS IMPACT ON THE ENCRYPTION DEBATE

Policymakers' repeated calls for E2EE-supported platforms to provide the authorities with 'backdoor' access to data within their systems are often based on arguments in favour of national security and public order. Debates on this issue have repeatedly reignited following high-profile terrorist attacks in the West, particularly when there is evidence to suggest that perpetrators had used encrypted messaging platforms to communicate.

- **Apple vs FBI:** Following an Islamist terrorist attack on Pensacola Naval Base in Florida in December 2019, Apple refused to unlock the suspect's iPhone or build a 'backdoor' for law enforcement to access its encrypted data, on the basis that such a tool could be exploited by anyone if created, thus compromising the security of all Apple users. The company has maintained its position on this since a dispute between it and the US government following an attack in San Bernardino, California, in 2015. Summarising the government position, Attorney General William Barr said in a statement in January 2020 that the dispute "perfectly illustrates why it is critical that investigators be able to get access to digital evidence once they have obtained a court order based on probable cause. We call on Apple and other technology companies to help us find a solution so that we can better protect the lives of Americans and prevent future attacks".[163]

- **EU calls for mandatory backdoors:** In the wake of the January 2015 terrorist attacks in Paris, which targeted the satirical newspaper Charlie Hebdo and a kosher supermarket, the EU Counter-Terrorism Coordinator Gilles de Kerchove called for increased counterterrorism coordination efforts at the EU level. Amongst his recommendations on information sharing, he suggested that tech companies operating in the EU should be compelled to provide law enforcement with access to encrypted content, including via the sharing of encryption keys.[164] Since then, EU institutions, including de Kerchove himself, have increasingly issued calls for law enforcement access to encryption.[165] Most recently, they did so a few days after a terrorist attack in Vienna claimed by IS on 2 November 2020, as demonstrated by a leak draft Council resolution dated 6 November.[166]

[163] https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-findings-criminal-investigation-december-2019
[164] Council of the European Union, EU Counter-Terrorism Coordinator (2015), EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015; Europa Nu (2015), EU wants internet firms to hand over encryption keys. Interestingly de Kerchove's notes explicitly referred to tech companies rolling out E2EE in response to the Snowden revelations. However, there is no mention of how mandating backdoors would be perceived by the same public and tech companies that have turned to E2EE in response to governments led surveillance programmes.
[165] See: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/#; Meister Andre (2020), Anti-Terror-Koordinator der EU fordert Gesetz gegen Verschlüsselung, Netzpolitik.org; Commissioner Johansson, EU Commission (2020), Speech by Commissioner Johansson at a webinar on "Preventing and combating child sexual abuse & exploitation: towards an EU response",: Statewatch (2020), Security through encryption and security despite encryption; European Commission (2020), Leaked report on technical solutions to detect child sexual abuse in end-to-end encrypted communications.
[166] Council of the EU (2016) Draft Council Resolution on Encryption - Security through encryption and security despite encryption,

Attack	Response
January 2015 attacks in Paris, France	• The prosecutor, Francois Molins, said that at least one of the attackers had 'received instructions from abroad' • British Prime Minister David Cameron states that encrypted apps should not be 'exempt from being listened to' by the authorities.
November 2015 attacks in Paris, France	• Telegram had been downloaded on a phone discovered near the Bataclan. No recovered content is mentioned in police reports, suggesting that the attackers may have used the self-destruct feature. • An open letter published by special prosecutors in 2017 including one involved in the Paris case criticised encryption, claiming that it 'significantly weaken[s] investigations, sometimes to the point of making them impossible'.
December 2015 attack in San Bernardino, US	• One of the attackers had previously communicated with extremists domestically and abroad. • The attack sparked a debate between the US authorities and Apple over a password-protected iPhone used by one of the terrorists. Apple refused to unlock the device, despite being ordered to do so by a US judge.
March 2017 attack in London, UK	• The attacker used WhatsApp three minutes before mounting the attack. The authorities were unable to access the contents of the messages. • Home Secretary Amber Rudd described end-to-end encryption as 'completely unacceptable', adding that 'there should be no hiding place for terrorists'.
May 2017 attack in Manchester, UK	• The attack reignited policy debates about encryption. Media outlets reported that the government was intending to lobby MPs to ensure that new rules get passed through parliament to enable the authorities to demand access to encrypted apps under warrant.
December 2019 attack in Pensacola, US	• The terrorist attempted to destroy his phone, leading investigators to believe that it contained crucial information. • The dispute between Apple and the US government flared up again, with the latter demanding access to the password-protected handset. Apple refused, but investigators gained access to the handset four months later.
October-November 2020 attacks in France and Vienna, Austria	• A video critical of the French teacher murdered near Paris in late October had reportedly circulated on messaging apps including WhatsApp and Facebook Messenger. A pupil's parent reportedly exchanged messages with the attacker on WhatsApp in the days running up to the murder. • Home Affairs ministers from EU member states released a statement in November calling on heads of state to "consider the matter of data encryption so that digital evidence can be lawfully collected and used by the competent authorities".

13. MONITORING OF ENCRYPTED PLATFORMS BY LAW ENFORCEMENT AGENCIES

There are no publicly available case studies where law enforcement have intercepted end-to-end encrypted communications in transit. But they have used various techniques to access encrypted messages at their endpoints, or to identify and arrest suspects by means other than 'breaking' encryption. Below is an overview of some of the key techniques used by states to access encrypted communications, including case studies.

13.a Sock puppets

● **Law enforcement agencies use publicly-available information** to investigate and track criminal and terrorist suspects online through open-source intelligence. Sock puppet accounts can be used to find, track and monitoring terrorist and violent extremist networks operating in both public and private domains. Terrorists and violent extremists, as well as non-violent activists, utilise public channels and social media accounts for propaganda and recruitment purposes in an attempt to reach a broad audience. By following these accounts and pages, law enforcement can access limited encrypted channels via join links, which are often shared on the open web by those being monitored.

● **This monitoring can be either passive or participative.** Passive monitoring in this instance refers to online investigations that do not engage or otherwise communicate with terrorists. This can present impediments to entry, particularly to encrypted messaging channels and groups. Some are accessible to a 'passive' observer via join links, which can be shared on public channels or pages. Others require authentication to access, such as a set of questions to prove an individual's identity or ideological allegiance. Participative monitoring goes further, involving active engagement and communication with violent extremists and terrorists online. The FBI in particular is known for its participative investigations and active infiltration of terrorist networks online, during which undercover agents pose as members of terrorist cells and communicate directly with suspects. In a recent example, a far-right extremist was arrested by the FBI in September 2019 after an undercover FBI agent discussed plans with him on Telegram Messenger to mount a terrorist attack in Texas, USA.[167]

[167] *Levine Mike (2019), FBI arrests Army soldier who allegedly discussed plans to bomb major American news network ABC News.*

13.b Targeted malware

● There have been only a small number of publicly-reported instances in the past five years of law enforcement agencies and states using malware to access encrypted communications sent on tech platforms. Depending on the jurisdiction of the action this can be legally questionable, however, and particularly so if a warrant is not obtained ahead of the operation.

● A key example of this kind of approach is Pegasus, a spyware that can be installed on devices running versions of iOS, as well as some Android devices. The spyware can be installed on targeted devices upon the clicking of a malicious link, which secretly enables a jailbreak allowing access to text messages, calls, and information from encrypted apps including WhatsApp, Telegram, Skype and iMessage. The spyware has been widely abused, including to spy on peaceful activists and journalists and policy makers by nation states.[168]

A coordinated operation between European states led to the arrests of hundreds of organised criminals in July 2020. The operation concerned EncroChat, a Europe-based secure communications network and service provider that offered specially modified and end-to-end encrypted handsets. All messages sent with an "Encrophone" were encrypted using the ZRTP protocol, and transmitted over a closed loop network. The company also removed the camera, microphone and GPS from the devices.[169] The service became extremely popular among organised criminals.[170] The company described itself as an 'end-to-end security solution' that could 'guarantee anonymity' to its users via specially modified devices.[171] As part of a years-long operation, the French gendarmerie managed to identify that the network was hosted on a server in France, later penetrating the network and installing malwar which allowed them to intercept millions of messages sent between EncroChat users globally and led to several arrests of organised criminals. EncroChat has described the operation as 'illegal'. It is unclear precisely how the French authorities were able to do this, as the details remain classified.[172] But the success of the operation was reportedly contingent on the use of a malware that had been specifically created for the X2 model of phone used in most Encrophones. The malware allowed the authorities to read affected users' screen lock passwords, and also disrupted a feature that allowed users to quickly wipe their data. EncroChat responded to an initial attack by pushing an update to the X2 models that would restore their features. But the authorities struck again, this time with malware that changed the lock passwords.[173] After attempting to protect itself from the attack, EncroChat shut down both its SIMs and its network. Over the course of the operation, law enforcement extracted a significant cache of data from EncroChat devices, including text messages and images. Over 800 people had been arrested as a result of the operation by the time of the announcement in July 2020.[174]

[168] *Walker Shaun, Kirchgaessner Stephanie, Lakhani Nina and Safi Michael (2021), Pegasus Project: spyware leak suggests lawyers and activists at risk across globe, The Guardian.*
[169] *Garrick Law (2020), Encrochat Encrypted Telephones Hacked June 2020 – Drugs, Telephones, NCA Police & Searches.*
[170] *Eurojust/Europol (2020), Le démantèlement d'un réseau crypté crée une onde de choc au sein des groupes criminels organisés à travers l'Europe.*
[171] *EncroChat website: https://encro.co.uk/*
[172] *Filippone Dominique (2020), Comment la Gendarmerie Nationale a fait tomber EncroChat, Le Monde Informatique.*
[173] *Cox Joseph (2020), How Police Secretly Took Over a Global Phone Network for Organized Crime, Motherboard – Vice News.*
[174] *Shaw Danny (2020), Hundreds arrested as crime chat network cracked, BBC News, and UK National Crime Agency (2020), NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation.*

13.c Wiretapping and log-in hacking

Targeted wiretapping has long been a technique used by law enforcement to monitor the communications of suspected criminals, and there appear to have been limited instances in the past few years where this has enabled authorities to access encrypted messages either from the device of origin or destination. There are no publicly-available instances where police were able to intercept end-to-end encrypted messages in transit. Nevertheless, police and secret services typically do not publish data or details on their methods or techniques, often citing reasons of national security.

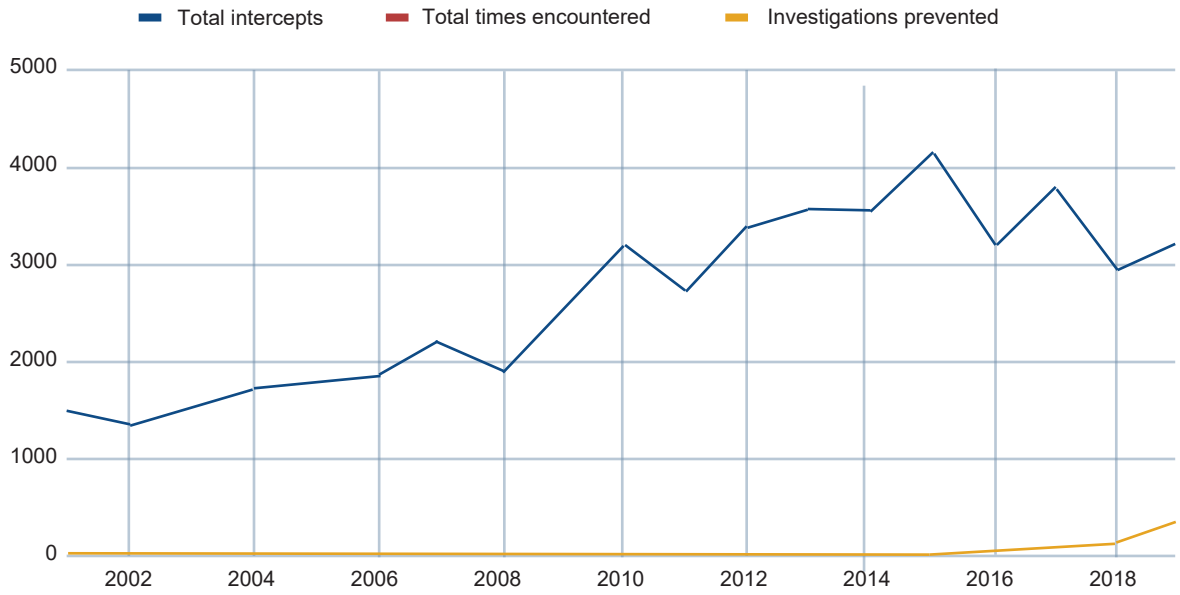
In Germany, the Federal Criminal Office (BKA) gained access to the encrypted Telegram accounts of members of the extreme far-right Old School Society in the summer of 2015. They were able to do so using telecommunications surveillance (TKÜ), after obtaining a judicial permit on the basis that they suspected that the group were plotting terrorist attacks. The method reportedly involved investigators registering their own devices in the account of the target suspect. Upon registration, Telegram sends a user's registered telephone number an SMS with an authentication code. The BKA were able to intercept this code using the TKÜ, thus gaining access to the suspect's Telegram account. They momentarily deregistered the original device so that the suspect received no notification of the new login. They were unable to access 'secret chats', however, which are device-specific, protected by secure E2EE, and include a self-destruction feature.[175] Both lawyers and politicians expressed doubts about the legality of the investigation, however, citing law § 100a, which permits cell phone monitoring only if the company offering the service has been shown a judge's order and then transmits the data to investigators.[176]

In the US, the judicial system releases metadata annually on the number of wiretaps it grants to law enforcement investigations, including statistics on the presence of encryption in those investigations. The data shows that encryption has been encountered much more frequently in the past few years, in line with a significant increase in the use of encrypted technologies by the general public. The data shows that in most, but not all, cases, encryption is reported by the justice system to have hindered law enforcement investigations when it is encountered. In 2019, for example, encryption prevented investigations in 334 of the 343 cases. But this figure represents just over 10% of the total wiretaps for that year: 3,225. The data includes domestic wiretaps by law enforcement, and not international wiretaps or those placed for the purpose of intelligence collection. The reports do not include further information on how law enforcement was able to bypass encryption in the relatively small number of instances where it did.

[175] Flade Florian (2016), „Dann knallen wir eine Moschee nach der anderen hoch", Welt.de; Lipp Sebastian and Hoppenstedt and Max (2016), Exklusiv: Wie das BKA Telegram-Accounts von Terrorverdächtigen knackt, Vice News; and Telegram –Secret chats: https://telegram.org/faq#secret-chats.
[176] Rebiger Simon (2016), Bundeskriminalamt knackt 44 Telegram-Accounts in zwei Jahren, Netzpolitik.

ENCOUNTERS WITH ENCRYPTION DURING US WIRETRAP INVESTIGATIONS

Source: US Courts Annual Wiretrap Reports, 2001-2019



13.d Europol's 16th Joint Referral Action Day – Joint operation with Telegram

Europol's European Internet Referral Unit engaged in its 16th joint referral action day in November 2019, focusing on countering terrorist propaganda online.[177] The operation targeted multiple platforms but the most affected was Telegram Messenger, on which Islamic State and other jihadist groups had found a safe haven for several years. The group and its supporters had moved to Telegram after being largely kicked off more mainstream apps like Facebook and Twitter in around 2015.[178] The operation was the most significant of its kind to date, hugely depleting jihadist networks on Telegram through widespread and persistent takedowns of channels, groups and accounts that had posted or engaged with violent Islamist content.

Europol and other European authorities declared the operation a success, with Belgium's Federal Prosecutor Eric van de Sypt announcing that Islamic State was "not present on the internet anymore".[179] But rather than removing the group from the Internet entirely, the operation scattered jihadist networks across the web and onto other, even more niche platforms. Principle among these was TamTam, a Russian messaging app. TamTam acted quickly, again largely removing accounts and channels associated with IS within around 24 hours. Nevertheless the group has since been experimenting with several other similar apps including but not limited to Hoop, Rocketchat, Threema, BCM, Riot (now Element) and Vkontakte. This has simultaneously made IS content harder for their supporters to find and more difficult for law enforcement agencies to monitor, as it is no longer found in one place.

[177] *"Europol and Telegram take on terrorist propaganda online", Press Release, Europol, 25 November 2019, available at: https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online*
[178] *David Gilbert, 'The Russian social network letting ISIS back online', Vice, 3 December 2019, available at: https://www.vice.com/en/article/d3ane7/islamic-state-cant-find-an-online-home-so-they-might-build-their-own-app*
[179] *Ibid.*

Tech Against Terrorism has observed a gradual re-establishment of IS-affiliated networks on Telegram over the past year. But unlike prior to the action day last November, most channels and groups on which propaganda is posted are private, rather than public. These are protected by client-server encryption, but not E2EE.[180] Access is possible only via unique join links, which are posted by violent Islamists in other Telegram channels and on third-party platforms, as well as on request from points of contact representing terrorist organisations or media outlets. This is almost certainly a tactic used to circumvent further content moderation by Telegram, who state on their website that "all Telegram chats and group chats are private amongst their participants", adding that they "do not process any requests related to them". Their position on takedown requests is that they only process those that are related to illegal content that has been posted in a public channel.

Telegram operation: a snapshot of online terrorist displacement and migration

The coordinated takedown of IS-related Telegram channels led to a temporary displacement of the IS and its supporters onto alternative messaging apps such as TamTam and Hoop Messenger by December 2019. Despite persistent attempts by IS networks to re-establish their presence on Telegram, they spent the following months experimenting with a number of alternative platforms. On 2 June Nashir News Agency, an official IS propaganda outlet, started to disseminate all official content on Hoop. By mid-June there were at least 70 IS-related groups on Hoop, each with between 500 and 1,500 users. The new presence was due to Hoop's failure to remove content based on Terms of Service violation referrals.

At the time of writing, IS networks were still attempting to maintain a persistent presence on Telegram whilst still dispersed across multiple platforms. They were no longer concentrated primarily on Telegram. The operation has had the dual effect of simultaneously making IS content more difficult for prospective terrorists to find reliably in one place, whilst also making it more difficult to monitor for law enforcement and researchers.

[180] *Telegram FAQs, available at: https://telegram.org/faq#q-how-secure-is-telegram*

tech against terrorism

PART 3

STRATEGIES FOR RISK MITIGATION

KEY FINDINGS

14. STRATEGIES FOR RISK MITIGATION

This part of the report investigates the different strategies for risk mitigation of terrorist and criminal use of encrypted messaging services, and what risks and concerns ought to be considered with regard to each.

1. User demand for online privacy has led to E2EE becoming the norm for online communication, with the vast majority of leading messaging services offering E2EE either as default or as an opt-in.
2. Policymakers globally are wary of criminal exploitation of E2EE, including by terrorist actors, and are pressuring E2EE service providers to implement technical solutions to counter illegal activity on their services.
    - Policymakers have, for example, called for providing law enforcement agencies with direct access to E2EE services to counter terrorism, and for E2EE providers to conduct systematic screening of content to detect child sexual abuse material.
3. It is technically impossible to create so-called backdoors to enable access to E2EE communication without creating security risks. In Tech Against Terrorism's view, the adverse security implications of backdoors would outweigh any possible positive impact that such measures would have on individual cases or investigations.
4. Screening tools to detect illegal content on E2EE services are also flawed. All technical tools for screening content shared on E2EE services:
    - Present significant security and privacy risks.
    - Raise questions related to jurisdictional and applicational scope.
    - Signal the possibility for systematic surveillance of private communication, without technically breaking encryption but by still defeating its privacy promise.
    - Would have a detrimental impact on the right to privacy, and potentially freedom of expression.
5. Homomorphic encryption would appear to be a less intrusive and less risky solutions for screening content on E2EE services. However the technology is not yet fully developed, and developing such solutions is expensive. Further, it presents security and privacy risks, raises jurisdictional questions, and breaches privacy.
6. User reporting is the easiest and less privacy-intrusive solution to moderate E2EE services. However, it entirely relies on users' willingness to report content.
7. Metadata analysis also offers a viable and less privacy-intrusive alternative to identify criminal use of E2EE services.
8. Law enforcement agencies and policymakers should focus on innovative investigative techniques and adapt to the evolving online space rather than call for counterproductive and risk-inducing regulations of E2EE. Targeted investigation techniques – including lawful hacking and targeted monitoring – are worth exploring, although they currently represent imperfect solutions.
9. At the cross-roads of lawful hacking and technical tools to monitor E2EE communications, the "ghost proposal" advanced by the UK GCHQ raises similar concerns to those of technical solutions to screen E2EE content.

15. COUNTERING CRIMINAL USE OF E2EE

The different strategies for mitigating risks of terrorist and criminal exploitation of encrypted messaging services, identified for this report, can broadly be divided into three categories:

- **Preventing criminal use:** Limiting the attractiveness of EMS for malevolent use, based on a risk assessment of the EMS. This includes introducing – or avoiding introducing – certain features which might make a platform more attractive to terrorists.
- **Identifying patterns of criminal use:** Identifying patterns of behaviours and uses of the services indicating terrorist and criminal activities on EMS. The main method identified in this regard is the use of metadata for behavioural analysis. Metadata can also be used to identify signs of association with or support for a terrorist organisation.
- **Disrupting criminal use:** Disrupting malevolent use of E2EE services, and encouraging innovative law enforcement investigation strategies whilst safeguarding encryption and its privacy promise. Key measures are user reporting mechanisms and targeted investigation techniques, notably lawful hacking and targeted monitoring, as well as technical tools for identifying illegal content shared on EMS. However, the latter present significant risks for online security and privacy.

16. PREVENTING CRIMINAL USE – EMS FEATURE ATTRIBUTES

E2EE offering does not in and of itself mean that terrorists and violent extremists will favour a platform instead of another. As we explained in Part 2 of this report, Criminal Use of E2EE – Terrorists and Violent Extremists Focused Assessment, terrorists and violent extremists consider four sets of characteristics when selecting an app or platform for exploitation: security, stability, audience reach, and usability.

Based on this framework, Tech Against Terrorism has identified features that increase the risk of E2EE messaging apps becoming attractive to malevolent actors. The table below outlines what these are and why platforms should either consider avoiding, or at the very least carefully consider introducing such features, due to the risks associated.

16.a Overview of features attractive to terrorist and violent extremist actors

Features	Characteristic	Uses and benefits for terrorists and violent extremists
Delete / Destruct message (including time delete)	**Security**	• This feature allows terrorists and violent extremists to leave limited digital evidence behind, as incriminating messages can be deleted without trace.
Private (password protected) chats	**Security**	• Any additional layer of security is potentially attractive to terrorists and violent extremists in their search to avoid unwanted monitoring of online communications. • Passwords can be used to protect access to one's conversation directly on the device (Wire, for instance, offers the possibility to password-protect conversations on its app), or to protect access to a group discussion by requiring users to enter a password to access it. • Password protected group chat, for instance an online forum, can significantly hinder the monitoring of terrorists and violent extremists' online chats, in particular if the sharing of the password is dependent on the user demonstrating ideological knowledge.
Invite-only groups	**Security**	• Similar to the password-protected group chats, invite-only groups can impede monitoring of terrorist and violent extremist groups on E2EE apps, in particular when invites are dependent on demonstrating one's ideological commitment to a particular group.
Secure file storage	**Security, stability**	• Terrorist or violent extremist actors use file storage to save material without risking content removal.
Sizable or unlimited file-size for sharing and storing	**Stability**	• Facilitates sharing of terrorist material, including large files (e.g. propaganda video, ideological guides, training material).
Proxy-servers / VPN via the app	**Security**	• Any feature that improves one's online security, including the possibility to conceal oneself is interesting for terrorist and violent extremist actors.[181]
Large group size	**Audience reach**	• Facilitates audience reach and terrorist in-group networking, organisation, and content dissemination.
Channels / public groups / broadcast list (especially if large audience capacity)	**Audience reach**	• These can offer significant audience reach to terrorists and violent extremists. Telegram's public and large capacity channels, for instance, are one reason why the platform is widely exploited by terrorist organisations.
Searchable groups / channels	**Audience reach**	• Facilitates the discovery of terrorist and violent extremist channels and chats. In particular if channels and chats can be searched directly within the app.[182] • It should be noted that even if an EMS does not offer a search function, join links (when available) can be aggregated in online directories searchable online via search engine.

[181] Online operational security (OPSEC) has been increasingly important for terrorists and violent extremists to ensure that their security and identity remain protected online. Several media outputs linked to terrorism and violent extremism illustrate this by their exclusive focus on providing supporters and members with OPSEC advice. This is the case of IS-linked Electronic Horizons Foundation and neo-Nazi OpSecGoy. These OPSEC bodies, and terrorist and violent extremist organisations in general, will recommend certain EMS to use to guarantee a user's online security. For more information about OPSEC recommendations and perception of E2EE platforms, please see Part 2 of this report: Criminal Use of E2EE: Terrorists And Violent Extremists Focused Assessment.
See: Gaudette Tiana, Scrivens Ryan, Venkatetsh Vivvek (2020), The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists, Terrorism and Political Violence; Bertram Luke (2016), Terrorism, the Internet and the Social Media Advantage, in Journal for Deradicalization, No. 7; Loedenthal Michael (2020a), "Evolving Digital OPSEC Practices Amongst Far-Right Networks", Global Network on Extremism and Technology; Loedenthal Michael (2020b), "Digital Resiliency and OPSEC Strategies Amongst Clandestine Networks", Global Network on Extremism and Technology; Conway Maura, Parker Jodie and Looney Sean (2017), "Online Jihadii Instructional Content: The Role of Magazines", in Terrorist Use of the Internet and Cyberspace: Issues and Responses, Conway et al. (Eds.), IOS press, pp.182-193.
[182] Including via keywords search function.

Features	Characteristic	Uses and benefits for terrorists and violent extremists
Shareable group join links	**Audience reach**	• Facilitates joining terrorist and violent extremist groups on E2EE apps.[183]
Open-source and/or decentralised model	**Stability**	• Open-source and decentralised technologies present adverse risks of terrorists and violent extremists developing their own version of an app and rendering it resistant to takedowns.[184]
Message forwarding	**Audience reach**	• Facilitates content "swarming" and other tactics deployed by terrorists to disseminate content online. • Complicates tracking of the original sender.[185]

[183] Even if an app does not explicitly offer this feature, there is the risk that users will creating indexes and lists of groups and share them online for anyone to join.
[184] A known case of such exploitation is Mastodon, a decentralised social network, that had its code forked by Gab against its creators' wishes. IS supporters are also known to have experimented with Mastodon's code.
See: Tech Against Terrorism (2019), Analysis: The use of open-source software by terrorists and violent extremists.
[185] In an attempt to limit the spread of misinformation online, Brazil and India have both seen discussion around the introduction of traceability requirements for online messaging apps, including those offering E2EE protection. Broadly, these legal provisions would require services providers to be able to trace back, and store messages log, for messages reaching a certain sharing threshold (messages shared more than X times, within a certain period.
See: Tech Against Terrorism (2021a), The Online Regulation Series Handbook.

METADATA ANALYSIS
17. IDENTIFYING PATTERNS OF CRIMINAL USE

Platforms using E2EE, whose content data is inaccessible to the service provider and thereby to third parties, can turn to metadata analysis for content moderation or cooperation with law enforcement, in particular to identify networks of criminal actors using the services. Metadata analysis is a better solution to that of "breaking" encryption as it provides insights to user activity whilst not presenting the security or privacy risks inherent in backdoors and the systematic screening of E2EE communications.

What is metadata?

Metadata is the bulk information relating to a users' information and communications behaviour[186] that usually contains descriptive information about other data.[187] This metadata, or non-content data, consists of "outside the envelope" information, such as sender and receiver identification, IP address, basic subscriber information, date, time, and location data.[188] Thus, this data is information that service providers can observe through the provisioning of services: when, how frequently, how long, and with whom users are communicating.[189]

Metadata and E2EE platforms

On end-to-end-encrypted platforms metadata can consist of:

- Personal data
- Account data
- Usage data

Examples are outlined below:

Personal data

First name, last name
Mobile number
Email address

Account data

Account name
Authentication information
Registration date
Contact information
Payment information

Usage data

IP address
Browser type and version
Activity on the service
Unique device identifiers and other diagnostic data

[186] *Schulz Wolfgang, and van Hoboken Joris (2016), Human Rights and Encryption, UNESCO Publishing.*
[187] *United Nations Office on Drugs and Crime – UNODC (2018), Privacy, investigative techniques and intelligence gathering.*
[188] *Woods Andrew (2017), Encryption Substitutes, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1705.*
[189] *Schulz and van Hoboken (2016).*

The text boxes above outline how various E2EE services often organise metadata collection. The types of metadata collected range from platform to platform and, while some collect more, others might collect the least amount to guarantee more anonymity or privacy to their users. However, it is important to note that platforms need to require a certain amount of information from their users in order to authenticate an account during registration or for certain features to operate during use of the service.

Figure 1. Word cloud based on an analysis of 25 platforms' privacy policies and terms of service, which range from messaging to video calling, social media, email services, search engines, and file hosting platforms, that use encryption. This word cloud demonstrates the type of metadata collected by platforms according to publicly available information, shedding light on the type of information that E2EE services request of their users.

17.a Benefits of metadata: behavioural analysis

Metadata can be revealing about an individual or an online network, and therefore valuable for identifying networks of malevolent actors. Whereas one piece of information or content can provide little information, one can acquire an in-depth understanding about an individual's activities through combining multiple pieces of information contained in metadata.[190] According to a 2016 UNESCO report on human rights and encryption, "it is possible to infer communication graphs as well as in-depth behavioural patterns from such data. Metadata can also be used to track people geographically and can interfere with their ability to communicate anonymously". As noted by a Berkman Klein Center report, metadata is generally not encrypted in ways that make it inaccessible for governments, and accordingly "provides an enormous amount of surveillance data that was unavailable before [internet communication technologies] became widespread".[191]

Case study: Malte Spitz and Deutsche Telekom

There are many studies that demonstrate how metadata can provide extremely detailed visualisations of people's lives. One such study was conducted when, in 2010, a German politician named Malte Spitz got access to all of the phone metadata that Deutsche Telekom had on him over a period of six months. Spitz, together with the German newspaper Die Zeit, created an interactive visualisation that let viewers track six months of his life entirely via his metadata combined with public information – such as his Twitter feed, blog entries and websites, all of which is freely available on the Internet.[192]

[190] UNODC (2018).
[191] Schulz and van Hoboken (2016).
[192] Masnick Mike (2013), Anyone Brushing Off NSA Surveillance Because It's 'Just Metadata' Doesn't Know What Metadata Is, TechDirt.

This data, especially in bulk, can be very valuable and may give insight into an individuals' behaviour as well as social relationships. An E2EE expert consulted by Tech Against Terrorism stated that they were perplexed by the amount of people who focus on encryption when there are so many other ways of gathering information for law enforcement purposes. The expert stressed that "metadata gives you everything you need to know" and that content is not as important as context (metadata), which supplies more information. The expert additionally emphasised that law enforcement is aware of the benefits of metadata over content.

17.b Using metadata to detect signs of association with a terrorist organisation

EMS: Scanning vs content moderation

As we saw in Part 1 of this report, the main challenge of detecting criminal use of EMS is that it is impossible for any external party to view the content of the communication once encrypted. However, the technical impossibility to moderate encrypted content does not mean that it is not possible to scan for suspicious behaviour on EMS. Metadata can be used by EMS to detect behavioural signs to identify terrorist networks exploiting E2EE services, in particular for strategic purposes (including propaganda and content dissemination).

Depending on the metadata collection practices of a given EMS, metadata can also be used to detect signs of association with or support for terrorist organisations. Profile photos and usernames can be scanned to detect for visuals and terms usually associated with or used by terrorist groups. However, in tandem with such metadata scanning the consideration of context is essential in order to ensure that users are indeed demonstrating support for a terrorist actor or group.

In consultation with experts and informed by open-source intelligence research, Tech Against Terrorism has identified different behavioural indicators that can be used to identify terrorist actors during their user journey on an EMS. These behaviours do not require insights into content. Rather, one has to look at the context of the communications to inform behavioural network analysis.

1. ACCOUNT CREATION

Account information: Names or usernames, and user profiles (incl. status and photos) can be scanned for keywords and visuals indicating links to terrorist and violent extremist groups.

Join groups behaviour: User joins or creates an unusual number of group chats, channels, or broadcast lists.

2. RECEIVING BEHAVIOUR

Forward: User forwards received messages in-between chats, in particular group chats.

Passive reception: User has little to no reactivity to messages received (except forwarding).

3. SENDING BEHAVIOUR

Mass send out: Messages sent out simultaneously across group chats, channels and broadcast lists.

Non-text content: Frequent sharing of non-text content, including audio, images, and outlinks.

4. GROUPS & BROADCAST LISTS

Size and members:
- Large group size.
- Members across the world.
- Members do not have each other as address book contacts.

Broadcast behaviour:
- Only a handful of users, group administrators, share messages or content.
- Little to no interactions between group members.

Mirror groups and broadcast lists:
- Multiple versions of the same groups or lists, with the same administrators and members.
- Similar group names or images.
- Similar patterns of interaction across groups
- Messages forwarded in-between groups.

17.c Law enforcement and metadata

One possibility for law enforcement to gather intelligence without breaking encryption is thus the use of metadata.[193] According to Andrew Keane Woods in his paper on Encryption Substitutes: "[metadata] information is often as valuable or more so for law enforcement than content data".[194]

It may also be more accessible: Woods notes that "[US] Search-and-seizure law - in the form of the 4th amendment doctrine, the Omnibus crime Control and Safe Streets Act, and the Electronic Communications Privacy Act - draws a sharp distinction between content and non-content data, typically providing fewer legal barriers to law enforcement attempts to access metadata".[195] Woods also argues that given sufficient metadata, law enforcement can gather and infer "enormously useful information", such as who a subject was communicating with, about what, where, and when – "much of the most important information for conducting criminal investigations".[196]

Certain E2EE messaging apps already rely on metadata sharing when it comes to cooperation with law enforcement:

- **WhatsApp** only hands over metadata to law enforcement upon receipt and approval of a law enforcement request.[197] According to US court documents,[198] the most common kind of request ordered WhatsApp to install a pen register device which provide metadata to law enforcement for their investigations.[199]
- **Threema's** transparency reports provide insights into how E2EE apps can collaborate with law enforcement. By listing the different information, all metadata-related, they can provide upon receiving a user information request.[200]

Year	Requests by Swiss authorities	Requests by foreign authorities with Swiss legal assistance	Requests that have met the formal requirements	Requests that didn't meet the formal requirements	Handing over of data (# cases)	Handing over of data (# IDs)
2021	48 (*)		46	2	44	281
2020	105 (*)		104	1	98	558
2019	101 (*)		98	3	93	317
2018	28 (*)		25	3	25	69
2017	2	2	4	–	3	12
2016	–	1	1	–	1	1
2015	1	–	–	1	–	–
2014	–	–	–	–	–	–

* Since the new BÜPF act has come into force on March 1, 2018, Threema can no longer distinguish between requests by Swiss authorities and requests by foreign authorities with Swiss legal assistance.

Last update: 2021-07-05

Figure 2: Screenshot of Threema's transparency reports indicating the number of information requests received since 2014

[193] *A 2017 report by the Center for Strategic & International studies on the effect of encryption on lawful access to communications and data highlights that "other capabilities can also help law enforcement agencies, such as tools to analyse metadata", and that, "as more devices are connected to the Internet, the amount of data generated by individuals will grow, offering greater opportunities to establish patterns of behavior". See: Lewis James A., Zheng Denise E., Carter William A. (2017), The Effect of Encryption on Lawful Access to Communications and Data, Center for Strategic and International Studies.*
[194] *Woods (2017).*
[195] *Woods (2017).*
[196] *Woods (2017).*
[197] *Ong Thuy (2017), WhatsApp reportedly refused to build a backdoor for the UK government, The Verge.*
[198] *https://www.documentcloud.org/public/search/projectid:31263-WhatsApp-data-requests*
[199] *Brewster Thomas (2017), Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops, Forbes.*
[200] *https://threema.ch/en/transparencyreport*

17.d Terrorists' acknowledgement of the availability of metadata

Most metadata is not protected by end-to-end encryption. By using E2EE services, a user protects the content of their communications but allows their communications metadata to remain available to service providers, and to third parties such as law enforcement.[201] Terrorists are aware of this. According to the Combating Terrorism Center at West Point, "a survey of terrorist publications and details that have emerged from interrogations suggest that terrorists are at least as concerned about hiding metadata as they are about encrypting communications". However, various apps and services are compelled to obtain and even store certain metadata in order to operate. The extent and types of metadata available range between platforms depending on their privacy policies – See Table B: Unencrypted metadata available on E2EE platforms and their information sharing with third parties including law enforcement.[202]

17.e The limits of metadata analysis

E-evidence and proving intent

A 2017 report on the effect of encryption on lawful access to communications and data, by the Center for Strategic & International studies, recognises a notable caveat to metadata analysis: "While metadata is useful, it cannot fully replace the content of communications as evidence. For example, it can show that two people communicated around the time of an incident, but it cannot show what they said, which is critical to proving intent".[203] Whilst metadata can play an important role in identifying criminal networks online, its use in a judicial court might be limited.

Metadata and the right to privacy online

It is important to note that The Office of the United Nations High Commissioner for Human Rights (OHCHR) states that metadata should be covered by the right to privacy when applied to the online space:

> The protection of the right to privacy is broad, extending not only to the substantive information contained in communications but equally to metadata as, when analysed and aggregated, such data "may give an insight into an individual's behaviour, social relationship, private preference and identity that go beyond event that conveyed by accessing the content of a communication". [204]
> See: A/HRC/27/37

This means that though metadata is more accessible, and its use for moderation or law enforcement purposes does not "break encryption" (making it considerably less privacy-intrusive than screening encrypted communications), the use of metadata should still be considered in light of its potential impact on users' right to privacy.

[201] *Schulz and Hoboken (2016).*
[202] *Graham Robert (2016), How Terrorists Use Encryption, CTC Sentinel.*
[203] *Lewis, Zheng, and Carter (2017).*
[204] *United Nations, Office of the High Commissioner for Human Rights (2018) The Right to Privacy in the Digital Age.*

EU ePrivacy Rules

In February 2021, the Council of the EU approved a new draft regulation regarding the privacy of electronic communications, the EU ePrivacy Rules.[205] The regulation reasserts that metadata falls under the scope of the fundamental right to privacy, and in doing so significantly limits how and why services providers can analyse metadata. According to the draft regulation, all electronic communications and related metadata for end users located in the EU[206] are to be protected from external interference.

In practice, this means that services providers are no longer allowed to analyse metadata collected on their services. This risks having major implications for how E2EE services providers can detect criminal use of their platforms, as they are no longer allowed to monitor and process metadata for behavioural analysis.

The regulation notes exemptions to the non-interference principle, and allows for the processing of electronic communications data without user consent for certain purposes, including, amongst others "cases where the service provider is bound by EU or member states' law for the prosecution of criminal offences or prevention of threats to public security." However, at the time of writing,[207] it is unclear how these exemptions work in practice, and whether service providers can conduct metadata analysis to detect terrorist and violent extremist use of their services.[208] Thus, platforms should be wary of the new EU ePrivacy rules' implications on metadata privacy, though there are relevant exemptions which can apply to platforms assisting in law enforcement investigations.

With metadata analysis representing the less intrusive technique to detect terrorist use of E2EE, and the only one that does not break E2EE nor its promise of private communications (See 18.b E2EE and proactive screening of content, on the risks associated with the pro-active screening of content), it is essential that service providers have clarity on whether they can use such techniques without violating the EU ePrivacy rules.

Limited collection by services providers

In an attempt to guarantee user's privacy, certain platforms will give their users the option of which metadata they would like to provide (unless it is necessary for account authentication or other services), and will limit the amount of data they store on their services. In general, metadata collection varies depending on the platform's stated privacy orientation, but also on how users typically interact with content and with each other.[209] For example, if a platform presents itself as primarily aimed at online privacy, it typically asks for as little information as possible from their users and stores little to none of what it collects, and therefore ultimately retains a minimal stock of metadata.

[205] *To read more about the draft regulation, see: Council of the EU (2021), Confidentiality of electronic communications: Council agrees its position on ePrivacy rules.*
[206] *Including cases where the processing takes place outside the EU or the service provider is established or located outside the EU.*
[207] *August 2021.*
[208] *In prevision of the rules being adopted, the EU Commission proposed a temporary derogation to the new regulation for the purpose of combatting child sexual abuse online, which will allow platforms to continue with voluntary mechanisms to detect CSAM. This derogation was approved by the European Parliament in July 2021. However, no similar derogation has been proposed for countering terrorist use of the internet, and no specifications have been provided regarding how exemptions listed in the rules can be operationalised.*
[209] *Cambridge Consultants for OfCom (2019), Use of AI in Online Content Moderation,*

Many platforms are aware and conscious of whether their users value privacy and anonymity. Though many of the platforms listed in the table below collect various types of metadata on their users, some platforms try to avoid giving any information to law enforcement. Techniques that platforms use include storing as little metadata information on their services as possible, so that they cannot surrender the data requested by law enforcement. For instance, some platforms will limit metadata collection to what is absolutely necessary in order for the service to authenticate a user's account and to function, and make it optional to supply any other information.

Threema: limited metadata collection

"Threema GmbH is not required to store communication metadata ("data retention"), as it does not exceed the revenue limits set by the Federal Act on the Surveillance of Post and Telecommunications (BÜPF) (version in effect since 01.03.2018) and the accompanying decree VÜPF. However, Threema GmbH must provide information that it already has upon judicial order. Therefore, **we make a point of processing and storing as little information about our users as possible**."[210]

"If the legal requirements are fully met, we can provide the following information associated with a given Threema ID:"

- Hash of phone number, **if provided by the user**
- Hash of email address, **if provided by the user**
- Push token, if a push service is used
- Public key
- Date (without time) of Threema ID creation
- Date (without time) of last login

17.f. Metadata and human rights

As the OHCHR has noted, metadata should be covered by the right to privacy when applied to the online space.[211] This is particularly important when considering how such metadata could be used maliciously, whether by individuals or governments, particularly non-democratic ones.

United Kingdom & metadata

This issue of government collection of metadata has recently been addressed by the Grand Chamber of the European Court of Human Rights.[212] On 25 May 2021, a Grand Chamber judgment against the UK set new boundaries in the regulation of bulk interception capabilities requiring enhanced safeguards to protect the rights to privacy and freedom of expression.[213] The Grand Chamber of the European Court of Human Rights ruled that the UK government's historical mass interception program, which involves the interception of both content and metadata, violates the rights to privacy and freedom of expression.[214]

[210] https://threema.ch/en/transparencyreport
[211] See "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights": https://undocs.org/A/HRC/39/29
[212] See "CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM": https://hudoc.echr.coe.int/eng#{"itemid":["001-210077"]}
[213] Privacy International (May 2021), "UK mass interception laws violates human rights and the fight continues...". https://www.privacyinternational.org/long-read/4526/uk-mass-interception-laws-violates-human-rights-and-fight-continues
[214] Privacy International (May 2021), "UK mass interception laws violates human rights and the fight continues...". https://www.privacyinternational.org/long-read/4526/uk-mass-interception-laws-violates-human-rights-and-fight-continues

In relation to metadata collection, the Court rejected the UK government's claim that "the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content." It ruled "that the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content."[215]

It was established that the UK government lacks safeguards on bulk interception, and therefore the Court found the mass interception of communications data to violate Article 8 ECHR[216], which enforces the right to respect for private and family life.[217]

ARTICLE 8
Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[218]

Russia & metadata

In Russia in 2016, a new set of online regulation laws, the "Yarovaya amendments"[219], required telecom providers, social media platforms, and messaging services to allow the Federal Security Service of the Russian Federation access to users' metadata and encrypted communications. According to the Brookings Institution, "while there is little known information on how Russian intelligence agencies are using these data, their very collection is an opportunity for intimidation and harassment of private companies and civil society organizations".[220] The Brookings Institution highlights that civil society groups and independent media have been the primary targets of legal surveillance, repression, and censorship.[221]

Global implications on human rights

Governments, including of non-democratic countries, can thus use the collection of metadata in bulk at the expense of users' privacy rights. The collection of metadata in bulk, thus, risks major abuses by governments. Democratic countries should be conscious of the potential influence of their own collection and safeguards of such data and consider how this could be used as a template in non-democratic countries – with the risks this poses to privacy rights.

[215] *Privacy International (May 2021), "UK mass interception laws violates human rights and the fight continues...". https://www.privacyinternational.org/long-read/4526/uk-mass-interception-laws-violates-human-rights-and-fight-continues*
[216] *Privacy International (May 2021), "UK mass interception laws violates human rights and the fight continues...". https://www.privacyinternational.org/long-read/4526/uk-mass-interception-laws-violates-human-rights-and-fight-continues*
[217] *See: "Guide on Article 8 of the European Convention on Human Rights": https://www.echr.coe.int/documents/guide_art_8_eng.pdf*
[218] *https://www.echr.coe.int/documents/convention_eng.pdf*
[219] *https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship*
[220] *Meserole and Polyakova (2019) "Exporting Digital Authoritarianism". The Brookings Institution. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf*
[221] *Meserole and Polyakova (2019) "Exporting Digital Authoritarianism". The Brookings Institution. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf*

Unencrypted metadata available on E2EE platforms and their information sharing with third parties including law enforcement

Legend

Automatically collected metadata
Option user provided data collected

	Metadata collection							Use of metadata to detect and counter illegal activities	
	Name or username	Phone Number	IP address	Email address	User Activity on service	Device Information	Other Metadata/ or optional metadata collected	Use of metadata to detect to detect illegal activities	Information sharing with Third party including LE
Telegram[222]	Username		✓			✓	History of username changes		✓
WhatsApp	Profile name	✓	✓		✓	✓	"About" information; registration date; profile photo; location information; log files and diagnostic, crash, website, and performance logs and reports; features the users use; group name, group picture, group description; payments or business features; profile photo; how users interact with others using our Services, and the time, frequency, and duration of their activities and interactions, payment and transaction information (if used)	✓ Monitoring of unencrypted information to detect CSA material, including PhotoDNA to scan profile photos.[223]	✓
Hoop Messenger	Full name and username	✓	✓		✓	✓			✓
Signal		✓					Technical information: including randomly generated authentication tokens, keys, push tokens, and other material that is necessary to establish calls and transmit messages.		✓
Line	LINE ID (if provided)	✓					Contact Phone Numbers in Address Book (optional), Location Information (optional)		✓
Threema	Threema ID, Nickname (if provided)	✓		✓		✓	Registration date, public key, operating system and version of the Threema app, date of the last login		✓ Small transparency report:[224]
Wire Personal	Name	✓		✓		✓	Log files		✓ Transparency report

[222] *Not enough publicly available information, only provides limited examples, including: IP address, device information, and history of username changes.*
[223] https://faq.whatsapp.com/general/how-whatsapp-helps-fight-child-exploitation/?lang=fb
[224] https://threema.ch/en/transparencyreport

	Metadata collection							Use of metadata to detect and counter illegal activities	
	Name or username	Phone Number	IP address	Email address	User Activity on service	Device Information	Other Metadata/ or optional metadata collected	Use of metadata to detect to detect illegal activities	Information sharing with Third party including LE
Wickr	Wickr ID					✓	Crash logs, aggregate usage data. Optional User-Provided Information, such as push notifications, avatar, ID connection, invitations, contact finder, encrypted cloud data, and key verification		✓
Element/ Riot	Username, display name (if provided)	✓	✓	✓					✓
FortKnoxster		✓		✓			Number of messages sent, storage space user, country code login		✗ ✓ "Any authority must direct a request to the relevant authorities, which may then possibly contact us, following the protocol that the relevant legislation stipulates. We will not comply with demands from any authorities to a higher extent than the law demands."
Session	No metadata collection: "Session doesn't store, track, or log your messaging metadata. IP address protection: Device IP addresses are never exposed to the person you're talking to or the servers holding your data. Users don't need a phone number, e-mail, or any information tied to user real identity to make a Session account."								✓ Small Transparency report. [225]

[225] https://loki.foundation/transparency/

	Metadata collection							Use of metadata to detect and counter illegal activities	
	Name or username	Phone Number	IP address	Email address	User Activity on service	Device Information	Other Metadata/ or optional metadata collected	Use of metadata to detect to detect illegal activities	Information sharing with Third party including LE
Viber	Name	✓		✓	✓		Registration date; date of birth; Billing information when necessary, the value added services users are using over Viber and/or apps (such as games) they have downloaded through Viber. Interaction with other users such as who called who and who messaged who and at what time. information about the messages users have liked, comments left and websites viewed through links in them or otherwise links viewed from within Viber.	✓ "We may use your information to prevent, detect, and investigate fraud, security breaches, potentially prohibited or illegal activities, protect our trademarks and enforce our Terms of Use."[226]	✓

[226] https://www.viber.com/en/terms/viber-privacy-policy/#uses-and-retention

18. DISRUPTING CRIMINAL USE – TECHNICAL TOOLS TO DETECT ILLEGAL CONTENT

Contrary to what certain policymakers have been arguing when calling for backdoors to encryption and warning tech companies about the risks of criminal actors exploiting E2EE services, content moderation is not "fundamentally incompatible with end-to-end encrypted messaging".[227] As Jonathan Mayer, a lawyer and computer scientist at Princeton University, has argued in a landmark article on the topic, certain tools and processes for content moderation "may be compatible" with E2EE.[228] Or, at least, technically compatible with E2EE in the sense that they neither systematically break the technical protection offered by encryption nor create permanent backdoors to E2EE. However, as we will see below, most of the technical tools proposed to moderate E2EE content do violate the promise of privacy inherent to E2EE.

Proactive vs. reactive content moderation

Two content moderation strategies are usually available to tech companies: reactive and proactive measures. Platforms can either act following a user report, or other flagging mechanisms, or they can actively screen content uploaded or shared on their services to identify and remove material, and in certain instances prevent the upload of content altogether.

For an overview of content moderation techniques used by E2EE messaging apps, see Section 6, E2EE Challenges for Content Moderation, of Part 1, Use and Perception of E2EE: Landscape Review.

18.a Reactive content-moderation and E2EE

User reporting is the content moderation mechanism the most compatible with E2EE due to its very limited impact on user privacy and the ease with which it can be implemented – an email address to report abuse suffices.

Most E2EE messaging apps already offer users the possibility to report abuse. The table below reviews the different user reporting solutions that are compatible with E2EE and which messaging apps have implemented them already.

[227] *Mayer Jonathan (2019), Content Moderation for End-to-End Encrypted Messaging, Princeton University.*
[228] *Mayer (2019)*

User reporting mechanism	Platforms known to implement it	Characteristics	Feasibility	Limitations
Direct user reporting via the app	• Facebook Messenger (using message franking) • WhatsApp • Line • Snapchat • Rocket.Chat	The most recent messages shared in the reported conversation are forwarded to the app's Trust & Safety team. Depending on the app, the content of the last messages are either decrypted prior to being shared with the Trust & Safety team, or after sharing (in which cases an encryption key is attached to the user report). Technical tools: • Message franking (metadata required) • Asymmetric message franking (no metadata) • On device decryption prior to sending	Already implemented by major messaging apps offering E2EE.	• Cannot verify the identity of the sender (of the reported message).
Indirect user reporting via email	• Viber • Wickr • iMessage • Hoop Messenger • Telegram	Users can email the service provider to report abuse. Such emails can include screenshots from the conversation as evidence of the abuse (as recommended by iMessage)	Already implemented by major messaging apps offering E2EE.	• Possible friction in the process due to the sending a separate email rather than directly reporting within the app, which might lead to insufficient reporting by users. • Cannot verify the identity of the sender (of the reported message).

User reporting: limitations

Whilst there are clear benefits to user reporting, mainly due to the limited impact on user privacy, content moderation strategies solely based on user reporting present limitations in terms of detecting and preventing the dissemination of illegal content online. Whilst relying entirely on the recipient's willingness to report content works for unwanted messages, or for the accidental discovery of illegal content, user reporting is unlikely to significantly prevent the spread of illegal and harmful content online when such content is consensually received or sought out.

If we take the case of a terrorist group disseminating material and propaganda to its supporters via a E2EE messaging app, or of any other criminal network using such a platform to organise its members or adherents, we can assume than most participants have willingly joined the conversation and are unlikely to report any illegal content they see.

18.b E2EE and proactive screening of content

As we saw in Part 1 of this report, there is no safe backdoor to encryption.[229] The below review of technical tools thus focuses on the existing and proposed tools to screen E2EE communications content to identify illegal content and prevent it from being shared.

[229] *Backdoors are technically impossible without breaking end-to-end encryption, and creating significant security risks*

Technology type	Technical tool	Description	Limitations
Hashing & screening – This screening and matching of content is hash-based (PhotoDNA). Image and audio content shared along text messages via an E2EE application is screened to verify whether there is a match with known illegal content (database of hashes). All hashing and screening is done prior to the message and attached content being sent to the recipient(s). If a match occurs during the screening process, the message and content flagged are sent to the service providers' moderation team for review and the transmission to the intended recipient(s) is blocked altogether. In short, the communication and sharing of content can be disrupted before reaching the intended recipient(s).	**On-device hashing and detection**	• Images and videos are hashed on the device, the hash is then screened to see if there is a match with a hash database of known illegal content. • All hashing and matching is to be done on device prior to the content being encrypted and sent to the recipient. • If there is a match with known illegal content, the content is sent to the moderation team for review and the transmission to the recipient is blocked.	• Requires large amounts of storage to function. • Limited to content already included in the hash database to function. • Limited to images and video content.
	On-device hashing with detection on servers	• Audio and images are hashed on the device, then sent to the service provider's servers alongside the encrypted message for screening and matching against a hash database. • Screening and matching can be done by third-party servers, which would then forward matched content to the platform's moderation team. This could be done by a single or multiple third parties to limit the risks of servers being compromised (the sheer number of servers would frustrate unauthorised access).	
Classifiers and AI – Content is screened on device prior to being encrypted and transmitted to its intended recipient(s). Classifiers and AI algorithms based on database of known illegal content are used to screen the content and assess whether it is illegal. If deemed illegal, the message and content are sent to the service provider's moderation team for review and the transmission to the intended recipient(s) is blocked altogether. Similarly to hashing and screening, this means that communication and sharing of content can be disrupted before reaching the intended recipient(s).	**On-device classifiers**	• Classifiers, coupled with machine-learning to detect illegal content. • Classifiers are integrated on the sender's device to assess whether content should be reported to the moderation team. • This would work for both known and unknown content: Classifiers would allow for screening and matching against a database of known illegal content, but could also be used to identify new illegal content not yet included in a database.	• Classifiers need to be fed constantly with new data to stay up-to-date and identify new content. • Machine learning has shortcomings, including significant error rates. • Image classifiers are already in use by tech platforms, but significant development is still required.[230]
	On-device AI moderation	• An AI model would be used to screen all messages and content prior to sending. • Screening would be based on the platform's community guidelines. • Violating content would be prevented from sending.	• Depending on the protocol in place, content would not be transferred to the service provider's moderation team, which would remain blind to what the violation is.

[230] *EU Commission (2020a), Leaked report on technical solutions to detect child sexual abuse in end-to-end encrypted communications.*

Technology type	Technical tool	Description	Limitations
Trusted environments and homomorphic encryption – Messages and attached content are encrypted prior to being screened to determine whether there is a match with known illegal content. Depending on the tool used, content will either be screened when encrypted or following decryption. As for the other tools, content is screened before being transmitted to the recipient(s). This means that communication and sharing of content can be disrupted before reaching its intended recipient(s).	**Secure enclaves** – Also known as "Trusted execution environments" and "trust platforms module".	• Encrypted messages are sent to "secure" cloud servers, before being decrypted and screened for illegal content on those servers. • Depending on the results of the checks, content is either sent to the moderation team or re-encrypted and forwarded to the recipient • The technology needed is still being develop, however similar systems are already in use.[231] • Secure enclaves could either be located on the service provider's servers, or hosted by third parties. • For smaller platforms, the third party conducting the screening within a secure enclave could be a larger platform with the resources needed to access and deploy this technology.	• Only technical tool that involves encrypting then decrypting content. • Complex technology that most tech companies do not have access to.
	Homomorphic encryption	• Greg Gentry, the creator of homomorphic encryption has compared it to a "glovebox", that anyone can access and manipulate from the inside, without being able to take anything out • Homomorphic encryption allows for the computation of encrypted content without having to decrypt it. • Content – messages and attached files – would be encrypted on the device, and then sent to the platform's servers for screening and matching. • Hashes are then computed from the already encrypted content and are verified against database of known illegal content for screening. • If there is a match, the content flagged is sent to the moderation team for review and sending to the recipient is blocked.	• Limited to images (too heavy for video hashing) • Similar concerns and risks than for other solutions relying on hashing techniques. • Technology is still in its early day, in particular for full homomorphic encryption.[232] • Expensive technology to develop and unlikely to be available to smaller platforms in the first instance

[231] *EU Commission (2020a), Leaked report on technical solutions to detect child sexual abuse in end-to-end encrypted communications.*
[232] *Meaning that multiple operations can be supported an unlimited number of time.*

Risks associated with the pro-active screening of E2EE content

All of the technical tools reviewed in the above table present security and privacy flaws which ultimately defeats the "fundamental" promise of encryption: "the promise that no one but you and your intended recipients can read your messages or otherwise analyse their contents to infer what you are talking about". They also present significant security risks and raise important questions regarding the potential scope and jurisdiction of application.

In general, Tech Against Terrorism warns against the roll-out of such screening techniques, and against government legally mandating, or otherwise urging,[232] tech companies to implement them.

Bypassing the encryption debate altogether?

Scanning all pieces of content to search for illegal material without having to create a backdoor access to the E2EE protocol seems to be the ideal compromise to the so-called encryption debate. However, these technical tools for screening content prior to sending not only violate privacy, but they also bypass the encryption debate altogether and send an important signal to governments about this.[235]

Rather than answering policymakers' call to backdoor access for law enforcement, the development of such tools signals that backdoor access is not necessary, and that the screening of the content of E2EE communication can be conducted despite encryption. This could open the door to systematic screening of private communication channels.

The possibility to conduct client-side scanning in order to bypass the impossibility to screen encrypted content is also hinted at in the amended EARNT IT Act, introduced to US Congress in March 2020. Whilst the amended act prohibits holding companies liable for offering E2EE, the Electronic Frontier Foundation has criticised it for "encourage[ing] lawmakers to look for loopholes […[such as demanding that messages be scanned on a local device before they get encrypted and sent along to their recipient." [236]

Technical "solutions"

Technical tools to screen E2EE communications for illegal content are often presented by policy-makers as "technical solutions". This is the case of the EU Commission using the denomination of "technical solutions" to title its review of technical tools to screen E2EE protected content.[237] Such language is misleading in implying that it offers a solution to detect illegal content on E2EE services, when they do not provide a solution for moderating content without breaking encryption nor its promise of privacy.

[233] *Portnoy Erica (2019), Why adding client-side scanning breaks end-to-end encryption, The Electronic Frontier Foundation.*
[234] *For instance by listing such tools a best practice to follow in order for a platform to not be held liable for user-generated content.*
[235] *Leetaru Kalev (2019a), Facebook is already working towards Germany's End-to-End Encryption Backdoor Vision, Forbes.*
[236] *Mullin Joe (2020), The New EARN IT Bill Still Threatens Encryption and Free Speech, Electronic Fronter Foundation.*
[237]

Security risks

● *Compromised database and reverse engineering:* Risks the matching technology, or the database itself, being tampered with. This means that the technology could be modified to not detect certain content, or on the contrary to introduce false positives.

● *Leaked detection tools:* The hashing and detection algorithms risk being hacked or leaked, thus reducing the effectiveness of other detection tools. Technical experts have raised concerns about the adverse risks it would pose if a malevolent party were to obtain access to the technologies powering the moderation of encrypted discussions.[238]

● *Access to unencrypted data:* The "secure server enclaves" proposal further presents the risk of malevolent actors gaining access to the server, hence, to decrypted data. This would fully defeat the purpose of encryption entirely.

● *Adversarial use of classifiers:* Malevolent actors gaining access to classifiers could use the database to reverse search similar content on the web.

Defeating privacy

● *Privacy vulnerabilities:* By introducing a third party in the transmission chain (anyone who is not the sender nor the intended recipient), all technical tools reviewed bar the on-device ones create privacy vulnerabilities by exposing the users' conversations. These vulnerabilities ensue from the different security risks presented above, as users' data (even if hashed) is available to either the ISP or a third-party.

● *Any vulnerability is a security risk:* As we saw in Part 1 of this report, Use and Perception of E2EE - Landscape Review, E2EE is only as strong as its weakest point. The introduction of any privacy vulnerabilities entails its potential exploitation by malevolent actors, including by terrorists and violent extremists, or hostile state actors.[239]

● *Breaking the privacy promise:* All on-servers screening tools imply that the content screened, or its hash, will be known by the servers. This defeats the purpose of encryption by revealing the content of a private communication and breaking the users' expectation for privacy.[240] This is all the more important if flagged content is shared with a human reviewer.[241]

Long-term perspective

● *Mass surveillance:* The roll-out of systematic screening of E2EE content, or the mandating of backdoors access, would also signal the possibility of screening all content shared in private communication channels, including legal and non-extremist content: "What happens as governments themselves awaken to the idea of pre-emptively stopping all private communications they dislike?"[242] This could lead to governments legally requiring systematic monitoring of E2EE, either via backdoors or screening of content, for censorship. A long-term security vision is required both in the interest of national security, and for the protection of citizens from their own governments.[243]

[238] *Internet Society and the Global Encryption Coalition (2020), Breaking encryption myths What the European Commission's leaked report got wrong about online security. For more information about the EARNT IT Act, please see Part 1 of this report, Use and Perception of E2EE – Landscape Review.*
[239] *Internet Society and the Global Encryption Coalition (2020).*
[240] *Internet Society and the Global Encryption Coalition (2020), Breaking encryption myths What the European Commission's leaked report got wrong about online security.*
[241] *Internet Society and the Global Encryption Coalition (2020).*
[242] *Leetaru (2019a)*
[243] *It is worth noting that the creation of a digital database of citizens' biometric data in France has been criticised on similar grounds by the Commission Nationale de L'informatique et des Libertés (National Commission on Computer Technology and Freedom) and the Conseil National du Numérique (National Digital Council), which argued that the rise of populism in Europe make "these bets on the future unreasonable" regarding the end use of the database. Similarly, we cannot be guaranteed that in the future a government won't employ its access to E2EE for purposes beyond those stated at the time of the legislation being passed.*
Untersinger Martin, (2016), Que reproche-t-on au TES, le "mégafichier" des 60 Millions de Français ?, Le Monde.

● *Abuse by non-democratic countries:* Privacy advocates have long warned about the risk of a backdoor or ban on encryption introduced in a democratic country being replicated by authoritarian governments.[244] Similar concerns can be raised with regard to the introduction of pre-encryption screening which could be abused by non-democratic governments to monitor political dissent and minority groups.
● *Built-in device screening of content*: One could also imagine a situation where device manufacturers start building their own screening technologies to automatically screen all content hosted on one's device.[245] As well as such technologies becoming a legal requirement, thus creating a regime of mass surveillance and fully burying all expectations of online privacy. This could have a significant impact on freedom of expression, with users refraining from communicating if they fear their conversations are monitored.[246]

Jurisdiction
● *Who is in charge?:* Whether it is an on-device or on-server matching, all technical tools raise the question of who is to decide on content to be included in the hashing or classifier list. In other words, who is to decide what constitutes illegal or harmful content? The answer depends on the aim of the screening (e.g. identifying CSAM or terrorist and violent extremist content, or reviewing content based on an ISP's community guidelines):

- Whereas CSA is illegal in most, if not all countries, and the majority of tech companies are already taking action against it, a global agreement on what constitutes illegal content otherwise, in particular for terrorist content, is a complicated question.
- Criticisms levelled against the Global Internet Forum to Counter Terrorism's hash-sharing database for terrorist content illuminate the likely forms of reproach if the screening of E2EE content was to become the norm for moderating E2EE. The database has been criticised for the lack of transparency surrounding its use – including what content is added to the database – and the content removal that it contributes to.[247]
- The EU Commission itself, in its Leaked report on technical solutions to detect child sexual abuse in end-to-end encrypted communications, underlines that all "solutions" it reviews in the report would lack transparency. According to the report, this is partly due to the need of ensuring the security of the matching system precluding transparency oversight.[248]

[244] *Less democratic governments already copy mechanisms for the online regulation of online speech and content created and implemented in Western democracies. See: Tech Against Terrorism (2021a).*
A similar risk applies to platforms themselves, especially those that are particularly concerned with user privacy. Telegram, for example, is currently based in Dubai, but states on its website that it is "ready to relocate again if local regulations change". See: https://telegram.org/faq
[245] *Leetaru Kalev (2019b), The Encryption Debate Is Over - Dead At The Hands Of Facebook, Forbes.*
[246] *Ibid*
[247] *See: Tech Against Terrorism (2021a); Windwehr Svea and York Jillian (2020), One Database To Rule Them All, Vox-Pol; Radsch Courtney (2020), GIFCT: Possibly the Most Important Acronym You've Never Heard Of, JustSecurity; Diaz Angel (2019), Global Internet Forum to Counter Terrorism's 'Transparency Report' Raises More Questions Than Answers, JustSecurity.*
[248] *EU Commission (2020), Leaked report on technical solutions to detect child sexual abuse in end-to-end encrypted communications.*

19. GOING BEYOND THE ENCRYPTION DEBATE

Use of strong encryption has become the backbone of data security and online privacy and is likely to remain so going forward. Messaging apps offering E2EE epitomise this trend. Whilst concerns over misuse of E2EE are warranted, there is a need to go beyond the encryption debate, and the continual dichotomy between ensuring privacy and security online and preventing the emergence of online safe havens for criminals.

Rather than calling for backdoor access to or systematic screening of E2EE communication, which are likely to create significant security risks, innovative investigative techniques adapted to the evolving online space should be explored. Below, we provide an overview of some approaches and techniques that can provide an alternative to systematic and indiscriminate monitoring practices, whether that be via backdoor access or the screening of content

19.a Collaboration between law enforcement and tech companies

Most tech companies are willing to act against criminal exploitation of their platforms and to collaborate with law enforcement to assist with investigations – when such requests are lawfully made and respect due process.

Tech sector initiatives – Tackling the threat in a collaborative manner

Beside direct collaboration between tech companies and law enforcement, tech sector initiatives and public-private partnerships, focused on providing tech companies with the tools and knowledge required to counter terrorist use of the internet, demonstrate the tech sector's willingness to act against terrorist exploitation. The Global Internet Forum to Counter Terrorism (GIFCT) and Tech Against Terrorism are leading initiatives in this domain.

- The GIFCT was founded[249] in 2017 with the goal of" foster[ing] technical collaboration" between tech platforms in response to the increased threat of terrorist exploitation.
- Tech Against Terrorism, is a public-private partnership supported by the United Nations Security Council, whose core aim is to support the tech sector in tackling terrorist exploitation whilst respecting human rights, by providing smaller companies with the technical tools and policy support required.

[249] *The GIFCT was originally founded by Facebook, Microsoft, Twitter and Youtube, and has continued to expand its membership to other tech platforms. See: https://gifct.org/membership/*

Innovative investigation techniques

Tech companies are usually willing to counter illegal activity on their platforms but are often hindered by lack of capacity and clear guidelines from governments. Law enforcement agencies should focus on increasing collaboration with tech platforms, as well on developing relationships based on trust to think through innovative solutions to identify and disrupt criminal use of encrypted platforms.

The Europol Innovation Lab is one example of how law enforcement can adapt to emerging technologies. The Lab is intended to be "a strategic actor in the field of innovation", and designed to identify and respond to the challenges posed by emerging technologies, including with regard to data and ethics and by engaging in a dialogue with the private sector.[250] The EU Strategy on CSAM also listed the creation of an Innovation Hub by Europol to ensure the development of capacities to follow technical developments.

Adapting HUMINT to the digital world

Innovations in investigative techniques should be sought not only in the development of technical tools, but also in the incorporation and adaptation of traditional law enforcement investigation techniques. In particular, human intelligence (HUMINT) techniques should be rethought for the online space, and adapted to online monitoring. HUMINT should also be combined with the analysis of publicly available information via open-source intelligence (OSINT) techniques.

Transparency

Transparent and lawful cooperation between law enforcement and encrypted platforms should be encouraged.[251] Such collaboration has worked in the past and has been improving in recent years.[253] The E2EE platforms interviewed for this report all stated that they were working with law enforcement agencies to counter criminal use of their services, so long as this did not mean weakening the security and privacy enjoyed by their users.

[250] *Europol (2019), Written contribution to JPSG – The Europol Innovation Lab; and Monroy Matthias (2019), New Technologies: Europol sets up an „Innovation Laboratory".*
[251] *Provided that they are not contingent on a requirement for platforms to provide "technical assistance" to ensure that law enforcement can access encrypted communication channels or decrypted content. For more information about technical assistance requirements incorporated in legislations, please see Section of Part 1 of this report, Landscape Review, on "Policy-Makers Calls for Access to and Traceability E2EE".*
[252] *Macdonald Stuart and Staniforth Andrew (2021), The Tech Industry And The Regulation Of Online Terrorist Content: What Do Law Enforcement Think?, Hedayah.*

Transparency reports – insight into tech sector & law enforcement collaboration

Tech companies' transparency reports[253] on the requests received from law enforcement and governments provide great insights into the extent of their collaboration with national authorities.

These reports also demonstrate the tech sector's efforts at increasing transparency around such cooperation, and how they respond to law enforcement requests, in a landscape still characterised by users' concerns for the privacy of their data. Given the lack of similar reports from governments and law enforcement agencies, transparency reports provide a unique insight for the public into what law enforcement are requesting from the tech sector.

Even though E2EE limits data sharing, some E2EE platforms have nonetheless published transparency reports on government and law enforcement requests received. Outlining what countries made the requests, and what type of information they were able to disclose.

19.b Targeted surveillance of E2EE communications: monitoring of encrypted platforms and lawful hacking

As we saw in Part 2 of this report, law enforcement authorities have already been using different monitoring techniques to gain access to the content of communications shared on E2EE messaging apps.

Overall, targeted surveillance solutions – when legally mandated – offer a means of disrupting terrorist use of E2EE services and of conducting e-investigations. Moreover, they offer the possibility of doing so without mandating tech companies to create backdoors to encryption or systematically screen the content of E2EE communications. Lawful hacking, in particular, has often been held as the "better (although imperfect) alternative solution to exceptional access"[254] in response to the "going dark" phenomenon.

In general, targeted actions for accessing E2EE conversations can be categorised as follows:[255]

[253] *For examples of EMS publishing transparency report see: Unencrypted metadata available on E2EE platforms and their information sharing with third parties including law enforcement.*
[254] *Liguori Carlos (2020), Exploring lawful hacking as a possible answer to the "going dark" debate, Michigan Technology Law Review.*
[255] *Taxonomy inspired by Stepanovich Amie (2016), A Human Rights Response to Government Hacking, AccessNow. For more information about the different techniques presented in the table, and examples of their use by law enforcement, see: Part 2 of this report, Criminal use of E2EE.*

Surveillance technique	Sub-category
Lawful monitoring: Accessing communication channels via sock puppet accounts to monitor terrorist activities and networks online.	**Use of publicly available online information:** Sock puppet accounts can be used to find, track, and monitor terrorist and violent extremist networks operating in both public and private channels through open-source intelligence.
	Passive monitoring: Communication channels are accessed for monitoring purposes, although there is no engagement or other communication with other participants.
	Participative monitoring: Communication channels are accessed and active engagement and communication are undertaken online with violent extremists and terrorists.[256]
Lawful hacking: Use of hacking techniques, allowing access into a user's device(s) by law enforcement and security agencies when conducting an investigation.[257]	**Endpoint compromise:** Hacking techniques using targeted malware to target the user device and directly implement "trojans or malware, or [create] malicious resources and [convince] the target to visit that resource."[258]
	Host compromise: Similar to the endpoint compromise but targeting the host servers rather than the user device. A well-known example of this is the hacking of Encrochat coordinated by European law enforcement agencies.[259]
	Breaking encryption protocols: This technique focuses on cracking the overall encryption protection of a specific system in order to directly access encrypted communication channels. At the time of writing, there is no public record of such techniques having been used to break E2EE protocols, which remain the most secure form of encryption available.

"Ghost Proposal": At the cross-roads of technical tools and lawful hacking

In a 2018 article for Lawfare,[260] Ian Levy and Crispin Robinson – respectively the Technical Director of the UK's National Cyber Security Centre (NCSC) and the Technical Director for Cryptanalysis at the UK Government Communications Headquarter (GCHQ) – laid out the UK's principles for access to encrypted data.

This set of 6 principles for ensuring minimum standards of privacy, oversight and trust in the tech sector when requesting exceptional and targeted access to encrypted communication was followed by a proposal to "silently add a law enforcement participant to a group chat or call." According to Levy and Robinson, this would allow for an easy access to encrypted communication channels without "weakening encryption or defeating the end-to-end nature of the service"

This "potential solution" suggested by Levy and Robinson is commonly known as the "Ghost proposal", and has been widely criticised by civil society, cryptographers and tech companies alike for being nothing like the solution alleged. Broadly, this proposal would require tech companies to add a "ghost user" to an existing encrypted chat (1-on-1 or group chats), without notifying users that an additional person was added, so that law enforcement could have access to entire decrypted conversations.

[256] *The FBI is known for the use of participative monitoring techniques and online undercover agents. More recently, the "Ulysse" trial shed light on how participative monitoring can be used to disrupt terrorist activities: the active online engagement – mainly via Skype and Telegram – of three undercover agents from the French General Directorate For Internal Security, led to the arrest of three individuals planning a terrorist attack in France, under the direction of an Islamic State operatives in Syria.*
See: FranceInfo (2021), On vous explique l'opération "Ulysse", la cyber-infiltration de la DGSI qui a permis de déjouer un projet d'attentat en France; Suc Matthieu (2021a), Au procès «Ulysse», les zones d'ombre de la cyber-infiltration subsistent, Mediapart; Suc Matthieu (2021b), «Ulysse» et les djihadistes, les dessous d'un attentat empêché, Mediapart.
[257] *Liguori (2020).*
[258] *Stepanovich (2016).*
[259] *See: Europol (2020), Dismantling of An Encrypted Network Sends Shockwaves Through Organised Crime Groups Across Europe. Cox Joseph (2020), How Police Secretly Took Over a Global Phone Network for Organized Crime, Vice News.*
[260] *Levy Ian and Robinson Crispin (2018), Principles for a More Informed Exceptional Access Debate, Lawfare. This article was part of a series from the Crypto 2018 Workshop on Encryption and Surveillance.*

Contrary to what was suggested by Levy and Robinson, and to the principles they espouse,[261] introducing a ghost user would require services providers to significantly change their operating systems, by requiring them to add a new public key into a conversation[262] (owned by law enforcement) and to suppress all notifications to users that are normally sent when a new participant is added to a chat.

In an open letter to GCHQ, signed by a coalition of 47 signatories (representing civil society organisations, tech companies and trade associations),[263] the Open Technology Institute at New America, outlined the main concerns with the "ghost proposal":[264]

- **Undermines trust:** Requiring service providers to significantly change their systems will undermine users' trust in the security of their communication and, therefore, in tech companies.
- **Impacts the core of E2EE, authentication:** Modifying the authentication system (change in the public key and no user notifications) will create authentication concerns, and thus significantly impact E2EE systems whose integrity relies largely on the security of authentication and the encryption keys used.[265]
- **Creates vulnerabilities:** As with all the technical tools to screen encrypted content reviewed above, the introduction of a ghost user will create unintentional security and privacy vulnerabilities impacting all users of the service and not just selected criminal users. Additionally, there is the risk that users will refuse to update their apps and operating systems, if they think that this will lead to their conversations being monitored, which will leave them vulnerable to security risks that would otherwise be resolved by system updates.
- **Creates risks of abuse and misuse:** All technical tools to monitor encrypted communications, or provide access to law enforcement, can "open the door to surveillance abuses that are not possible today".[266] They also risk being hacked and used by malevolent actors.[267]
- **Contrary to the UK Principles for access to encrypted services:** Notably, the proposal is contrary to principles 5 and 6 on ensuring user trust and transparency, given the secrecy inherent in the idea of a "ghost" user.
- **Impacts average users without solving the problem of criminal use of E2EE:** As we saw above, most technical tools proposed by law enforcement to access encrypted communication creates security risks for the average users when tech-savvy criminal actors migrate to other encrypted services that do not collaborate with law enforcement. In the case of a ghost-user, critics have also suggested that criminal actors could refuse to update their systems and encrypted apps to stop a ghost user being added to their conversations.

[261] *Principle 5: "Any exceptional access solution should not fundamentally change the trust relationship between a service provider and its users"*
[262] *For more information about public and private keys, and the functioning of end-to-encryption, please see: Part 1 of this report, Use and Perception of E2EE: Landscape Review, Annex 1 | Encryption technology.*
[263] *Including WhatsApp and Facebook (the latter via the Reform Government Surveillance Coalition)*
[264] *Open Technology Institute, at New America, (2019), Open Letter to GCHQ on the Threats Posed by the Ghost Proposal.*
[265] *This is especially true for encrypted services based on the Signal Protocol, including WhatsApp. See: Schulman Ross (2019), Why the Ghost Keys 'Solution' to Encryption is No Solution, JustSecurity.*
[266] *Open Technology Institute (2019)*
[267] *Ibid.*

- **Ghost-users can be detected**: The Electronic Frontier Foundation has outlined four different techniques to detect ghost users: "binary reverse engineering, cryptographic side channels, network-traffic analysis, and crash log analysis." [268]

Whereas lawful and targeted surveillance techniques can represent an interesting manner to detect and disrupt terrorist use of E2EE, the requirement on tech companies to technically modify their systems presents a similar set of risks and abuse to those common to all technical tools to proactively screen E2EE content – See Section 6.c Risks associated with the pro-active screening of E2EE content. Tech Against Terrorism thus cautions against any legal requirement for a "ghost-user".

The targeted surveillance techniques above warrant further discussion of the regulation of lawful hacking and monitoring, whilst ensuring a minimal impact on human rights and the right to privacy.

Due process and rule of law

For targeted solutions to constitute a viable alternative, due process and the rule of law must be respected when conducting E2EE communication-related investigations. Amie Stepanovich and Carlos Liquori, in their respective publications, underline the need for the regulation of lawful hacking to be considered further, including as a way to bring existing investigation practices within the law.

Ensuring due process for lawful hacking is also essential to maintain public trust in the cooperation between tech companies and law enforcement . User concerns about privacy have remained high since the Snowden revelations of US government surveillance and the 2018 Cambridge Analytica scandal, both of which significantly impacted user trust in tech companies.[269] To avoid this trust being further eroded, the human rights and security impacts of lawful hacking and targeted monitoring need to be carefully considered.

[268] *Cardozo Nate and Schoen Seth (2019), Detecting Ghosts By Reverse Engineering: Who Ya Gonna Call?, Lawfare.*
[269] *Interestingly, the Snowden revelations, though shedding light on government surveillance programmes, appeared to have had a more significant impact on user trust in tech companies themselves.*

Rather than calling for misguided regulation insisting on backdoors and the systematic monitoring of E2EE, there is a need for regulatory frameworks to adapt to the realities of the online landscape and ensure that public trust in governments and tech companies is not further undermined. Whilst such regulations have been passed in certain countries,[270] policymakers are still all too often calling for backdoors to encryption.

To ensure that trust and due process are not compromised, the following must be considered:

- **Reporting of vulnerabilities:** Lawful hacking relies on the exploitation of pre-existing vulnerabilities in the systems targeted, and thus raises questions of how to report these vulnerabilities to the service, software or device providers. Should it be disclosed? If so, when, how, and to whom? Answers might differ depending on the investigation. However, and despite the case-by-case specificities, regulation should reflect the intricacies of lawful hacking and the disclosure of vulnerabilities.

- **Indiscriminate use:** For lawful hacking and targeted monitoring to be viable solutions, such practices must not permit blanket surveillance. A regulatory framework needs to ensure that lawful hacking does not become an indiscriminate practice which undermines public trust.

- **"Permissible" infringement of the right to privacy:** Any legal obligation that vitiates the right to privacy needs to be clearly and narrowly defined by law, applicable in a limited set of circumstances, and supervised by judicial authorities. Amie Stipanovich adds a further desirable limitation to lawful hacking, arguing that as a breach of privacy privacy, it should only be used when proven to be "the least invasive legal means to get specified protected information".[271]

- **International cooperation:** Targeted solutions also raise questions concerning jurisdiction and international cooperation, given the inherently transnational nature of the internet, and its use by terrorist actors. These practices thus "require an enhancement of international treaties regarding law enforcement cooperation for local lawful hacking frameworks to be effective".[272]

[270] *For a complete overview of regulation related to encryption and lawful hacking, please see: http://www.fgv.br/direitosp/cryptomap/#home*
[271] *Stepanovich (2016).*
[272] *Liquori (2020)*

tech against terrorism

PART 4

TECH AGAINST TERRORISM'S RECOMMENDATIONS FOR ENCRYPTED MESSAGING SERVICES

20. RECOMMENDATION: MITIGATING RISKS OF TERRORIST AND VIOLENT EXTREMIST USE OF EMS

20.a Encrypted messaging apps' features offering

As outlined in Part 3, Criminal Use of E2EE – Strategies for Risk Mitigation, some platform features are attractive to terrorist and violent extremists, whereas others might actually deter such actors from using specific platforms. Based on our understanding of what specific features are attractive to terrorist and violent extremist actors, Tech Against Terrorism recommends the following:

- **Size of group chats, channels and broadcasts lists:** large group chat permissions are attractive to terrorists, who make use of them to facilitate the dissemination of terrorist content, to organise, and to foster in-group networking.

1) EMS should remain cognisant of size for group chats, channels, and broadcasts lists and its implications for exploitation by terrorists and violent extremists.

- **Group join links:** Even when a group is not searchable within an app, join links can be used to build repositories of group chats online, which can then be used to search for terrorist and violent extremist groups. Join links also allow malevolent actors to easily build online networks by disseminating them across online platforms.

2) EMS should introduce a time limit on the validity of join links. This would allow average users to keep making use of them whilst reducing terrorists' ability to easily store and share them.

- **Group member visibility:** Terrorist actors often seek online anonymity. The ability for members of a group chat to view each other's profile information - even for group members not in a user's contacts - reduces online anonymity and might deter terrorist actors from using a specific app.

3) EMS should take into account that increasing anonymity between group, channel, or broadcast lists members could make the service more attractive to terrorist groups.

- **User reporting:** The easiest and most E2EE-compatible means of identifying malign use of messaging services.

4) Tech Against Terrorism recommends that EMS ensure that a user reporting function is easily visible to and navigable by its users.

  - EMS could launch "awareness" campaigns to remind users of the availability of such a function. This should be done in a manner that makes clear to users that reporting will not affect E2EE protection.[273]

[273] *For instance, by clearly explaining what messages will be decrypted and sent to the Trust & Safety teams, and by reminding users that their other conversations won't be affected and cannot be viewed by anyone else but the sender and recipient(s).*

Further to these recommendations, **Tech Against Terrorism recommends that EMS carefully consider the privacy benefits and the potential risk of terrorist and violent extremist use of the following features:**

Set of characteristics	Specific features
Security	Delete / Destruct message (including time delete)
	Private (password protected) chats
	Proxy-servers / VPN via the app
Proxy-servers / VPN via the app	Proxy-servers / VPN via the app
Stability	Large or unlimited file-size for sharing and storing
Audience reach	Large group size
	Channels / public groups / broadcast list (especially if large audience capacity)
	Ability to search in-app for groups or channels

20.b Metadata analysis

Platforms using E2EE whose content data is inaccessible to the service provider and to third parties can employ metadata analysis for content moderation or to cooperate with law enforcement without breaking encryption.

● **Behavioural analysis:** As highlighted by Schulz and van Hoboken in a 2016 UNESCO report, metadata can be used to conduct behavioural analysis and identify unusual patterns of communication indicating the use of E2EE services by criminal actors. Unlike communication data, metadata is usually unencrypted and is therefore preferable to breaking encryption as it provides insights to user activity whilst safeguarding security and privacy.

5) Platforms offering E2EE should use metadata to detect behavioural patterns of criminal use of their services – according to ePrivacy regulations in place.[274]

- o Metadata can also be used to identify networks of terrorist actors and supporters using encrypted services.
- o This should be done in a transparent manner, explaining to users why metadata is needed to counter criminal use and how metadata is used for that purpose.

● **Keyword analysis:** Platforms using encryption can also use keyword and image analysis on non-encrypted metadata to surface specific accounts, channels or groups for potential counterterrorism enforcement. Keywords and images can signal affiliation with or support to a terrorist group by re-using elements of language or imagery common to a group propaganda apparatus.

6) Platforms should support the development of keyword analysis to identify terrorist networks on encrypted messaging services.

- o Profile pictures, profile names, status, as well as names and icons of group chats and channels can be used as the basis for such analysis.
- o When conducting keyword analysis, platforms should be cautious of strategies used by terrorist groups and their supporters to bypass moderation by tech platforms. This includes “broken text” tactics which are commonly used by terrorists and violent extremists to evade automated flagging tools and text analysis.[275]

[274] *The Council of the EU approved in February 2021 a new draft regulation regarding the privacy of electronic communications, with implications for the monitoring and processing of E2EE communications data and metadata. The draft states that all data related to private online communications fall under the scope of the fundamental right to privacy. All electronic communications, and related metadata, for end-users located in the EU are to be protected by this regulation: any interference with data by anyone other than the end-user will be prohibited. However, the regulation notes exemptions to this rule. Permitted processing of electronic communications data without the consent of the user includes “cases where the service provider is bound by EU or member states’ law for the prosecution of criminal offences or prevention of threats to public security.” Thus, platforms should be wary of the new EU privacy rules’ implications for communications data and metadata privacy, though there are relevant exemptions which can apply to platforms assisting in law enforcement investigations or monitoring for illegal activities. However, these exceptions would require clarifications for platforms to act against terrorist and illegal content.*

[275] *A typical example of a “broken text” is the use of a “hyphen” in the middle of a word likely to part of a platform’s keywords database for automated detection of terrorist content and networks (e.g. “muja-hideen” instead of “mujahideen”).*

1. ACCOUNT CREATION

Account information: Names or usernames, and user profiles (incl. status and photos) can be scanned for keywords and visuals indicating links to terrorist and violent extremist groups.

Join groups behaviour: User joins or creates an unusual number of group chats, channels, or broadcast lists.

2. RECEIVING BEHAVIOUR

Forward: User forwards received messages in-between chats, in particular group chats.

Passive reception: User has little to no reactivity to messages received (except forwarding).

3. SENDING BEHAVIOUR

Mass send out: Messages sent out simultaneously across group chats, channels and broadcast lists.

Non-text content: Frequent sharing of non-text content, including audio, images, and outlinks.

4. GROUPS & BROADCAST LISTS

Size and members:
- Large group size.
- Members across the world.
- Members do not have each other as address book contacts.

Broadcast behaviour:
- Only a handful of users, group administrators, share messages or content.
- Little to no interactions between group members.

Mirror groups and broadcast lists:
- Multiple versions of the same groups or lists, with the same administrators and members.
- Similar group names or images.
- Similar patterns of interaction across groups
- Messages forwarded in-between groups.

Figures 2 and 3: The above figures depict behavioural patterns on encrypted messaging services that can be used to detect terrorist networks on the services. For more information about metadata analysis to identify suspicious patterns of behaviours, please see Part 3 of this report, Risks Mitigation Strategies, Section 5: Identifying Patterns of Criminal Use – Metadata Analysis.

20.c Technical content moderation solutions on E2EE

None of the solutions to screen the content of E2EE communication for the purpose of detecting illegal content technically breach encryption – no backdoors to the encryption protocols are needed. However, all of these solutions entail interference in the transmission chain and thus present significant risks to security and privacy, including the adverse risk of terrorist actors exploiting such weaknesses. The screening of content also breaks encryption's fundamental promise of privacy when it determines whether a piece of content is identical to another or not.

7) Tech Against Terrorism strongly warns against the introduction of any of the technical tools to moderate encrypted content which have been reviewed in this report.[276]

- o This includes homomorphic encryption. Whilst permitting the analysis of encrypted content, homomorphic encryption still allows for the systematic screening of user content which contradicts the privacy promise of E2EE.

20.d Acting against criminal use

As we saw in Part 2, Assessing Terrorist and Violent Extremist Use of E2EE, the way in which an app brands itself and is perceived by terrorists and violent extremists determines whether malevolent actors will use it or not. The same applies for how an app communicates about the action it takes to counter criminal use.

8) EMS should have an explicit and emphatic zero-tolerance policy for criminal actors, especially terrorists and violent extremists.

- o Policies and methods of enforcement against these actors should be clearly explained, regularly re-asserted, and be reported on transparently.
- o This should be emphasised whenever calls for backdoors to E2EE are made by policymakers, or user privacy is questioned.

9) Platforms should prioritise public communication around the different considerations and risk mitigation strategies developed to limit illegal use of their E2EE messaging services. This will address concerns that E2EE is detrimental to the fight against terrorism and violent extremism online, and further show that a platform considers this risk seriously and is committed to countering it.

[276] *See Part 3 of this report, "Strategies for Risks Mitigation", Section 2.c "Disrupting Criminal Use – Technical Tools to Detect Illegal Content".*

20.e Innovative investigation techniques

Rather than calling for backdoors to encryption and screening solutions that would put the security of billions of users at risk, innovative investigation techniques need to be developed by law enforcement to adapt to the new digital space.

To support this, and show to concerned users that a tech company is determined to not have its messaging services become “safe spaces” for criminals, encrypted messaging services should:

10) Maintain constructive working relationships with law enforcement agencies and consider how to support investigations involving digital evidence and encrypted data – when lawfully warranted and without weakening encryption.

11) Create a resource centre on their websites for law enforcement and governments, facilitating access to:

- o Guidelines for information requests.
- o Additional information on technical capacity to support investigations involving digital evidence without undermining users’ security and privacy.

21. RECOMMENDATION: TAKING A STAND FOR ENCRYPTION

Since Facebook announced its plan to roll-out E2EE on all its messaging services in 2019,[277] public discussion about E2EE and the risks of criminal use has been dominated by policymakers calling for backdoors to encryption. In response, digital rights groups and privacy-focused platforms have increased their advocacy for encryption. However, the arguments for encryption raised by digital rights groups and encryption experts all too often remain limited to a niche audience of privacy-wary individuals, with limited reach when it comes to the general public. This has given too much space for a tech-blaming narrative to set in when the argument of "uncooperative tech platforms" is made repeatedly by certain policymakers and law enforcement officials.

In light of this, tech platforms should further work to counter the arguments against encryption, and raise awareness amongst the general public and policymakers about the significance of E2EE for online privacy and security.

12) Tech platforms, in particular when offering encryption, should emphasise in addition to the benefits of E2EE, the following inherent risks of backdoors to and systematic monitoring of encrypted communication:

- The impact on users' right to privacy and freedom of expression.
- The security risks for all users, including exploitation of these risks by terrorists and adversarial states.
- The question of jurisdiction and scope of application.
- The broad language of laws which risks increased surveillance of private communications in the future.
- The risk of mass surveillance of user communications.

13) Particular emphasis should be placed on the argument that there is no guarantee that backdoors to or systematic monitoring of encrypted content will be efficient in countering and disrupting criminal activities. In particular, the following should be emphasised:

- The lack of substantial evidence that the inability to access encrypted communications significantly hinders the work of law enforcement, or that the monitoring of criminal actors cannot be done in another manner.
- The risk of criminal actors migrating to other, non-cooperative, platforms and using other encryption tools.
- The fact that E2EE is not necessarily a determining factor for terrorists when establishing themselves on an app, especially if the service is used for strategic and propaganda purposes rather than organisational ones.

14) In general, EMS should increase public communication about how E2EE is the backbone of today's security and privacy, online and offline, including in protection of the public against criminal actors.[278]

15) EMS should also support public-private partnerships to effectively counter illegal use of E2EE services whilst protecting human rights, including the right to privacy.

[277] *Zuckerberg Marc (2019), A Privacy-Focused Vision for Social Networking.*
[278] *An interesting, yet too exceptional, example of this is the Internet Society's article on the risks for children if encryption was to be weakened: Campbell Natalie (2021), Don't Make Parents Raise Kids in a World Without Encryption, Internet Society; and De Guzman Noelle Francesca (2020), Kids need encryption too, Internet Society.*

21.a Communication around encrypted messaging services'

Privacy and security are integral parts of most EMS branding. Beyond branding and making a public commitment to safeguarding privacy and security online, Tech Against Terrorism recommends that EMS:

16) Give users explicit and digestible explanations of how the messaging service is designed to protect both privacy and security, with a clear distinction between features working to safeguard privacy and features designed to ensure security.

17) To facilitate communication around features and policy updates, and security and privacy in general, EMS should create easily accessible "Safety" or "Resources" centers, which could include:

- o Infographics or videos explaining what end-to-end encryption is and why it matters.
- o Infographics summarising the app's privacy and security offering.
- o Infographics or video providing safety tips to users, with mention of the app's commitment to counter criminal use, how to detect spam behaviour, misinformation and how to counter it, and what to do when receiving an unsolicited message.
- o Infographics summarising how metadata are collected and handled.
- o Information about upcoming changes, including when to expect them, what they mean for privacy, with a hyperlink to a page detailing the update.
- o A newsroom providing direct user access to major announcements made by the EMS.
- o Direct access to "request my information" forms, when available.
- o Direct access to transparency reports, when available.

21.b Transparency

Technical features such as encryption and metadata or the exact relationship between a parent company and its different services can be confusing and difficult to understand for users. EMS can improve their transparency in this regard to ensure that users do not misunderstand how their data is collected and handled.

18) In addition to a privacy policy, which can be difficult for users to understand, EMS should consider creating dedicated data transparency centers.

- o Such centers should include easy to understand blog posts and infographics about data collection and its purposes.
- o Where no data is collected or shared, this should be further underlined.

19) EMS should transparently report on their efforts to counter terrorist use of their services, given the limits to their capacity and the constraints of E2EE and online privacy – some encrypted services already do so.[279] This would provide transparency on how platforms cooperate with law enforcement agencies and showcase their willingness to support investigations when lawfully mandated but without compromising encryption.

- To support increased and meaningful transparency from the tech sector, Tech Against Terrorism has published its Guidelines on Transparency Reporting on Online Counterterrorism Efforts, in which we ask companies to report on a small number of core metrics covering policies, processes, systems, and outcomes.

[279] *See: Threema, Transparency Report; Wire, Transparency Report; Mega.nz (2020), Transparency Report; ProtonMail (2020), Transparency Report.*

tech against terrorism

ANNEX

Annex 1. Encryption technology

Encryption refers to the "mathematical process of making a message unreadable except to a person who has the key to 'decrypt' it into readable form".[280] There are two major ways encryption is applied: to scramble data at rest and data in transit.

- Data that is "at rest" is stored somewhere – on a mobile device, laptop, server, or external hard drive – and is not moving from one place to another.
- Data "in transit" is moving over a network from one place to another. Examples of this are a message being sent on a messaging app or web browsers.[281]

There are two ways to encrypt data in transit: the transport-layer encryption, also known as transport layer security (TLS), and end-to-end encryption (E2EE).[282]

Annex 1.a. End-to-End-Encryption (client-side encryption)

E2EE is a method for encrypting communications between a receiver and a sender such that it can only be read on the two ends of the communication line, and not by a third party monitoring the server.[283] E2EE is usually associated with communication channels such as messaging or video calls.[284]

In order for E2EE to function, each user needs two encryption keys, one public and one private. Users keep a private key on their device, while the public key is used to encrypt and connect with other users. Once a message is received, the private key decrypts it.[285]

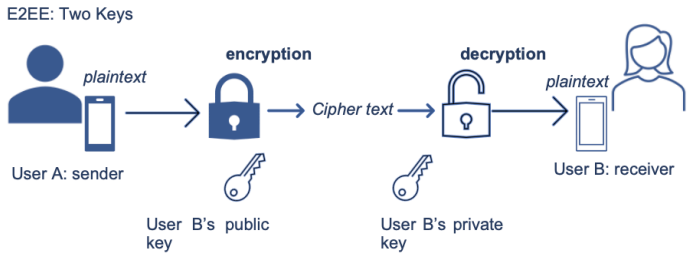
- For example, if a user A wants to send an encrypted message to user B, user A's message will first be encrypted by user B's public key. It then travels, in encrypted form, to user B. Once it reaches user B, their private key decrypts the message. This private key is solely available to user B, and the fact that the key is not travelling, but rather kept on the receiver's device, makes it impossible for any other party to decrypt the message.[286]
- This use of a private key and a public key is also known as "asymmetric" encryption – see the table on relevant encryption terms below for more information.[287]

Since E2EE ensures that no one can eavesdrop on the contents of a message in transit, it forces third party actors to either go directly to the sending or receiving device to try to compromise them in order to read the content of the encrypted message – such as by hacking directly into the sender's or recipient's device.[288] As third party actors unable to eavesdrop include governments, this level of security has caused for certain authorities who remain anxious to access data for their investigations, to ask technology companies to include 'backdoors' to encryption or other mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format.[289]

[280] *What should I know about Encryption, SSD*
[281] *Ibid.*
[282] *Ibid.*
[283] *What is End-to-End Encryption, Lifewire*
[284] *What is End-to-End Encryption and Why Does it Matter, NextCloud*
[285] *What is End-to-End Encryption, Dataprot*
[286] *What is End-to-End Encryption, Lifewire*
[287] *Ibid.*
[288] *What Is End-to-End Encryption? Another Bull's-Eye on Big Tech, NY Times*
[289] *'We want backdoors to E2E encrypted platforms for law enforcement': India, Japan, Five Eyes to companies, Medianama*

End-to-End Encryption

E2EE: Two Keys



E2EE: Multi-End Message and Object Encryption

Multi-End Message and Object Encryption (OMEMO) is an XMPP Extension Protocol (XEP) for secure multi-client end-to-end encryption. It differs from other end-to-end-encrypted protocols in the way that it allows users the benefits of message synchronization – users can be online with multiple devices simultaneously – and offline delivery. OMEMO is available in the Android XMPP-Client Conversations (on Google Play), the iOS client ChatSecure, or as a plugin for the Desktop client Gajim.[290]

Annex 1.b. TLS Encryption (server-side encryption)

E2EE differs from transport layer security encryption TLS, which only protects data in transit between the device and the service provider.[291] Thus, TLS is used extensively to secure connections between clients and servers.[292] TLS protects messages as they travel from the sender's device to the servers and from the servers to the recipient's device. In the middle, the server (such as a messaging service provider, website, or app) can see unencrypted copies of the messages. Since messages can be seen by (and are often stored on) company servers, they are vulnerable to law enforcement requests or leaks if company's servers are compromised.[293]

TLS is most prominently used to secure the data that travels between a web browser and a website via HTTPS, but it can also be used to secure emails and other protocols.[294] Two examples of TLS encryption implementation are HTTPS and VPN:

- Hypertext Transfer Protocol Secure, or HTTPS, which is the secure version of HTTP – the primary protocol used to send data between a web browser and a website – is an implementation of TLS encryption.[295]
- A Virtual Private Network, or VPN, is another example of TLS encryption. With a VPN, traffic travels over the ISP's connection, but it is encrypted between the user and their VPN provider. While using a VPN hides the traffic from a user's ISP, it exposes all of their traffic to the VPN provider, who will be able to see, store, and modify that traffic.[296]

[290] *OMEMO Multi-End Message and Object Encryption, conversations.im.*
[291] *What is End-to-End Encryption, Proton Mail*
[292] *What is End-to-End Encryption, Binance Academy*
[293] *What should I know about Encryption, SSD*
[294] *What is TLS and How Does it Work?, Comparitech*
[295] *What is HTTPS?, Cloudflare*
[296] *What should I know about Encryption, SSD*

Annex 1.c Encryption technology: glossary

There are various ways in which literature refers to client-client encryption and client-server encryption. Below, each key technical term is listed and briefly explained.

General Encryption Terminology

Keys	• An encryption key is typically a random string of bits generated specifically to scramble and unscramble data. Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable. The longer the key, the harder it is to break the encryption code.[297]
Ephemeral key	• A cryptographic key that is generated for each execution of a key-establishment process and that meets other requirements of the key type (e.g., unique to each message or session).[298]

Client-Client encryption: End-to-End-Encryption (E2EE)

"Client-side" encryption	• Client-side encryption is "any encryption that is applied to data before it is transmitted from a user device to a server". • E2EE can be viewed as a specialised use of client-side encryption for the purpose of exchanging messages.[299] • Client-side encryption is sometimes used interchangeably with E2EE.
"Asymmetric" encryption	• End-to-end encryption is an implementation of asymmetric encryption.[300] • Asymmetric encryption makes use of a recipient's public key, along with a private key that mathematically matches the public key. A user can then send a message encrypted with the public key, which is then decrypted by the recipient, using their matching private key.[301]
"Public Key" encryption	• Synonym for asymmetric encryption.
Multi-End Message and Object Encryption (OMEMO	• Multi-End Message and Object Encryption (OMEMO) is an XMPP Extension Protocol (XEP) for secure multi-client end-to-end encryption. • Different from other E2EE protocols by allowing users the benefits of message synchronization – users can be online with multiple devices simultaneously – and offline delivery.[302]

[297] *About Encryption Keys, IBM Knowledge Center*
[298] *Ephemeral Key, National Institute of Standards and Technology*
[299] *PKWARE, Client-Side Encryption vs. End-to-End Encryption: What's the Difference?,*
[300] *Unuth Nadeem (2019), What is End-to-End Encryption, Lifewire.*
[301] *Pixel Privacy, Encrypted Messaging: What is it, why you should use it and what are the best apps.*
[302] *Conversations.im, OMEMO Multi-End Message and Object Encryption.*

Client-Server / Server-side Encryption: TLS Encryption

"Client - server" or "server - side" encryption	● In the client-server model, the service provider acts as a middleman between the sender and the receiver.[303] As soon as the data arrives, the server encrypts it.[304]
Transport Layer Security (TLS) Encryption	● Only protects data in transit between the device and the service provider:[305] TLS protects messages as they travel from the sender's device to the servers and from the servers to the recipient's device. ● Used extensively to secure connections between clients and servers.[306] ● In the middle, the server (such as a messaging service provider, website, or app) can see unencrypted copies of the messages.[307]
Symmetric encryption	● The same key is used to encrypt and decrypt on both sides. ● Both legitimate parties need to have the key (making it 'symmetric') which may involve sending it over from one side to the other.[308]
"Private key" encryption	● Synonym for symmetric encryption.[309] ● Both keys are the same, allowing both parties to encrypt and/or decrypt the information.[310]

Major encryption protocols used for client-server encryption:	
Advanced encryption standard (AES)	● A US. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.[311] ● AES has three different key lengths. The main difference is the number of rounds that the data goes through in the encryption process, 10, 12 and 14 respectively. 192-bit and 256-bit provide a greater security margin than 128-bit. 128-bit AES is enough for most practical purposes. Highly sensitive data handled by those with an extreme threat level should probably be processed with either 192 or 256-bit AES.[312]
Secure sockets layers (SSL)	● An encryption-based internet security protocol. It is the predecessor to the modern TLS encryption used today. ● A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP." [313]
Hypertext transfer protocol secure (HTTPS)	● The secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer.[314]

[303] *Binance Academy (2020), What is End-to-End Encryption.*
[304] *Poortvliet Jos (2018), What is End-to-End Encryption and Why Does it Matter, NextCloud.*
[305] *Proton Mail What is End-to-End Encryption.*
[307] *Binance Academy (2020)*
[307] *Electronic Frontier Foundation – Surveillance Self-Defense (2018), What should I know about Encryption.*
[308] *Unuth (2019)*
[309] *What is Encryption and How Does it Work? Pixel Privacy*
[310] *What is private key encryption? Koolspin*
[311] *Advanced encryption standard (AES), National Institute of Standards and Technology*
[312] *What is AES encryption and how does it work? Comparitech*
[313] *What is SSL? Cloudflare*
[314] *What is HTTPS? Cloudflar*

Annex 1.d E2EE vs Client-server encryption

Whereas TLS encryption enables the company server to access the content of messages as they hold the encryption keys, E2EE eliminates this possibility because the service provider does not possess the decryption key. Due to this, E2EE is much more secure than standard encryption.[315]

Asymmetric encryption, upon which E2EE is based, is the safest method for two-way encryption.[316] The symmetric method, which TLS uses, is less secure since it requires the user to share the private key with the other party, which risks a security breach while in transit.[317] Given that TLS relies on a third party (such as a tech company) to encrypt messages as they move across the web, law enforcement and intelligence agencies can get access to encrypted messages for TLS by presenting technology companies with a warrant or national security letter.[318]

	Law Enforcement Access	Type of Use	Security Level
E2E Encryption	✗	Messenger services, video calls	High: Encrypted on the server. While E2EE is safe, users' devices can still be compromised.[319]
TLS Encryption	✓ Yes – by presenting technology companies with a warrant or national security letter.[320]	HTTPs, VPN, email providers	Low: Law enforcement can access; possible malicious attacks on the server.

Annex 1.e E2EE and the protection of private communications

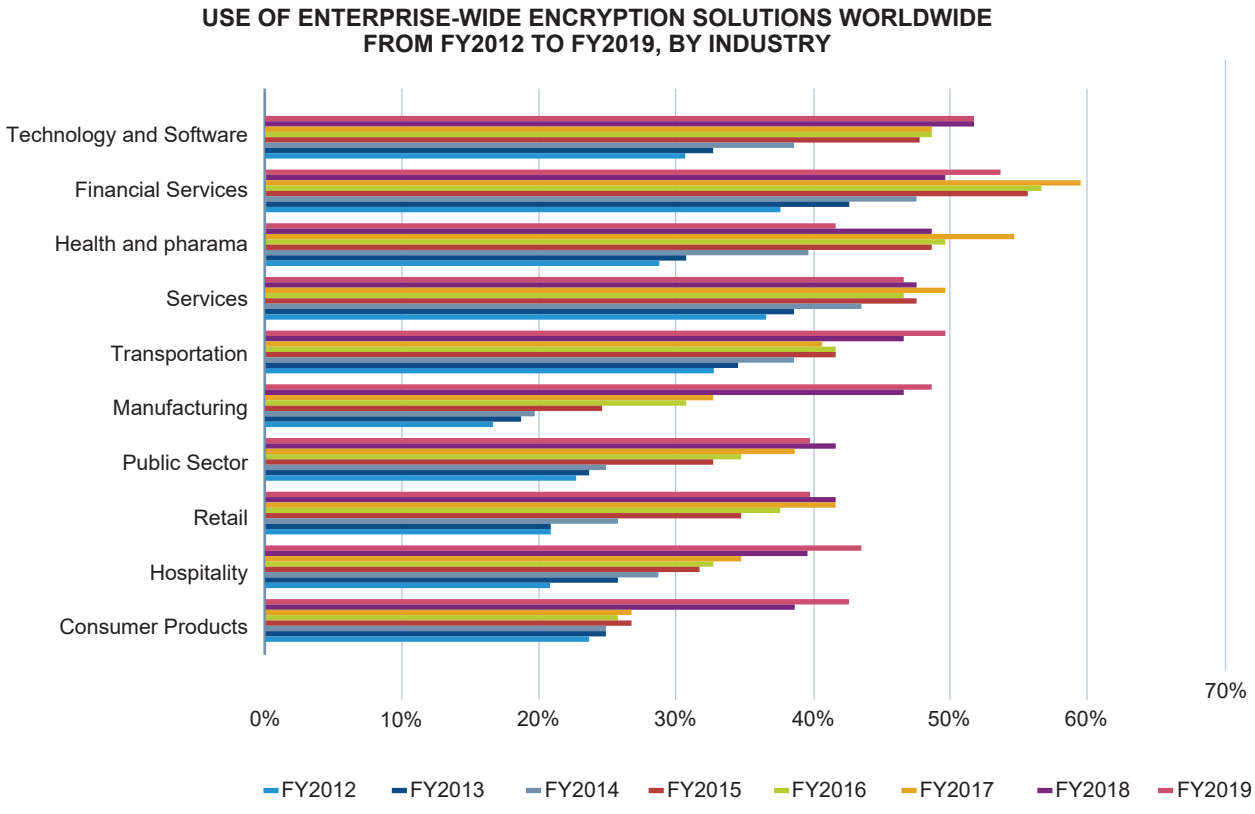
The use of encryption to ensure the integrity and safety of online data can be broadly divided into two general categories of encryption: Client-side or client-server encryption, and client-client encryption, including E2EE. Whereas for client-side encryption, encrypted data can be viewed and accessed by the online communications services, as data is encrypted when travelling to and from the ISP's servers, E2EE means that no-one but the sender and receiver can access the content which is encrypted and decrypted at both end of the transmission chain.

[315] *Proton Mail What is End-to-End Encryption.*
[316] *What is End-to-End Encryption, Dataprot*
[317] *Ibid.*
[318] *Pelroth Nicole (2019), "What Is End-to-End Encryption? Another Bull's-Eye on Big Tech", The New York Times.*
[319] *WhatsApp sues Israeli spyware company NSO Group for planting spyware in users' devices, Medianama*
[320] *What Is End-to-End Encryption? Another Bull's-Eye on Big Tech, The New York Times.*

Whereas client-side encryption mostly protects public information on the internet, including user-generated content on social media via HTTPS encryption,[321] E2EE is mainly used to protect user-generated communications such as instant messages and emails. When talking about the widespread use of E2EE, what is implied is the possibility for billions of users to benefit from private and secure communications in their daily life. Beyond individual users, E2EE ensures that the communications of all kinds of private and public organisations including financial institutions, governments and political parties, are safe from a breach or a leak that could expose confidential and sensitive information. The communications of public and private organisations cannot be accessed by malevolent external actors, including hostile foreign governments.

Annex 2. Encryption: a backbone of today's digital world

To protect users' information, most online platforms use client-server encryption[322] as a default option to encrypt data in transit and at rest. According to Fortinet, data encryption in recent years "has set a new bar", with encrypted traffic in 2018 already representing 72% of all network traffic, a 20% increase from the previous year.[323] Encryption has thus become the backbone that allows today's internet to exist, and is needed for all personal and professional business online.



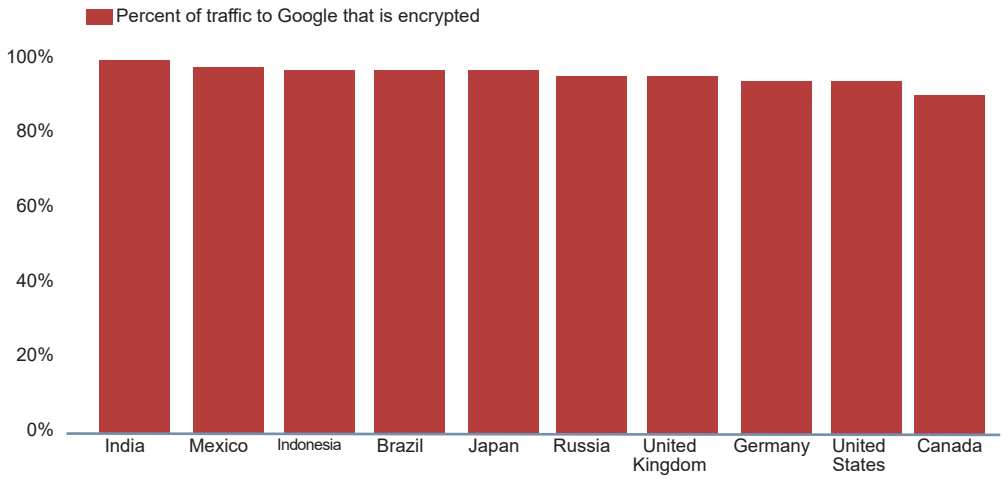
Source: Statista, Enterprise-wide encryption solution usage worldwide 2012-2019.

[321] *As for the majority of online platforms, most social media and content-sharing companies protect their platforms and data with HTTPS encryption, including, amongst other: Facebook, Instagram, Discord, Tumblr, Minds, Pinterest, Reddit, Twitter, and Youtube. Linkedin.*
[322] *Client-server encryption can include: transport layer security (TLS) protocol, advanced encryption standard (AES), or secure sockets layers (SSL) and the related hypertext transfer protocol secure (HTTPS)*
[323] *Fortiguard SE Team (2018), As the Holiday Season Draws Near, Mobile Malware Attacks Are Prevalent, Fortinet.*

The “encryption debate”, in which policymakers and law enforcement agencies calling for access to E2EE communications are opposed by encryption advocates (including technical experts), often makes it seem as if encryption is mostly a matter of users’ private communication vs. national security. However, encryption is not limited to private chats but underpins almost all daily activities that occur on the internet by allowing businesses to ensure the integrity and security of their users’ data. The fact that financial and health-related businesses are amongst the leading sectors using encryption to protect their data is indicative of this. Such businesses have to manage vast amounts of sensitive data, including their users’ PII, health records and banking details. For such entities, encryption is vital for ensuring that sensitive information cannot be accessed by malevolent actors.

Towards a fully encrypted web?

Google’s transparency report on encryption also offers us significant insights into the global volume of HTTPS encrypted web traffic and, thus, on how prevalent and common the use of encryption has become globally. In some regions, almost all web traffic is encrypted.[324]



Source: Google, HTTPS Encryption on the Web.

[324] *Google explains these volumes by the availability of software that can support encryption technologies, including TLS, in certain regions of the world, as well as by the type of devices available in these regions. Thus, the more individuals and organisations can have access to easy encryption, the more web traffic is likely to be encrypted.*

Annex 3.The encryption debate

Since the mid-1990s, as the development and widespread use of encryption technologies gained pace, policymakers, law enforcement officials and security agencies have raised concerns about how criminal actors could exploit such technologies to avoid law enforcement detection. The Clinton Administration was the first to make a proposal for a backdoor to encryption with the Clipper Chip -see below. Policymakers have since presented encryption as a security risk that severely hinders criminal investigations and provides online safe spaces for criminals. In particular, they have stressed that child sexual abuse and terrorist offenders could exploit such technologies. To counter this, prevent criminal use, and provide support to the victims, policymakers have argued that law enforcement should be granted safe access to encrypted communications, and that platforms implementing E2EE should consider content moderation mechanisms to detect illegal content (especially CSA material).

In response to these calls for "safe" backdoors to encryption, encryption experts, digital rights advocates, and in some cases tech companies – including Apple in its opposition to the FBI [325] – have argued that there is no such thing as a "safe" backdoor to encryption.[326] They have advanced technical arguments to demonstrate that E2EE content could simply not be accessed by any external party, not even the service provider, and that creating access for law enforcement would inevitably create security weaknesses that could be exploited by malevolent actors, including criminal actors and foreign governments. Overall, they have demonstrated that any sort of backdoor to encryption would create more security risks than it would resolve, and for a greater number of individuals and organisations.

Annex 3.a Privacy vs. Security: a polarising divide

Below, we present a summary of the two positions that have opposed each other in the encryption debate.

No backdoors – Online privacy and security should be safeguarded

Privacy and security benefits: E2EE is an essential technology to ensure the privacy and security of users' data and discussions, and thus has become an important tool to safeguard users' fundamental right to privacy. The same applies to private and public organisations, which can rely on E2EE to protect themselves from leaks and data breaches.

Trust in technology: Encryption, whether client-client or client-server, has become an integral part of our daily life online, and E2EE has become an important means for users to ascertain that their online communications and data are being protected: "Encryption is an anchor of confidence in digitalisation and in protection of fundamental rights." [327]

[325] *See: Part 2 of this report: Criminal Use of E2EE – Terrorists and Violent Extremists Focused Assessment*
[326] *Pelroth Nicole (2019), What Is End-to-End Encryption? Another Bull's-Eye on Big Tech, The New York Times; Kahney Leander (2019), The FBI wanted a backdoor to the Iphone, Tim Cook said no, Wired; Yadron Danny (2016), Apple CEO Tim Cook: FBI asked us to make software 'equivalent of cancer', The Guardian.*
[327] *Council of the EU (2020), Draft Council Resolution on Encryption - Security through encryption and security despite encryption,*

Fundamental right to privacy: The right to privacy is generally upheld as a fundamental one that ought to be safeguarded in democracies. This right is recognised both by the Charter of Fundamental Rights of the EU (Art. 7) and the US Constitution (4th Amendment). It is also enshrined in international human rights law, including in the Universal Declaration on Human Rights (Art. 12) and the International Covenant on Civil and Political Rights (Art. 17).[328]

Adversel risks to LE monitoring: E2EE advocates and technical experts agree that any "backdoor" or detection tools directly integrated into devices would break the purpose of E2EE and expose users to grave security risks. Any "backdoors" would create adverse risks for users' privacy and security, opening their data and communication to harmful actors.[329]

Pro-backdoors – Encryption impact on law enforcement work

The "going dark" argument: Widespread and easy access to E2EE can be abused by criminal actors. E2EE can be used as safe spaces for illegal activities, including fraud, terrorism and child sexual abuse in all impunity. Risks of criminal exploitation are said to increase as E2EE becomes widespread on mainstream platforms.

Challenges to access to e-evidence: E2EE is said to hinder criminal investigations, due to law enforcement not being able to access e-evidence.

Lack of tech sector cooperation: Policymakers have criticised tech companies for acting on their own when developing new encryption algorithms and deploying them on mainstream platforms. Moreover, tech companies are said to be uncooperative and to refuse to provide governments and law enforcement with the necessary keys to monitor encrypted communications.

WHO HAS BEEN SAYING WHAT ABOUT ENCRYPTION?

"From storing data on the cloud to online banking to identity verification, end-to-end encryption is essential for preventing data being accessed illegally in ways that can harm consumers, business and our national security."
Anthony Waler, techUK

"If the public's right of access is blocked, then these zones of personal privacy are converted into "law-free zones" insulated from legitimate scrutiny."
William P. Barr, Attorney General US

"It's hard to search for "middle ground" in the debate when middle ground is, by definition, a security flaw."
Joe Mullin, Electronic Frontier Foundation

"Independently of the technological environment of the day, it is therefore essential to preserve the powers of competent authorities in the area of security and criminal justice through lawful access to carry out their tasks, as prescribed and authorised by law."
Council of the E.U

[328] *See: United Nations Human Rights, Office of the High Commissioner, International Standards.*
On the right to privacy in the digital space see: United Nations Human Rights, Office of the High Commissioner (2014), The right to privacy in the digital age.
[329] *Ryan Polk (2020), European Union, Use Facts to Make Cybersecurity Decisions – Not Myths, Internet Society; Cohn Cindy (2020), Eight Epic Failures of Regulating Cryptography, Electronic Frontier Foundation; Ruiz David, There is no middle ground on encryption, Electronic Frontier Foundation.*

Annex 3.b A long standing debate

1990s – 2000s:"PGP" and the NSA's Clipper Chip → 2013: Snowden's revelations → 2016: WhatsApp goes fully E2EE; Apple vs FBI → 2019: FB pledge to deploy E2EE, 5Eyes open letter

The 1990s and the Clipper Chip: Already back in the mid-1990s, the development of "Pretty Good Privacy" (also known as PGP), a privacy software using an E2EE scheme, prompted the US National Security Agency under the Clinton Administration to announce the "Clipper Chip"[330]: "a piece of hardware designed for phones which would provide encryption on communications while also producing an encryption key and making it available to the NSA".[331] However, the US government backed down soon afterwards in 1996, as the chip had been widely criticised by a broad coalition including civil society organisations focused on defending civil liberties, Republican and Democratic senators, as well the Televangelist Pat Robertson, all recognising that any weakening of encryption for government purposes would also open the way for malevolent actors to exploit the same backdoors.[332] In an article summarising some of the arguments advanced against the chip back in the 1990s, Cindy Cohn, Executive Director at EFF, underlined how this was the first of a series of failed attempts by the government and law enforcement agencies in the US to call for a backdoor to encryption, as E2EE advocates argued that breaking into encryption would do more harm than good to US internet services providers and their consumers.

Even though the chip and related proposals to break into encryption were "declared dead" in the early 2000's, calls to develop government access to encrypted messaging services have resumed in recent years, often pushed by the argument of "encryption pos[ing] a grave threat to the public".[333] If the technical challenges – namely the impossibility of building a safe backdoor for legal law enforcement access that would not create more adverse risks for users – and risks for freedom of speech and the right to privacy remain the same, the online landscape surrounding the encryption debate has evolved. An evolution mostly motivated by users' concerns with their online privacy and the security of their data, which find its defining moment during the 2013 revelations by Edward Snowden on the NSA online surveillance programmes and that was further reinforced by the 2016 Cambridge Analytica scandal, that exposed the scale of government surveillance on internet users and the derives of users' data exploitation.

Following the revelations and to regain their users' trust, a number of tech companies announced that they would strengthen their encryption protocols, including Apple and Google. A promise to ensure users' privacy and safety that was met with criticisms from law enforcement officials in the US.[334]

In the years following the Snowden revelations, the digital environment was marked by the emergence and mainstream use of encrypted messaging services.[335]

[330] *Pelroth Nicole (2019), What Is End-to-End Encryption? Another Bull's-Eye on Big Tech, The New York Times*
[331] *Karsten Jack and West Darrell (2016), A brief history of U.S encryption policy, Brookings.*
[332] *See: Cohn Cindy (2018), "Resisting Law Enforcement's Siren Song: A Call for Cryptographers to Improve Trust and Security", Lawfare Pelroth (2019),*
[333] *Attorney General William P, Barr (2019)*
[334] *Mahlmann Ariel (2019), End-to-End Encryption Strategies Becoming the Norm for Social Media, Fortnix.*
[335] *Karsten and Wast (2016).*

Annex 4. Non-messaging E2EE services' cooperation with law enforcement

	T/VE policy	Take action against CSAM	Metadata Collection	information sharing with Third party including LE	Legal framework, illegal content, reporting	App ownership	Server location	Governing law
VIDEO CALLING APPS								
Zoom	✓	✓	**Technical information** about a user's device, network, and internet connection **Approximate location** **Metadata**, including duration of the meeting or Zoom Phone call; email address, name, or other information that participants enter to identify themselves in a meeting, join and leave time of participants, meeting name, the scheduled date and time of a meeting, call data records for Zoom Phone.	✓	✓	Zoom Video Communications, Inc	Worldwide	State of California
Skype	✓	✓	Yes, but the exact information is not specified clearly.	✓	✓	Microsoft	Not mentioned	Ireland (Europe users)
Jitsi	✗	✗	Chat content is stored during the meeting, the recording of the meeting is temporarily stored until it is uploaded to the file hosting service. If a livestreamed meeting, video content is temporarily stored to buffer the livestream. Optional personal profile information.	✓	✓ Outlined in the Terms of Service	8x8, Inc	Switzerland	State of New York

EMAIL SERVICES								
Outlook Email	✓	✓	Yes, but the exact information is not specified clearly.	✓ No specific TR, included in Microsoft's with no further details	✓ Legal and acceptable use detailed in Microsoft Code of Conduct	Microsoft	Not mentioned	
ProtonMail	✗	✗	It is not necessary to provide personal information in order to create an account Has access to email metadata: sender and recipient email addresses, the IP address incoming messages originated from, message subject, and message sent and received times.	✓ Law Enforcement Guidelines available.	✓ Legal and acceptable use detailed in Microsoft Code of Conduct	Proton Technologies AG	Switzerland	
Tutanota	✗	✗	email address, for paid products: invoicing information	✓ transparency report available	✗	Tutanota	Germany	
GSuite (Google Workspace)	✗	✓	Information about the apps, browsers and devices that users use to access Google services; Data on user activity; Location information.	✓ Transparency Report	✓ Outlined in Google Code of Conduct	Google	Worldwide; largely in US	

SEARCH ENGINE								
DuckDuckGo	✗	✗	Search history (not in a personally identifiable way, as do not store IP addresses or unique User agent strings).	✓ "we will comply with court ordered legal requests. However, in our case, we don't expect any because there is nothing useful to give them since we don't collect any personal information."	✗	Duck Duck Go, Inc	Not mentioned	United States

EMAIL SERVICES								
Mega	✓	✓	non-encrypted Personal Data: (email address, some activity detail relating to account access, file uploads, shares, chats). Full description of the information Mega stores about a user and their activities on Mega's system can be found in clause 7.3 of Mega's Privacy & Data Policy.	✓ Transparency Report	✓ Outlined in the Transparency report	MEGA	Not mentioned	New Zealand
Nextcloud	✗	✗	Collects non-personally-identifying information, such as the browser type, language preference, referring site, and the date and time of each visitor request.	✓ does not disclose personal information to third parties unless legally obliged to do so.	✗ Legal and acceptable use detailed in Microsoft Code of Conduct	Nextcloud	Not mentioned	Germany

Annex 5. The role of metadata in user-generated content & content moderation

The term 'metadata' has specific meanings in some technical protocols, but in the case of content moderation, there is specific metadata available on user-generated content (UGC) such as on a user's post, or other metadata which is not public but that is available to tech platforms – all which is relevant to the moderation process. According to a 2019 report on the use of AI in online content moderation produced on behalf of Ofcom, the UK's communications regulator, "the metadata is critical to understanding and detecting content that is only harmful when considered in the context of exchange." [336]

In Table A below, examples of metadata which are related to the content and context of user-generated content (UGC) are shown.

Table A: Examples of Metadata related to the content and context of UGC

Content	Context (Metadata)		
Posted content	**Context of the post**	**Context of the user identity**	**Context of the user's history**
• Text (including any hashtags) • Image • Audio • Video • Title	• History and previous posts of the threat • Date and time • Number of 'likes' from others (and their history and interests)	• IP address and geographic location • Device and browser data • Username • Real identity • Age • Registration information such as email address or mobile number • Other information held about the user (such as friends lists, followers, interests, etc.) • Length of time registered on the site • Amount of activity on the site • Previous posts which have been moderated as harmful	• Length of time registered on the site • Amount of activity on the site • Previous posts which have been moderated as harmful

It is important to note that metadata is not limited to that which is publicly visible in an online post, such as the username, the posting time, the group in which it is posted, the number of likes and the number of comments. Rather, it can also include information associated with a user such as their IP address, their time on the platform, their previous content history, their connection type, and other user identifiable information.[337] The difference between metadata available on a publicly visible post and additional information about the user to which the service provider would have access is outlined in Table B below.

Often publicly visible metadata	Other metadata which is not displayed within the post
• Date and time of post • Profile picture • Username • Context of other users mentioned • Destination of URL • Context of hashtags used • Number of 'likes'	• Geolocation • IP address • Confirmed real identity • Number of followers • Length of time user has registered on the site • Level of activity on the site • Number of previous posts which have been flagged for moderation

[336] *Cambridge Consultants for OfCom (2019).*
[337] *Ibid*

Annex 5.a Research related to use of metadata in identifying harmful content

A 2019 report on the use of AI in online content moderation produced on behalf of Ofcom, the UK's communications regulator, outlines research using metadata in identifying harmful content.[338] It concludes that research has shown that metadata is valuable in identifying harmful content but has limitations. The insights in the report include the following:

- Metadata can be especially useful for AI moderation of spam content or for finding fake accounts. AI can be trained to detect suspicious activity, such as an account reaching out to many more other accounts than usual, lots of seemingly automated activity, or the account having a different geographic source to the geographic location claimed by the account.[339]
- Research on other types of metadata being used (including number of previous posts by the user or number of replies to the specific post) has had conflicting results. This is because of the dependence of metadata on the source of the data (which can differ a lot, for instance from celebrity accounts to personal ones). As with many techniques reliant on data quality, which includes representativeness and diversity, machine learning will only be able to handle a dataset well if the model has been designed to deal with potentially poor- quality training datasets.

Beyond metadata: Market-driven data

Another substitute to encrypted data that Andrew Keane Woods suggests in his paper "Encryption Substitutes" for law enforcement is market-driven data. Woods cites a report by Harvard's Berkman Klein Center for Internet & Society, which argues that law enforcement has access to "ready substitute avenues of intelligence if and when current channels go dark". It finds that structural reasons explain why internet communication channels will never be fully encrypted; for example, while Apple can afford to take a strong pro-encryption stance because it derives most of its revenue from hardware sales, Google makes their money on advertisements, which often require the ability to scan through user data, a task that is currently not possible if the data is encrypted.[340] Thus, while some services would roll out encryption, others would remain unencrypted, possibly to monetise user-data. Woods additionally discusses how the wide adoption of sensors in everyday products ensures that there are many more sources of data available to law enforcement beyond phone calls and e-mails, such as security cameras, thermostats, internet-connected refrigerators, voice-enabled assistants like Amazon's Echo. These are a few examples of devices that collect user data which then can be accessed by law enforcement. Data from devices has already been used to successfully charge suspects in criminal cases.[341]

[338] *Cambridge Consultants for OfCom (2019).*
[339] *To see more on this read here: https://blog.twitter.com/official/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html.*
[340] *Woods (2017).*
[341] *Ibid.*

Annex 6. Safety by design

Certain governments have been exploring the merits of safety by design, calling for tech companies to introduce this thinking early on in their product and policy development process. Safety by design designates the introduction of risk prevention, preferably at the early stages of product development, by incorporating safety features such as that guided by a safety by design framework.[342]

Key proposed tenets of safety by design in Australia and the UK:

- Service provider responsibilities and clarity towards its users, such a clarity in terms of service violations
- Content detection systems[343] and trained moderators
- User empowerment and autonomy, such as improving user reporting and more control over their experience such as informed choices
- Transparency and accountability

Annex 6.a Safety by design in Australia

In May 2019, the eSafety Commissioner of Australia, who oversees Australia's online regulation, published a Safety by Design initiative report. It defines safety by design as "embedding the rights of users and user safety into the design and functionality of products and services."[344] In addition to privacy and security by design, safety by design thus becomes the third pillar in the product and policy development.

The Safety by Design Initiative of Australia's eSafety Commissioner includes three principles:[345]

1) Service provider responsibilities
2) User empowerment and autonomy
3) Transparency and accountability

The merits of adopting safety by design principles, according to the eSafety Commissioner include:

- Gives online services an edge in the marketplace
- Shows global leadership in developing online products and services that are truly centred around users[346]

Further, the eSafety Commissioner argues that "if online services can start to adopt key elements of the Safety by Design Framework, they will be taking affirmative steps to make user safety considerations a routine element of their product development cycles".

[342] *Mari Angelica (2019), UK introduces world's first online safety regulations, Computerweekly.com.*
[343] *It is important to note the risks of AI-based technology and content moderation. To read more on the issue, please read our position paper, which includes recommendations, here: Tech Against Terrorism (2021), Content personalisation and the online dissemination of terrorist and violent extremist content.*
[344] *eSafety Commissioner (2019), Safety by Design Overview, Government of Australia.*
[345] *The tables on safety by design initiative of Australia's safety commissioner are reconstructed from: http://www3.weforum.org/docs/WEF_Ethical_Principles_2020.pdf*
[346] *Ibid.*

1) Service provider responsibilities

● Nominate individuals, or teams – and hold them accountable – for user-safety policy creation, evaluation, implementation and operations.
● Develop community standards, terms of service and moderation procedures that are fairly and consistently implemented.
● Put in place infrastructure that supports internal and external triaging, clear escalation paths and reporting on all user-safety concerns, alongside readily accessible mechanisms for users to flag and report concerns and violations at the point that they occur.
● Ensure there are clear internal protocols for engaging with law enforcement, support services and illegal content hotlines.
● Put processes in place to detect, surface, flag and remove illegal and harmful conduct, contact and content with the aim of preventing harms before they occur.
● Prepare documented risk management and impact assessments to assess and remediate any potential safety harms that could be enabled, or facilitated by the product or service.
● Implement social contracts at the point of registration; these outline the duties and responsibilities of the service, user and third parties for the safety of all users.

2) User empowerment and autonomy

● Provide technical measures and tools that adequately allow users to manage their own safety, and that are set to the most secure privacy and safety levels by default.
● Establish clear protocols and consequences for service violations that serve as meaningful deterrents and reflect the values and expectations of the user base.
● Leverage the use of technical features to mitigate against risks and harms, which can be flagged to users at point of relevance, and which prompt and optimise safer interactions.
● Provide built-in support functions and feedback loops for users that inform users on the status of their reports, the outcomes of the reports, and offer an opportunity for appeal.
● Evaluate all design and function features to ensure that risk factors for all users – particularly for those with distinct characteristics and capabilities – have been mitigated before products or features are released to the public.

3) Transparency and accountability

● Ensure that user-safety policies, terms and conditions, community standards and processes about user safety are visible, easy to find, regularly updated and easy to understand. Users should be periodically reminded of these policies and proactively notified of changes or updates through targeted in-service communications.
● Carry out open engagement with a wide user base, including experts and key stakeholders, on the development, interpretation and application of safety standards and their effectiveness or appropriateness.
● Publish an annual assessment of reported abuses on the service, alongside the open publication of meaningful analysis of metrics such as abuse data and reports, the effectiveness of moderation efforts and the extent to which community standards and terms of service are being satisfied through enforcement metrics.
● Commit to consistently innovate and invest in safety-enhancing technologies on an ongoing basis and collaborate and share with others safety-enhancing tools, best practices, processes and technologies.

Annex 6.b Safety by design in the United Kingdom

In 2020, the UK government's Department for Digital, Culture, Media and Sport (DCMS) publicised that they would be developing "Safety by Design" Guidance for Online Platforms. This follows the UK's Online Harms White Paper acknowledgment of the impact that platform design decisions can have on the likelihood of online harm occurring. According to the UK government, Safety by Design guidance – which is not available at the time of writing – will play an important role in solving the current issue of many companies not having the necessary information to make safer decision choices.[347]

The UK government committed to developing a "Safety by Design Framework", a library of practical guidance for companies on how to design safer online services and products.[348] The Online Harms White Paper[349] hints that such guidance might highlight the need for providers to:

- Make it clear to users what forms of content are acceptable, as part of the terms of service and throughout their journey.
- Have effective systems for detecting and responding to illegal or harmful content, including the use of AI-based technology[350] and trained moderators.
- Make it easy for users to report problem content, and design an efficient triage system to deal with reports of policy violations.
- Give users control of their experience by collecting the minimum amount of personal data and giving them informed choices about how their personal information, including geolocation data, is used.[351]

[347] *Department for Digital, Culture, Media and Sport (2020), Development of 'Safety by Design' Guidance for Online Platforms, Government of the United Kingdom.*
[348] *Ibid.*
[349] *The Online Harms White Paper was published in April 2019 and outlines the key principles for online regulation in the UK. The paper suggests that tech companies should have a "mandatory duty of care" to protect users from "online harms".*
[350] *It is important to note the risks of AI-based technology and content moderation. To read more on the issue, please read our position paper, which includes recommendations. See: Tech Against Terrorism (2021).*
[351] *Government of the United Kingdom (2019), Online Harms White Paper.*

LEGO Life App[352]

The Australian Safety by Design Initiative and the UK Government's Online Harms Whitepaper provide the same example of a platform that has successfully and proactively accomplished safety by design: The LEGO Life App. In 2017, LEGO Life was launched, a social-themed app to inspire younger children to build and share their creations in a high-safety, high-trust environment.[353] The LEGO Life app fully embraces Safety by Design principles such as outlined by Australia's eSafety Commissioner, highlighting principles of service provider responsibility, user empowerment and transparency and accountability, by having:[354]

- Partnered with UNICEF to set new standards, which are embedded in all aspects of the design and operation of the LEGO Life app
- Internal investment in pre-moderation of all user-generated content
- Ensuring there is no inadvertent sharing of a child's personal information
- Introduction of verified parental consent, explaining and empowering parents to manage their children's digital permissions
- Robust escalation safeguarding processes
- Transparent policies and reporting

LEGO has recently strengthened its Safety by Design approach by introducing 'Captain Safety', a character who provides a safety tutorial from the beginning and becomes the child's guide throughout the experience, delivering empowering safety messages at certain critical points, such as before sharing certain data or commenting on public posts.[355] In addition, as an aside and in further recognition of this issue, the LEGO Group launched a new resource for families called Small Builds for Big Conversations: a series of creative challenges, which offer parents and their kids an enjoyable, guided method to engage in conversations about being a good digital citizen and the importance of online safety, in a relatable way.[356]

[352] *While LEGO is tailored to an audience of children, it is the main case study of a platform fully embracing and implementing Safety by Design principles. However, other platforms have attempted to increasingly use similar principles when rolling out new features. An example of this is Twitter's 2019 announcement that the platform was seeking public feedback on a draft set of rules to govern how it would handle synthetic and manipulated media. This report highlights how Twitter's efforts with respect to synthetic and manipulated media align with the three key areas of Safety by Design thanks to both the content of the adopted rule and the process by which they developed in.*

[353] *World Economic Forum (2020), Ethical Principles for Digital Media and Technology Design in the New Normal.*

[354] *Ibid.*

[355] *Government of the United Kingdom (2019.*

[356] *World Economic Forum (2020).*

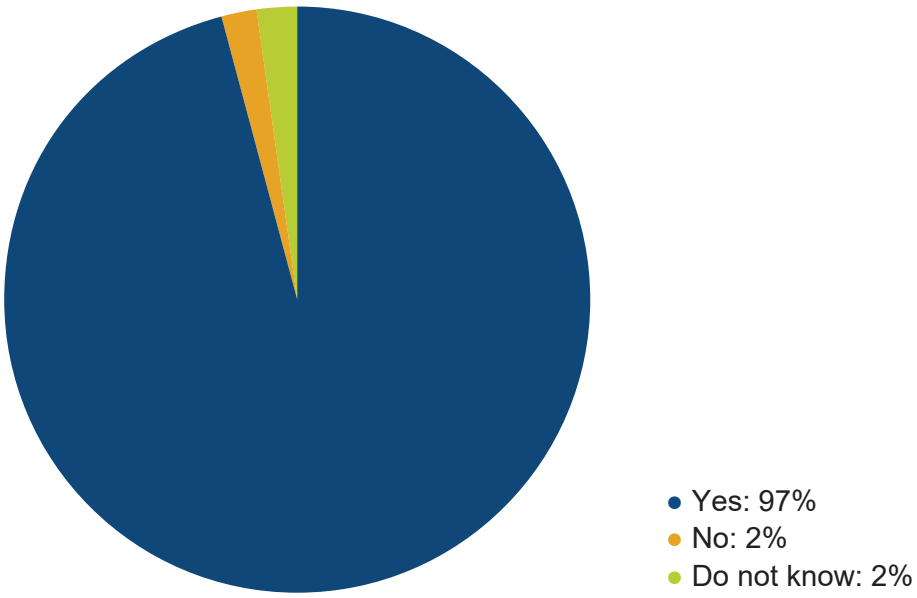
Annex 7. Public perception of E2EE: Survey

In order to improve our understanding of how the general public perceives end-to-end-encryption, Tech Against Terrorism launched a public survey on this topic. The survey was opened for two months from December 2020 to February 2021.

Overall, the results show a divide between the desire for secure and private online communication protected by encryption; and the need to mitigate risks of criminal use of encryption by ensuring law enforcement access to encrypted communication and metadata. The same divide is present when asking respondents whether they think content moderation is compatible with E2EE.

However, the recurrence of respondents stating that they do not know enough or have no opinion on the subject demonstrates the need to educate the general public about E2EE. In particular about the security and privacy of E2EE, and the risks of creating backdoors to or systematically monitoring encrypted communications.

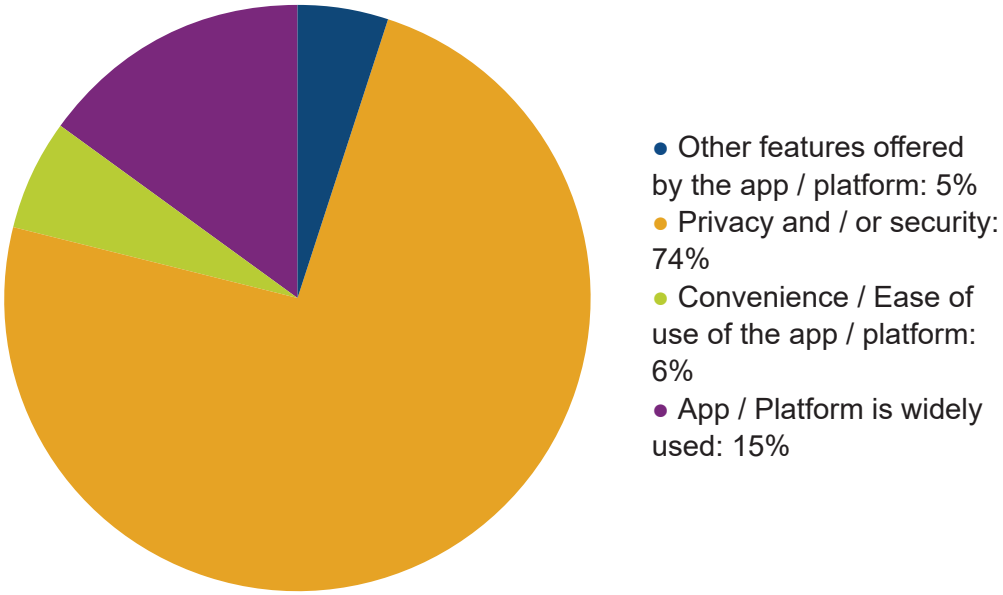
Do you use a messaging services offering end-to-end encryption (as a default or opt-in option) on a rugular basis?



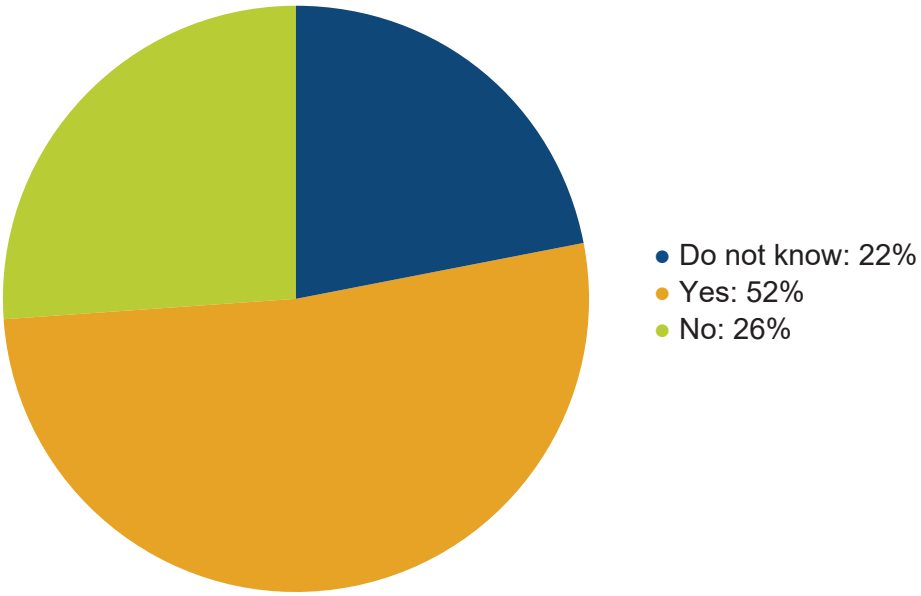
Amongst the encrypted messaging services used on a regular basis, the respondents listed the following:

- WhatsApp
- Signal
- iMessage
- Viber
- Telegram
- Session
- Facebook Messenger
- Wick
- Wire
- Keybase
- ProtonMail
- Zoom
- Threema
- Matrix – Element
- TutaNota

What most motivates you to use an encypted messaging services (EMS)?



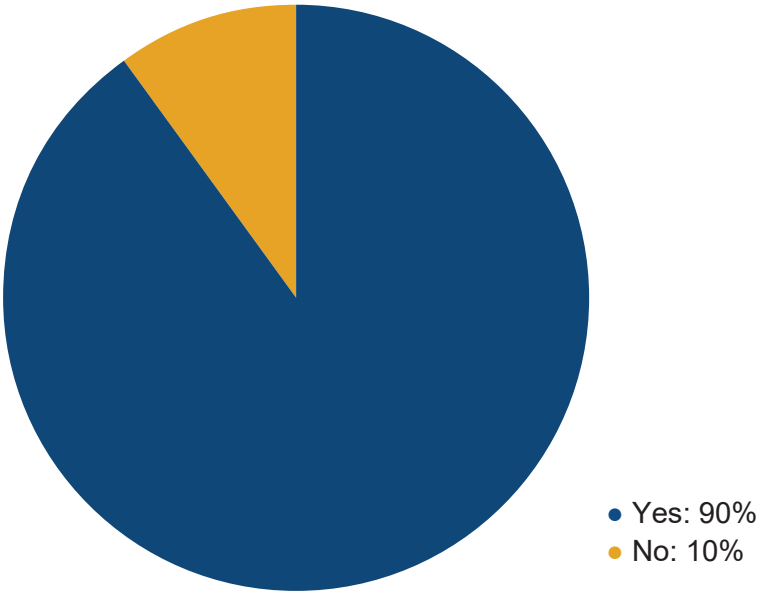
Besides EMS,do you use any other internet services that offers E2EE? If yes, which ones?



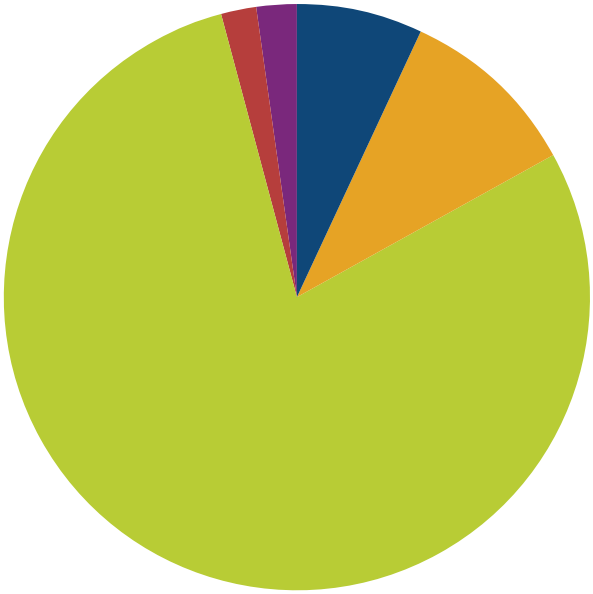
Amongst the encrypted services used, the respondents noted:

- Online banking
- Mega.nz
- onedrive
- Sync.com
- Cryptad
- Teams
- Gmail
- Secure drop
- GPG
- Facetime
- Zoom
- Instagram

Are you in favour of E2EE becoming the norm for online communications?

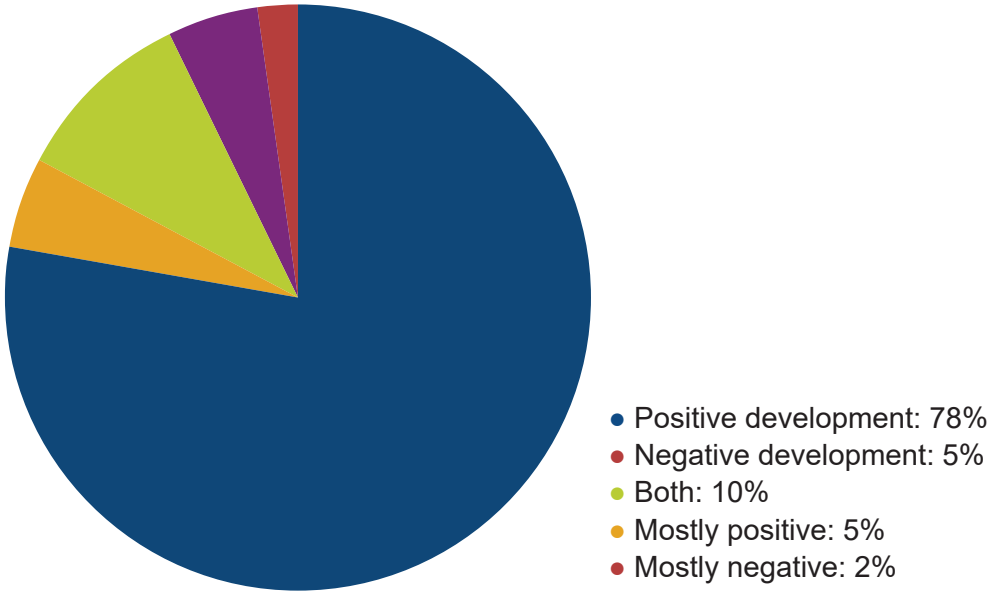


Why should E2EE be, not be, the norm for online communications?

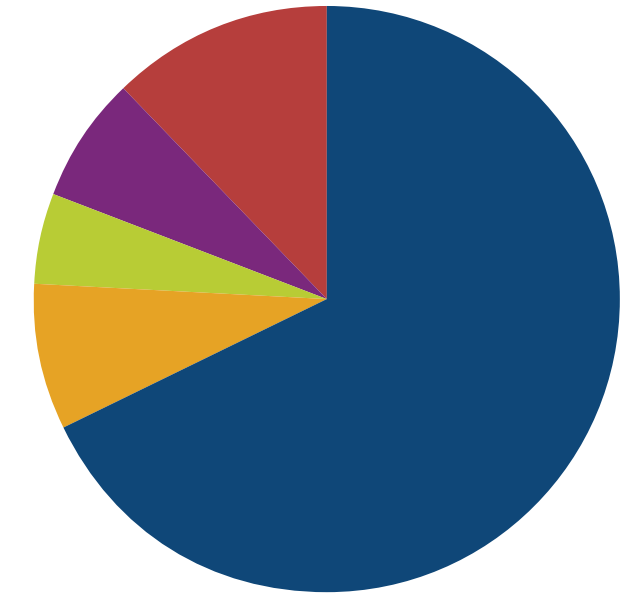


- Yes - To avoid commerical use of data: 7%
- No - Data shoudl be accessed for law enforcement or content moderation: 10%
- Yes - To ensure privacy and / or security: 79%
- No opinion / Do noyt know enough: 2%
- No - Not practical: 2%

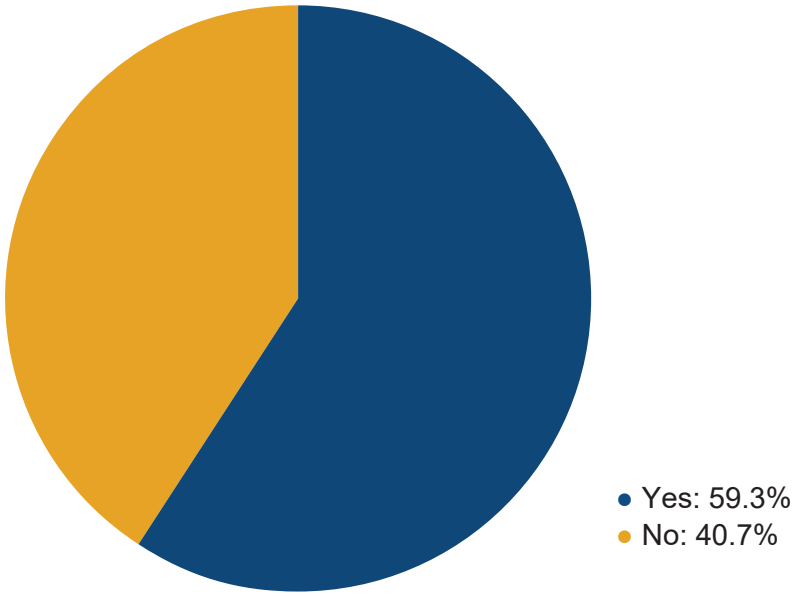
Do you see excryption, specifically E2EE, as a positive or negative development?



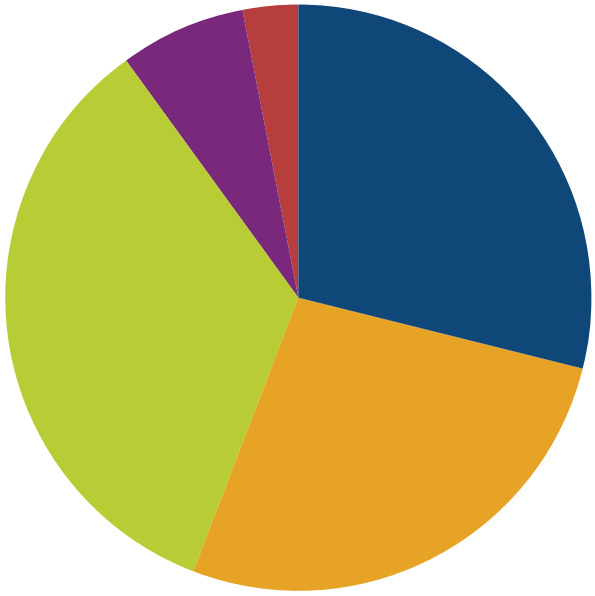
Does encryption further security or present increased security risks?



Do you think content moderation is compatible with E2EE?

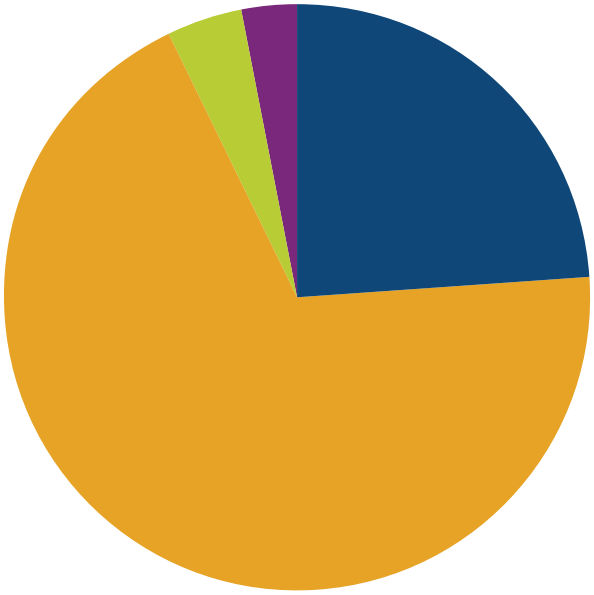


What do you think of existing proposals to moderate E2EE via hashing solutions and pre-encrption screenings?



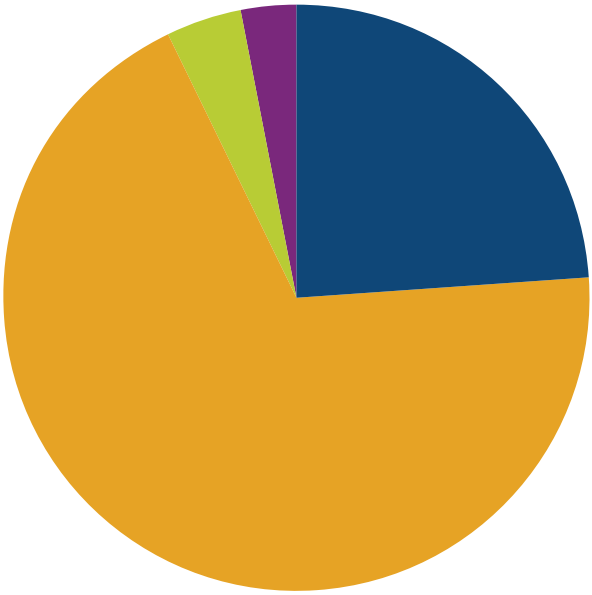
- Overall supportive: 29%
- No opinion / Don't know enough: 27%
- Overall against: 34%
- General support but concerns for security: 7%
- General support but moderation would have to be foolproof: 3%

Should law enforcement and governent have access to encrypted communications or decrypted communications data?



- Yes - encrypted content should be available for LE in principle:* 24%
- No - it presents too many risks: 69%
- Undecided: 4%
- There's a need to go beyond the encryption debate: 3%

Should metadata be encrypted or available for law enforcement?



- Yes - encrypted content should be available for LE in principle:* 24%
- No - it presents too many risks: 69%
- Undecided: 4%
- There's a need to go beyond the encryption debate: 3%

BIBLIOGRAPHY

General

Abelson H., Anderson R., Bellovin S., Benaloh J., Blaze M., Diffie W., Gilmore J., Green M., Landeau S., Neumann P., Rivest R, Schiller J., Schneier B., Specter M., Weitzner D. (2015), Key under doormats: mandating insecurity by requiring government access to all data and communications.

Abril Danielle (2019), Facebook 'Strongly Opposes' Reported Letter by AG Barr That Will Ask Mark Zuckerberg to Delay Encrypting Its App, Fortune.

AccessNow (2014), Google to enable end-to-end encryption for user emails.

AccessNow (2016), The FBI is out to undermine fundamental human rights. Access Now stands with Apple.

AccessNow and EDRi (2020), Response to the EU Draft Council Resolution.

Acharya Bhairav, Bankston Kevin, Schulman Ross and Thompson Andi Wilson (2017, revised in 2018), Deciphering the European Encryption Debate: Germany, New America.

Agraval Aditi (2019), WhatsApp sues Israeli spyware company NSO Group for planting spyware in users' devices, Medianama.

Agraval Aditi (2020), Encryption and issues related to Terrorism and Communications, Medianama.

Amnesty International (2020), Singapore: Social media companies forced to cooperate with abusive fake news law.

Apple (2016), A Message to Our Customers.

Arul R. (2016), Social Media and the Encryption Challenge, IDSA Comment.

Asia Internet Coalition (2020), Toolkit: Addressing Online Misinformation Through Legislation.

Barber Ian (2020), The UK Government's Full Response To The Online Harms White Paper: Initial Thoughts, Global Partners Digital.

BBC News (2018), Australia data encryption laws explained.

BBC News (2019), Pegasus breach: Will quitting WhatsApp make your phone safer?

Berger J.M and Perez Heather (2016), "The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters", GW Program on Extremism.

Bershidsky Leonid (2019), End-to-end encryption isn't as safe as you think, Bloomberg opinion.

Bertram Luke (2016), "Terrorism, the Internet and the Social Media Advantage", in Journal for Deradicalization, No. 7.

Bett Devlin (2018) , FBI repeatedly overstated encryption threat figures to Congress, public, The Washington Post.

Binance Academy (2020), What is End-to-End Encryption.

Boadle Anthony (2020), Brazil's Bolsonaro would veto bill regulating fake news in current form, Reuters; and Tulio dos Santos Diogo (2021), Brazil, democracy, and the "fake news" bill, Global Americans.

Borger Julian, Rankin Jennifer, Lyons Kate (2017), The rise and rise of international diplomacy by WhatsApp, The Guardian.

Brewster Thomas (2017), Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops, Forbes.

C. John (2020), "Most secure messaging apps on the market in 2020", AtlasVPN.

Cadwalladr Carole and Graham-Harrison Emma (2018), Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian.

Cambridge Consultants for OfCom (2019), Use of AI in Online Content Moderation.

Campbell Ian Carlos (2021), WhatsApp is having another go at explaining its privacy policy to users, The Verge.

Campbell Natalie (2020), Announcing the Launch of the Global Encryption Coalition, The Internet Society.

Campbell Natalie (2021), Don't Make Parents Raise Kids in a World Without Encryption, Internet Society.

Cardozo Nate and Schoen Seth (2019), Detecting Ghosts By Reverse Engineering: Who Ya Gonna Call?, Lawfare.

Center for Democracy & Technology (2019), Open Letter: Facebook's End-to-End Encryption Plans.

Cerulus Laurens (2020), EU Commission to staff: Switch to Signal messaging app, Politico.

Chen Siyuan and Chia Chen Wei (2019), Singapore's latest efforts at regulating online hate speech, Institutional Knowledge at Singapore University.

Clifford Bennet and Powell Helen (2019), Encrypted Extremism Inside the English-speaking Islamic State Ecosystem on Telegram, George Washington Programme on Extremis.

Cloudflare, Why Use HTTPs?

Cohn-Gordon K., Cremer C., Dowling B., Garratt L., Stebila D., (2019), A Formal Security Analysis of the Signal Messaging Protocol.

Cohn Cindy (2018), Resisting Law Enforcement's Siren Song: A Call for Cryptographers to Improve Trust and Security, Lawfare.

Cohn Cindy (2020), Eight Epic Failures of Regulating Cryptography, Electronic Frontier Foundation.

Collier Kevin (2019), Jared Kushner's use of WhatsApp raises concerns among cybersecurity experts, CNN.

Conway Maura, Parker Jodie and Looney Sean (2017), "Online Jihadii Instructional Content: The Role of Magazines", in Terrorist Use of the Internet and Cyberspace: Issues and Responses, Conway et al. (Eds.), IOS press, pp.182-193

Conway Maura, Scrivens Ryan, Macnair Logan (2019), "Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends", International Centre for Counter-Terrorism.

Cordozo Nate (2018), Pushing back against backdoors: 2018 year in review, Electronic Frontier Foundation.

Covington and Burling LLP (2020), Lawful Access to Encrypted Data Act Introduced, Lexicology.

Cox Joseph (2020), How Police Secretly Took Over a Global Phone Network for Organized Crime, Vice News.

Croker Andrew (2019), DOJ And FBI show no signs of correcting past untruths in their new attacks on encryption, Electronic Frontier Foundation.

Cuthbertson Anthony (2021a), WhatsApp sees sudden drop in downloads as millions turn to Telegram and Signal, The Independent.

Cuthbertson Anthony (2021b), WhatsApp Forces Users to Agree to Share Private Data Including Phone Number With Facebook, The Independent.

David Ruiz (2018), There's no middle ground on encryption, Electronic Frontier Foundation.

Davies Anne (2020), Angus Taylor v Clover Moore: WhatsApp messages reveal panic as minister's staff realised figures were wrong, The Guardian.

De Guzman Noelle Francesca (2020), Kids need encryption too, Internet Society.

Deck Andrew and Elliot Vittoria (2021), How Line is fighting disinformation without sacrificing privacy, Rest of World.

Devlin Bett (2018), FBI repeatedly overstated encryption threat figures to Congress, public, The Washington Post.

Diaz Angel (2019), Global Internet Forum to Counter Terrorism's 'Transparency Report' Raises More Questions Than Answers, Just Security.

Dodis Yevgeniy, Grubbs Paul, Ristenpart Thomas, Woodgae Joanne (2019), Fast message franking: from invisible salamander to encryptment.

Dofman Zack (2021), WhatsApp Beaten By Apple's New iMessage Privacy Update, Forbes.

Duckett Chris (2020), Labor Bill to fix Australian encryption laws it voted for hits second debate, ZDNet.

Dussutour Chloe (2020a), European Commission to use open source messaging service Signal, JoinUp

Dussutour Chloe (2020b), French government launches in-house developed messaging service, Tchap, JoinUp.

Electronic Frontier Foundation (2016), EFF to Support Apple in Encryption Battle.

Electronic Frontier Foundation – Surveillance Self-Defense (2018), What should I know about Encryption.

Elmer-Dewitt Philip (2016), Apple's Tim Cook Says 'Going Dark' Is a Crock, Fortune.

EncroChat website: https://encro.co.uk/

European Data Protection Supervisor (2020), Opinion on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online.

Europa Nu (2015), EU wants internet firms to hand over encryption keys.

Eurojust/Europol (2020), Le démantèlement d'un réseau crypté crée une onde de choc au sein des groupes criminels organisés à travers l'Europe.

Facebook (2019), Using AI to keep the platform safe.

Facebook Newsroom (2019), Facebook's Response to Open Letter on Private Messaging.

Facebook Newsroom (2021), Expanding Support for Security Keys on Mobile Devices.

Facebook Messenger News (2020), Preventing Unwanted Contacts and Scams in Messenger.

Farivar Cyrus (2020), "Feds announce largest seizure of cryptocurrency connected to terrorism", NBC News.

Filippone Dominique (2020), Comment la Gendarmerie Nationale a fait tomber EncroChat, Le Monde Informatique.

Fitsanakis Joseph (2020), "As ISIS goes online due to COVID-19, it publishes a new cybersecurity magazine", Intelnews.org.

Flade Florian (2016), „Dann knallen wir eine Moschee nach der anderen hoch", Welt.de

Fortiguard SE Team (2018), As the Holiday Season Draws Near, Mobile Malware Attacks Are Prevalent, Fortinet.

Franceschi-Bicchierai Lorenzo (2014), The 10 biggest revelations from Edward Snowden's Leaks, Mashable.

FranceInfo (2021), On vous explique l'opération "Ulysse", la cyber-infiltration de la DGSI qui a permis de déjouer un projet d'attentat en France.

Feiner Lauren (2020), Republican senators introduce bill that tech advocates have warned would weaken privacy, CNBC.

Gange David (2020), Boris Johnson and Emmanuel Macron's WhatsApp messages on quarantine-free travel blindsided officials, UK News Today.

Garcia Paulo (2019), U.K. proposal to 'Bcc' law enforcement on messaging apps threatens global privacy, The Conversation.

Garrick Law (2020), Encrochat Encrypted Telephones Hacked June 2020 – Drugs, Telephones, NCA Police & Searches.

Gaudette Tiana, Scrivens Ryan, Venkatetsh Vivvek (2020), The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists, Terrorism and Political Violence

Gay Mara (2017), Messaging App Has Bipartisan Support Amid Hacking Concerns, The Wall Street Journal.

Georgina Petcu Alina (2020), Is Telegram Secure? What You Need to Know Before Downloading the App, Heimdal Security.

Global Encryption Coalition, About Global Encryption Coalition.

Global Partners Digital, Encryption Policy Hub.

Global Web Index (2020), Messaging Apps: Understanding the potential of messaging apps for marketers.

Gorman Doug (2020), The new privacy landscape, Global Web Index.

Graham Robert (2016), How Terrorists Use Encryption, CTC Sentinel.

Greenberg Andy (2017), After 3 Years, Why Gmail's End-to-End Encryption Is Still Vapor, Wired.

Greenberg Andy (2020), Facebook Says Encrypting Messenger by Default Will Take Years, Wired.

Greenberg Andy (2020), Signal is Finally Bringing Its Secure Messaging to the Masses, Wired.

Griffin Andrew (2021a), WhatsApp Halts Rollout of Controversial Privacy Policy Update, The Independent.

Griffin Andrew (2021b), The Encryption Debate Is About All of Our Personal Messages – And That Must Be Acknowledged, The Independent.

Grossman Lev (2016), Inside Apple CEO Tim Cook's Fight With the FBI, The Time.

Hacot Valerie (2019), Messageries : plutôt WhatsApp à Matignon et Telegram à l'Elysée, Le Parisien.

HashedOut (2019), End-to-End Encryption: The Good, the Bad and the Politics.

Hayden Michael (2019a), Encryption Backdoors Won't Stop Crime But Will Hurt U.S. Tech, Bloomberg Opinion.

Hayden Michel (2019b), “Far-Right Extremists Are Calling for Terrorism on the Messaging App Telegram”, Southern Poverty Law Center.

HelpNetSecurity (2018), Cybercriminals are turning to Telegram due to its security capabilities.

Hern Alex (2015), Tech firms warn snooper’s charter could end strong encryption in Britain, The Guardian.

Hern Alex (2016), Technology firms’ hopes dashed by ‘cosmetic tweaks’ to snooper’s charter, The Guardian.

Hern Alex (2017), UK government can force encryption removal, but fears losing, experts say, The Guardian.

Hope Not Hate, (2020), “The Terrorgram network: a spiral towards bloodshed” in 2020 State of Hate Report.

Hutchens Gareth (2018), Leaked WhatsApp messages reveal Julie Bishop’s leadership bid scuppered by colleagues, The Guardian.

Internet Freedom India (2021), Latest Draft Intermediary Rules: Fixing big tech, by breaking our digital rights?.

Internet Society and the Global Encryption Coalition (2020), Breaking encryption myths What the European Commission’s leaked report got wrong about online security.

Internet Society, signed by a group of experts from the Global Encryption Coalition (2020). Breaking encryption myths What the European Commission’s leaked report got wrong about online security.

IronMarch Exposed: https://www.ironmarch.exposed/

Iqbal Mansoor (2020), WhatsApp Revenue and Usage Statistics (2020), Business of App.

Johnson Bridget (2019), “New ISIS Project Launched to Beef Up Jihadists’ Cyber Skills, Security Awareness”, Homeland Security Today.

Jovanovic Bojan (2020), What is End-to-End Encryption, Dataprot.net.

Kahney Leander (2019), The FBI wanted a backdoor to the Iphone, Tim Cook said no, Wired

Karstenn Jack and West Darrel (2016), A Brief History of U.S Encryption Policy, Brookings.

Kavanagh Camino, Carr Madeline, Bosco Francesco and Hadley Adam (2017), “Terrorist use of the internet and cyberspace: issues and responses”, in Terrorist’ Use of the Internet, Conway Maura et al. (Eds), IOS Press.

Kenber Billy and Parker Charlie (2020), Matt Hancock’s neighbour won £30m deal to supply vials for Covid tests, The Times.

Kirchgaessner Stephanie (2020), Jeff Bezos hack: Amazon boss’s phone ‘hacked by Saudi crown prince’, The Guardian.

Koch Richie (2020), Massive corporate databases become government tools of surveillance, ProtonMail Blog.

Koebler Jason (2016), FBI's iPhone Backdoor May Violate International Law, Says UN Human Rights Rep, Vice News.

Lamoureux Mark and Makuch Ben (2020), Inside a Neo-Nazi Terror Cell as It Reckons With FBI Arrests, Vice News.

Lamoureux Mack, Makuch Ben and Kamel Zachary (2020), How One Man Built a Neo-Nazi Insurgency in Trump's America, Vice News.

Langkemper Sjoerd (2019), Breaking message franking.

Lee Micah (2016), Battle Of The Secure Messaging Apps: How Signal Beats WhatsApp, The Intercept.

Leetaru Kalev (2019a), Facebook is already working towards Germany's End-to-End Encryption Backdoor Vision, Forbes.

Leetaru Kalev (2019b), The Encryption Debate Is Over - Dead At The Hands Of Facebook, Forbes.

Levine Mike (2019), FBI arrests Army soldier who allegedly discussed plans to bomb major American news network ABC News.

Levy Ian and Robison Crispin (2018), Principles for a more informed exceptional access debate, Lawfare.

Lewis James A., Zheng Denise E., Carter William A. (2017), The Effect of Encryption on Lawful Access to Communications and Data, Center for Strategic and International Studies.

Liguori Carlos (2020), Exploring lawful hacking as a possible answer to the "going dark" debate, Michigan Technology Law Review.

Lipp Sebastian and Hoppenstedt and Max (2016), Exklusiv: Wie das BKA Telegram-Accounts von Terrorverdächtigen knackt, Vice News.

Loedenthal Michael (2020a), "Evolving Digital OPSEC Practices Amongst Far-Right Networks", Global Network on Extremism and Technology.

Loedenthal Michael (2020b), "Digital Resiliency and OPSEC Strategies Amongst Clandestine Networks", Global Network on Extremism and Technology.

Lomas Natasha (2016), "WhatsApp completes end-to-end encryption rollout", TechCrunch

Macdonald Stuart and Staniforth Andrew (2021), The Tech Industry And The Regulation Of Online Terrorist Content: What Do Law Enforcement Think?, Hedayah.

Makena Kelly (2020), A weakened version of the EARN IT Act advances out of committee, The Verge

Mahlmann Ariel (2019), End-to-End Encryption Strategies Becoming the Norm for Social Media, Fornetix.

Makuch Ben (2019), "The Nazi-Free Alternative to Twitter Is Now Home to the Biggest Far Right Social Network", Vice News.

Mari Angelica (2019), UK introduces world's first online safety regulations, Computerweekly.com.

Marr Bernard (2019), What Is Homomorphic Encryption? And Why Is It So Transformative?, Forbes.

Martin Nick R. (2020), Heartland terror: The FBI said Timothy Wilson planned to blow up a hospital in Missouri. Before that, he was active in online chats for two neo-Nazi groups. The Informant.

Masnick Mike (2013), Anyone Brushing Off NSA Surveillance Because It's 'Just Metadata' Doesn't Know What Metadata Is, TechDirt.

Masnick Mike (2019), The DOJ Is Conflating The Content Moderation Debate With The Encryption Debate: Don't Let Them, TechDirt.

Masnick Mike (2020), New EARN IT Act Creates An Insane New Dilemma: Either Encrypt All Or Spy On All, TechDirt.

Mastodon (2019), "Statement on Gab's fork of Mastodon".

Matsakis Louise and Hay Newmann Lily (2020), Everything We Know About the Jeff Bezos Phone Hack, Wired.

Mayer Jonathan (2019), "Content Moderation for End-to-End Encrypted Messaging", Princeton University.

Mazzoni Valerio (2019), "Far Right extremism on Telegram: A brief overview", European Eye on Radicalization.

McCullough Patrick (2021), EARN IT and LAEDA: How Private Is Too Private?, Reporter Magazine

Meister Andre (2020), Anti-Terror-Koordinator der EU fordert Gesetz gegen Verschlüsselung, NetzPolitik.org.

Meleagrou-Hitchens Alexander and Hughes Seamus (2017), The threat to the United States from the Islamic State's virtual entrepreneurs, CTC Sentinel.

Meserole and Polyakova (2019), "Exporting Digital Authoritarianism". The Brookings Institution.

Mihindukulasuriya Regina (2019), Prying government eyes drive politicians, terrorists to WhatsApp, Telegram, Signal, The Print.

Moechel Erich (2020), Auf den Terroranschlag folgt EU-Verschlüsselungsverbot, Radio FM4.

Monroy Matthias (2019), New Technologies: Europol sets up an „Innovation Laboratory".

Morrison Sara (2020), The Jeff Bezos Hack Could Happen To Anyone, Vox.

Mullin Joe (2019), Carnegie experts should know: defending encryption isn't an "absolutist" position, Electronic Frontier Foundation.

Mullin Joe (2020), The New EARN IT Bill Still Threatens Encryption and Free Speech, Electronic Fronter Foundation.

Newton Casey (2019), How the spread of child abuse imagery online is changing the debate over encryption, The Verge.

Newton Casey (2020), India's proposed internet regulations could threaten privacy everywhere, The Verge.\

Nojem Greg (2020), CDT Helps Lead Launch of the Global Encryption Coalition, Center for Democracy and Technology.

Ong Thuy (2017), WhatsApp reportedly refused to build a backdoor for the UK government, The Verge.

Open Technology Institute, at New America, (2019), Open Letter to GCHQ on the Threats Posed by the Ghost Proposal, Lawfare.

Open Technology Institute, at New America, (2019), Open Letter to GCHQ on the Threats Posed by the Ghost Proposal

Owen Tess (2019), How telegram became White Nationalists' go-to messaging platform, Vice News.

O'Brien Danny (2020), Orders from the top: The EU's timetable for dismantling End-to-End encryption, Electronic Frontier Foundation.

Pelroth Nicole (2019), "What Is End-to-End Encryption? Another Bull's-Eye on Big Tech", The New York Times.

Pickworth Jonathan and Hickman Tim (2016), Investigatory Powers Act 2016 becomes law, White & Case.

Pixel Privacy, Encrypted Messaging: What is it, why you should use it and what are the best apps.

PKWARE , Client-Side Encryption vs. End-to-End Encryption: What's the Difference?,

Polk Ryan (2020), European Union, Use Facts to Make Cybersecurity Decisions – Not Myths, Internet Society.

Poortvliet Jos (2018), What is End-to-End Encryption and Why Does it Matter, NextCloud.

Porter Jon (2020), Signal Becomes European Commission's messaging app of choice in security clampdown, The Verge.

Portnoy Erica (2019), Why adding client-side scanning breaks end-to-end encryption, The Electronic Frontier Foundation.

Privacy International (2021), "UK mass interception laws violates human rights and the fight continues..."

ProtonMail About, We're building an internet that protects privacy, starting with email.

ProtonMail (2018), What is end-to-end encryption and how does it work?

Puranik Marty (2017), Tim Cook was right to fight the FBI, The Next Web.

PYMNTS.com (2020), India's New Social Media Rules Would Strip Anonymity — When Asked — From Accounts.

Radsch Courtney (2020), GIFCT: Possibly the Most Important Acronym You've Never Heard Of, JustSecurity.

Rai Saritha (2020), 400 Million Social Media Users Are Set to Lose Their Anonymity in India, Bloomberg.

Rebiger Simon (2016), Bundeskriminalamt knackt 44 Telegram-Accounts in zwei Jahren, Netzpolitik.

Riley-Smith Ben and Hope Christopher (2020), Boris Johnson communicated with Saudi crown prince on WhatsApp, ex-UK officials say, The Telegraph.

Robertson Adi (2021), India sets stricter rules for social media giants, The Verge.

Rodriguez Kattza and Schoen Sean (2020), FAQ: Why Brazil's Plan to Mandate Traceability in Private Messaging Apps Will Break User's Expectation of Privacy and Security.
Rotella Sebastian (2016), ISIS via WhatsApp: 'Blow Yourself Up, O Lion', ProPublica.

Rozenshtein Alan Z. (2019), Child Exploitation and the Future of Encryption, Lawfare.

Ruiz David (2018), There is no middle ground on encryption, Electronic Frontier Foundation.

Rukmini Callimachi (2017), How a couple's dream trip ended in tragedy at the hands of ISIS, Independent.

Schulman Ross and Bankston Kevin (2017), Deciphering the European Encryption Debate: France, New America.

Schulman Ross (2019), Why the Ghost Keys 'Solution' to Encryption is No Solution, JustSecurity.

Schulz Wolfgang, and van Hoboken Joris (2016), Human Rights and Encryption, UNESCO Publishing.

Shaw Danny (2020), Hundreds arrested as crime chat network cracked, BBC News.

Speckhard Anne and Yaila Ahmet S (2017), Telegram: The Mighty Application That ISIS Loves – Part I, Vox-Pol.

Speckhard Anne and Bodo Lorand (2018), "Fighting IS on Facebook – Breaking ISIS brand counter-narratives project", ICSCVE Research Reports.

Speckhard Anne and Ellenberg Molly (2020), "Inside the Sisterhood Springing Jihadis From Jail", The Daily Beast

Squire Megan (2020), "Alt-tech & the radical right, part 3: why do hate groups and terrorists love Telegram?", Centre for Analysis of the Radical Right.

Stepanovich Amie (2016), A Human Rights Response to Government Hacking, AccessNow.

Signal (2018), Setback in the Outback.

Singh Manish(2020), WhatsApp is now delivering roughly 100 billion messages a day, TechCrunch.

Smith Adam (2021), WhatsApp Privacy Controversy Leads Company to Take Out Full-Page Adverts Asking Users to Stay, The Independent.

Stanford Internet Observatory (2019), Workshop – Mitigating abuse in an end-to-end world, Stanford Internet Observatory.

Statt Nick (2021), WhatsApp clarifies it's not giving all your data to Facebook after surge in Signal and Telegram users, The Verge.

Suc Matthieu (2021a), Au procès «Ulysse», les zones d'ombre de la cyber-infiltration subsistent, Mediapart.

Suc Matthieu (2021b), «Ulysse» et les djihadistes, les dessous d'un attentat empêché, Mediapart.

Tech Against Terrorism (2019a), "Insights from Europol's 2019 European Counter Terrorism Centre Advisory Network Conference".

Tech Against Terrorism (2019b), "ISIS use of smaller platforms and the DWeb to share terrorist content".

Tech Against Terrorism (2019c), Analysis: The use of open-source software by terrorists and violent extremists

Tech Against Terrorism (2021a), The Online Regulation Series Handbook.

Tech Against Terrorism (2021b), Content personalisation and the online dissemination of terrorist and violent extremist content.

Telegram –Secret chats: https://telegram.org/faq#secret-chats

The Indian Express (2019), WhatsApp Pegasus attack: Signal, Wire and other apps that offer end-to-end encryption.

The Internet Society, Encryption.

The SSLS Store (2019), Homomorphic Encryption.

The Telegraph (2019), Facebook's Zuckerberg defends decision on encryption.

Tsavkko Garcia Raphael (2020), Brazil's "fake news" bill won't solve its misinformation problem, MIT Technology Review.

United Nations, Office of the High Commissioner for Human Rights (2018) The Right to Privacy in the Digital Age.

United Nations Office on Drugs and Crime – UNODC (2012), The use of the internet for terrorist purposes.

United Nations Office on Drugs and Crime – UNODC (2018), Privacy, investigative techniques and intelligence gathering.

Untersinger Martin, (2016), Que reproche-t-on au TES, le “mégafichier” des 60 Millions de Français ?, Le Monde.

Unuth Nadeem (2019), What is End-to-End Encryption, Lifewire.

Walker Shaun, Kirchgaessner Stephanie, Lakhani Nina and Safi Michael (2021), Pegasus Project: spyware leak suggests lawyers and activists at risk across globe, The Guardian.

Waterson Jim (2019), Tories switch to messaging app Signal after WhatsApp leaks, The Guardian.

WhatsApp (2021), How WhatsApp Helps Fight Child Exploitation.

Wingfield Richard (2020), The UK’s Online Harms Bill: Potential Implications for the Right to Privacy, The GNI Blog.

Wintour Patrick (2016), Internal report slams culture in UK Foreign Office, The Guardian.

Wooley Samuel (2020), Encrypted Messaging Apps are the Future of Propaganda, Brookings – Tech Stream

Yadron Danny (2016), Apple CEO Tim Cook: FBI asked us to make software ‘equivalent of cancer’, The Guardian.

ZDnet (2018), What’s actually in Australia’s encryption laws? Everything you need to know.

Zoom (2020), 90-Day Security Plan Progress Report: July 1.

Zuckerberg Marc (2019), A Privacy-Focused Vision for Social Networking, Facebook Newsroom.

Statistics

99Firms (2019), Most Popular Messaging Apps.

BondCap Internet Trends 2019

Buckle Chase (2016), 2 in 3 Messenger users worried about personal data, Global Web Index.

Bucher Birgit (2020), WhatsApp, WeChat and Facebook Messenger Apps – Global useage of Messaging Apps, Penetration and Statistics, MessengerPeople.

Clement J. (2020a), Viber: number of registered user IDs 2011-2020, Statista.

Clement J. (2020b), Daily active users of Snapchat 2014-2020, Statista.

Google, HTTPS Encryption on the Web.

Messenger People, WhatsApp, WeChat and Facebook Messenger Apps – Global useage of Messaging Apps, Penetration and Statistics.

Rainie Lee and Madden Mary (2015), Americans' Privacy Strategies Post-Snowden, Pew Research Centre.

Statista, Enterprise-wide encryption solution usage worldwide 2012-2019.

Statista, Most popular global mobile messenger apps as of October 2020, based on number of monthly active users.

Statista (2020), LINE – Statistics & facts.

United Nations Human Rights, Office of the High Commissioner (2014), The right to privacy in the digital age.

United Nations Human Rights, Office of the High Commissioner, International Standards.

Waldeck Yasmin (2020), Number of monthly active users of KakaoTalk in South Korea 2015-2020, Statista.

Windwehr Svea and York Jillian (2020), One Database To Rule Them All, Vox-Pol.

World Economic Forum (2020), Ethical Principles for Digital Media and Technology Design in the New Normal.

Woods Andrew (2017), Encryption Substitutes, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1705.

Legislations impacting encryption and related governments' statements

Australian Department of Home Affairs, The Assistance and Access Act 2018.

Australian Department of Home Affairs, Assistance and Access: Overview; The Assistance and Access Act 2018.

Brazil, Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, The Brazilian Internet Freedom, Responsibility and Transparency Act, or Law PLS2630/2020.

Council of the European Union, EU Counter-Terrorism Coordinator (2015), EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015.

Council of the European Union, EU Counter-Terrorism Coordinator (2015), EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015.

Council of the EU (2020), Draft Council Resolution on Encryption - Security through encryption and security despite encryption.

Council of the EU (2021), Confidentiality of electronic communications: Council agrees its position on ePrivacy rules.

Department for Digital, Culture, Media and Sport (2020), Development of 'Safety by Design' Guidance for Online Platforms, Government of the United Kingdom.

EU Commission (2020a), Leaked report on technical solutions to detect child sexual abuse in end-to-end encrypted communications.

EU Commission, Commissioner Johansson (2020), Speech by Commissioner Johansson at a webinar on "Preventing and combating child sexual abuse & exploitation: towards an EU response".

EU Commission (2020b), Proposal for a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC.

European Commission (2020c), EU strategy for a more effective fight against child sexual abuse

European Data Protection Supervisor (2020), Opinion on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online.

European Parliament Research Services (2021), Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse – Targeted Substitute Impact Assessment.

Europol (2019), Written contribution to JPSG – The Europol Innovation Lab.

Europol (2020), Dismantling of An Encrypted Network Sends Shockwaves Through Organised Crime Groups Across Europe.

eSafety Commissioner (2019), Safety by Design Overview, Government of Australia.

Five Country Ministerial (2019), Joint Meeting of FCM and Quintet of Attorneys-General.

Government of the United Kingdom (2019), Online Harms White Paper.

Governments of the United States, United Kingdom, and Australia (2019), Open Letter: Facebook's "Privacy Frist" Proposals.

Governments of the United Kingdom, United States, Australia, New Zealand, Canada, India and Japan (2020), International Statement: End-To-End Encryption and Public Safety.

Inman-Grant Julie, Australian eSafety Commissioner (2020), End-to-end encryption: a challenging quest for balance.

US Department of Justice (2019), Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security.

US Department of Justice (2020), International statement: End-to-end encryption and public safety.

US Senate, Committee on the Judiciary (2020), Graham, Cotton, Blackburn Introduce Balanced Solution to Bolster National Security, End Use of Warrant-Proof Encryption that Shields Criminal Activity.

United Kingdom Government, Investigatory Power Act 2016.

United Kingdom Government, Investigatory Powers (Codes of Practices) Regulations 2018.

United Kingdom Government, Interception of Communications Code of Practice (2018).

United Kingdom Government (2019), Online Harms White Paper.

United Kingdom Government (2020), Online Harms White Paper: Full government response to the consultation.

UK National Crime Agency (2020), NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation.

Sen. Graham, Lindsey, EARN IT Act, The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2019, Congress.gov.

Encryption technical whitepapers

Apple Platform Security: iMessage overview

Conversations, OMEMO Multi-End Message and Object Encryption.

FortKnoxster (2019), What happens in FortKnoxster – stays in FortKnoxster.

Jefferys Kee, Shishmarev Maxim, Harman Simon (2020), Session: A Model for End-To-End Encrypted Conversations With Minimal Metadata Leakage.

LINE (2016), Encryption Overview Technical White Paper.

Google Security Blog (2014), Making end-to-end encryption easier to use.

Khron Max (2020), Zoom Rolling Out End-to-End Encryption Offering, Zoom Blog.

Threema (2020), Cryptography Whitepaper.

Viber Encryption Overview.

WhatsApp (2020), Encryption Overview Technical White Paper.

Wickr (2017), Wickr Messaging Protocol Technical Paper.

Wire (2020), Security White Paper.

Zoom, End-to-End Encryption Whitepaper.

Zoom (2021), Encryption Whitepaper.