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

REPORT SUMMARY

tech against terrorism

BACKGROUND

Tech Against Terrorism's report on "Terrorist Use of E2EE: State of Play, Misconceptions, and Mitigation Strategies" provides a comprehensive overview of the risks and mitigation strategies related to the abuse of services offering end-to-end encryption (E2EE) by terrorists and violent extremists.

For this report, Tech Against Terrorism consulted over 160 publicly available reports, articles, whitepapers, and legislations related to the use of encryption, particularly end-to-end encryption, and the associated risks of criminal actors exploiting such technology. In addition, we interviewed five encryption experts from the civil society and tech sectors.

This policy paper summarises the key findings from the report.

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

KEY FINDINGS FROM THE REPORT

1. **User concerns over online privacy and misuse of data have driven an increase in E2EE offering by online communications providers** in particular messaging services. As a result, most leading messaging services now offer E2EE as a default or opt-in.

2. **Privacy has become a competitive advantage for tech companies** who have incorporated the privacy argument into their branding and public-facing communication.

3. **Messaging services represent the second most common online activity**, with users increasingly favouring private messaging services to social media.[1]

4. **Despite user demand for E2EE, policymakers and law enforcement agencies have made calls to reign in E2EE use**, often motivated by concerns over criminal exploitation of E2EE technology. For example, governments have called for the introduction of so-called backdoors to counter terrorist use of E2EE and have asked that companies monitor their platforms to detect child sexual abuse material.

5. **Encryption experts, digital rights advocates, and tech companies all agree that there is no safe backdoor to encryption**. Instead, any backdoor would create more security risks, including for individual users, than it would solve. Any friction in the message transmission chain, or security vulnerabilities in the encryption protocol, risks being exploited by adversarial (state and non-state) actors.

6. **Backdoors to and monitoring of encrypted communications raise significant jurisdictional questions and present a significant infringement on the fundamental right to privacy.**

7. **Legal requirements for backdoors or monitoring will set a dangerous precedent for online privacy.**

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

8. Contrary to the rationale underpinning policymakers' calls for backdoors, **E2EE is not in and of itself a crucial feature for terrorists when deciding to establish themselves on an app or platform**. Terrorists assess several features of platforms before deciding to establish a presence, including usability, stability, security, and audience reach.

9. To counter criminal use of E2EE, **we need to go beyond the "encryption debate"** which juxtaposes a misperception of E2EE features causing or leading to criminal and/or terrorist activity on one side against heavy handed interventions that risk harming security protocols and the right to privacy on the other. Instead, countering criminal use of E2EE should be done alongside the safeguarding and strengthening of online security protocols. Further, law enforcement should consider innovative online investigation techniques to adapt to the digital space. Human intelligence (HUMINT) and open-source intelligence (OSINT) techniques can be combined for this purpose. Tech platforms can on their part explore metadata analysis, network analysis, and link analysis as privacy-compliant solutions for detecting criminal actors using E2EE services.

TECH AGAINST TERRORISM'S RECOMMENDATIONS

Tech Against Terrorism strongly warns against the introduction of the tools proposed by policymakers to moderate encrypted content reviewed in the report. This includes homomorphic encryption**.** Whilst permitting for analysis of encrypted content, homomorphic encryption still allows for the systematic screening of user content which contradicts the privacy promise of E2EE.

We recommend governments:

1. Ensure that any proposals regarding countering abuse of E2EE communications:
    - o Are anchored in the rule of law.
    - o Do not violate fundamental freedoms.
    - o Provide clear guidelines for any legal requirements imposed on tech companies.

2. Ensure that appropriate redress mechanisms exist for individuals whose rights have been compromised as a result of government monitoring efforts.

3. Clarify what evidence exists of E2EE significantly impeding the work of law enforcement with regards to counterterrorism investigations.

4. Publish regular transparency reports on removal, user information, preservation, and other requests issued by government and law enforcement entities to tech companies, in line with the Tech Against Terrorism Guidelines on Transparency Reporting on Online Counterterrorism Efforts for Governments.

We recommend that tech companies:

Publicly commit to end-to-end encryption:

1. Increase knowledge sharing and public communication around the benefits of encryption and about the inherent risks of backdoors to (and systematic monitoring) of encrypted channels content. With regards to risks, particular focus should be placed on:
    - o Impact on users' right to privacy and freedom of expression.
    - o Security risks for all users, including exploitation of these risks by criminals, terrorists, and adversarial state actors.
    - o Questions relating to the scope of application.
    - o The risks associated with vague terminology used in legislation and related risks for increased surveillance of private communications in the future.
    - o Risks of mass surveillance of user communications.

2. Emphasise that there is no guarantee that backdoors to or systematic monitoring of encrypted content will be efficient in countering and disrupting criminal activities, including by highlighting:
    - o The lack of substantial evidence that prevented access to encrypted communications significantly hinders the work of law enforcement, or that monitoring of criminal actors cannot be done in another manner.
    - o The risk of threat actors migration to non-cooperative platforms[2] and increased usage of other encryption tools.
    - o The fact that E2EE is not in and of itself a decisive factor for terrorists when establishing themselves on an app, especially if the service is used for strategic and propaganda (as opposed to operational) purposes.

3. Increase public communication about how E2EE constitutes the backbone of today's security and privacy, online and offline**.**

4. Work towards improving public understanding of how their 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.

Mitigate risks of terrorist and violent extremist exploitation of E2EE:

5. Design and implement an explicit zero-tolerance policy for criminal actors, especially terrorists and violent extremists.

6. Develop and implement risk mitigation strategies to counter criminal use of their E2EE messaging services.

7. Conduct risk assessments on how specific features – including audience reach, usability, stability

[2] There is significant evidence suggesting that terrorist actors are increasingly migrating to niche 'alt-tech' sites or building their own websites, both of which arguably offers improved audience reach and stability. For more, see Tech Against Terrorism's threat assessment update of Q1-2 of 2021: https://www.techagainstterrorism.org/2021/07/30/trends-in-terrorist-and-violent-extremist-use-of-the-internet-q1-q2-2021/

[3] 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 of data by anyone other than the end-user will be prohibited. However, the regulation notes exemptions of 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 on 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.

and security – could cause increased use by terrorists and violent extremists and develop proportionate counter-measures.

8. Explore use of metadata to conduct behavioural analysis and detect criminal use of their services in line with relevant ePrivacy regulations.[3]

9. Develop or support the development of keyword analysis to identify terrorist networks on encrypted messaging services.

10. Ensure that user reporting is easily available to users.

Support innovative investigation techniques:
11. Maintain and promote constructive working relationships with law enforcement agencies and (capacity allowing) establish points of contact to facilitate cooperation.

12. Develop clear law enforcement guidelines detailing what information can be provided (and under which conditions) to increase transparency and accountability regarding cooperation with law enforcement and governments.

13. Publish regular transparency reports on collaboration with and requests from law enforcement and subsequent content moderation decisions in line with the Tech Against Terrorism Guidelines on transparency reporting.[4]

A more detailed list of recommendations for tech companies, in particular encrypted messaging services, can be found in Part 4 of the report.

We recommend governments and tech companies

To support efforts to counter terrorist and violent extremist abuse of E2EE, we recommend that governments and tech companies:

1. Support public-private collaboration to effectively counter illegal use of E2EE whilst protecting human rights, including the right to privacy.

2. Support further research on the use of E2EE by terrorists and violent extremists to ensure that countermeasures are proportionate and evidence-based. This includes research on criminal actors' cross-platform migration.

3. Support research on the potential risks created by the implementation of technical tools to monitor screen communications for illegal content.

4. Support research on how metadata can be used to detect illegal use of E2EE services.[5]

[4] See: https://transparency.techagainstterrorism.org/. To find out more about Tech Against Terrorism's work on transparency reporting, see: Transparency reporting for smaller platforms; and Summary of our webinar on transparency reporting for smaller tech companies.
[5] Whilst taking into consideration that metadata is also protected by the right to privacy. On the protection of privacy in the digital age, and how this applies to metadata, see: United Nations Human Rights Office of the High Commissioner (OHCHR), OHCHR and privacy in the digital age.

SUMMARY

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

E2EE guarantees that no one, not even the service provider, can access the content of a communication or file, thus pre-empting the risks of data leaks or surveillance programmes. This is one reason why policymakers and government entities also use E2EE services to secure their online communications.[6]

User demand for online privacy and security – often motivated by concerns of government surveillance programmes and perceived risks of data being misused by tech platforms, have led tech companies to increasingly offer security and privacy features on their services. For messaging services, this has meant offering E2EE as a default or opt-in option. E2EE is now offered by almost all leading messaging apps (see Annex 1. Overview of E2EE apps), and the most used messaging app globally, WhatsApp, delivers about 100 billion messages a day (all of which are end-to-end encrypted).[7]

Due to concerns over misuse by terrorist groups and other criminal networks (such as child sexual abuse offenders), governments and law enforcement agencies have been calling for E2EE services to be monitored to detect illegal content or accessed by law enforcement.[8] However, none of the technical tools suggested by policymakers for monitoring or accessing E2EE communications assessed in this report are viable or secure. For example, creating backdoors would not be possible without risking these backdoors being used by criminal actors. Monitoring and backdoor creation have been criticised by cryptographers, technical experts, and digital rights groups, raising concerns of the potential privacy and security risks that such solutions would entail.[9]

[6] *In the US, the Clinton emails leak likely spurred the use of WhatsApp by close aides to US policymakers and politicians themselves. In general the use of WhatsApp by world leaders is referred to as "WhatsApp Diplomacy": recent reports note that the UK Prime Minister, Boris Johnson, has also been known to use WhatsApp to communicate with French President, Emmanuel Macron, and the Saudi Crown Prince, Mohammed bin Salman. Besides WhatsApp, Signal is also recommended by the European Union for external communications, and the UK Conservative Party switched to Signal in 2019. In France, the government developed its own E2EE services for public servants – Tchap, based on Element's Matrix protocol. President Macron is also known to use Telegram, whereas WhatsApp was preferred by former Prime Minister Édouard Philippe.*
See: 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; Gange David (2020), Boris Johnson and Emmanuel Macron's WhatsApp messages on quarantine-free travel blindsided officials, UK News Today; Borger Julian, Rankin Jennifer, Lyons Kate (2017), The rise and rise of international diplomacy by WhatsApp, The Guardian; Dussutour Chloe (2020a), European Commission to use open source messaging service Signal: Dussutour Chloe (2020b), French government launches in-house developed messaging service, Tchap, JoinUp; Hacot Valerie (2019), Messageries : plutôt WhatsApp à Matignon et Telegram à l'Elysée, Le Parisien.
[7] *Singh Manish (2020), WhatsApp is now delivering roughly 100 billion messages a day, TechCrunch*
[8] *See: Council of the EU (2020), Draft Council Resolution on Encryption - Security through encryption and security despite encryption: Governments of the United States, United Kingdom, and Australia (2019), Open Letter: Facebook's "Privacy Frist" Proposals; 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; Sen. Graham, Lindsey, EARN IT Act, The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act of 2019, Congress.gov; and United Kingdom, Investigatory Power Act 2016.*
[9] *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; 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.*
Portnoy Erica (2019), Why adding client-side scanning breaks end-to-end encryption, Electronic Frontier Foundation.

Technical tools to monitor E2EE communications

Most of the technical tools proposed by policy makers for monitoring illegal content on E2EE services rely on screening of content prior to it being transmitted to the recipient.[10] This would (if content is deemed to be unlawful) likely lead to blocking the transmission altogether by preventing the transmission of screened messages. These technical tools, which often rely on classifiers and hashing technology, scan content prior to encryption. In the case of "secure enclaves", this would entail decrypting content for monitoring purposes. Homomorphic encryption[11] is the only proposal that would allow for the screening of encrypted content. However, all tools suggested to monitor content shared on E2EE services present significant security risks and break the promise of privacy inherent to E2EE.

Terrorist use of the internet and E2EE

Terrorists exploit an entire tech ecosystem of online platforms.[12] Inevitably, this also includes encrypted services. Terrorists use encrypted platforms mainly for operational purposes, with E2EE messaging apps being exploited as a means to communicate online whilst reducing the risk of their communications being monitored or intercepted in transit.

However, security and privacy are not the only features that make a platform attractive to terrorists and violent extremists. Terrorists generally consider four main characteristics before choosing an app or platform:[13] Security, stability, usability, and audience reach. Terrorists analyse and assess the costs and benefits of using a platform according to these four sets of features, considering the broader context of operation and intended goal (e.g. spreading propaganda or organising).[14] Therefore, E2EE alone does not necessarily attract terrorist exploitation. Rather, terrorists will choose their preferred platforms depending on the suitability of the platform as a whole and the different features it offers.

[10]For an overview of such solutions, see: EU Commission (2020), Leaked report on technical solutions to detect child sexual abuse in end-to-end encrypted communications.
[11]Bernard Marr, (2019), What Is Homomorphic Encryption? And Why Is It So Transformative?, Forbes; The SSL Store (2019), Homomorphic Encryption.
[12]Tech Against Terrorism's analysis of more than 45,000 URLs shows that terrorists exploit over 330 platforms across the broader tech sector ecosystem, with the majority being smaller platforms.
See: Tech Against Terrorism (2019), Analysis: ISIS use of smaller platforms and the DWeb to share terrorist content.
[13]On the set of features favoured by terrorists and violent extremists see: 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 (2019), "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"; Tech Against Terrorism (2019b), "ISIS use of smaller platforms and the DWeb to share terrorist content"
[14]For example, a group might be willing to accept lower audience reach if a platform is secure (and vice versa), and if the choice is between two platforms with similar feature sets, terrorist groups are likely to choose the platform that is more user-friendly.

Tackling terrorist use of E2EE: key considerations

Below we highlight key considerations with regards to E2EE and the potential use of technical tools to screen content or backdoor access.[15]

Displacing rather than combating the threat: If technical tools for screening E2EE communications or backdoor access are introduced in law, we assess that it is highly likely that criminals including terrorists may migrate to other services and devices unwilling to cooperate with law enforcement or designed solely for criminal use.

Learning from previous terrorist migration

The joint November 2019 operation by Telegram and Europol to remove IS channels on the app led to a temporary displacement of IS and its supporters onto other messaging apps such as TamTam and Hoop Messenger by December 2019. At the time of writing, IS is still dispersed across many platforms, and have made persistent attempts to re-establish themselves on Telegram and continue to experiment with a number of alternative platforms. The operation therefore has simultaneously made IS content more difficult f or prospective terrorists to find, whilst also making it more difficult for law enforcement and researchers to monitor.[16]

Jurisdiction: Backdoors and monitoring also raise the question of jurisdictional limits, the scope of application, and who would be trusted with escrow keys or with informing databases of illegal content (needed to inform monitoring and matching). Experts have also raised concerns with criminals turning to services located in non-cooperative jurisdictions, as well as with non-democratic countries using the example of intrusive backdoors and bans implemented in democratic countries as a model for potentially repressive legislation.[17]

Security risks associated with monitoring and accessing E2EE communications: Privacy vulnerabilities and security risks exist in all the technical tools to screen E2EE communication, albeit to differing extents. The same goes for "backdoors", which would fundamentally weaken encryption protocols. E2EE is only as strong as its weakest point, and experts have cautioned that any security vulnerabilities in the encryption protocol means that it would be at risk of exploitation by criminal actors, including terrorists and violent extremists.

Safeguarding the fundamental right to privacy: The right to privacy has to be safeguarded.[18] Any infringement on the fundamental right to privacy ought to be proportionate to its aim and inscribed in the rule of law. Any provisions for backdoors or monitoring should therefore provide clear guidelines and requirements regarding the exact scope and processes that would frame the potential systematic monitoring of private communications, or the legal provision to create backdoors.[19]

[15] Encrochat, which was hacked by Europol in 2020; see: Garrick Law (2020), Encrochat Encrypted Telephones Hacked June 2020 – Drugs, Telephones, NCA Police & Searches;
[16] Cole Phil (2019), ISIS Is Now Harder to Track Online—but That's Good News, Wired; Basit Abdul (2019), Shaw Danny (2020), Hundreds arrested as crime chat network cracked, BBC News.
[17] More or less 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 (2020c), The Online Regulation Series | Insights from Academia I A similar "forum-shopping" 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
[18] The right to privacy 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 International Covenant on Civil and Political Rights (Art. 17).
[19] This argument has also been raised by The European Data Protection Supervisor's (EDPS) in its Opinion on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online.

Thinking beyond short term impact: There is a significant risk of long-term consequences with many of the suggested tools to detect criminal exploitation of E2EE. In particular, there is no guarantee that adversarial actors (state and non-state) will not exploit weakened encryption protocols. The roll-out of systematic monitoring of E2EE content, or the mandating of backdoors access, would also signal the possibility of screening all content shared in private communications, including beyond terrorist and other illegal content. These powers could be used by governments to monitor private communications for reasons of surveillance or censorship.[20]

Identifying terrorist actors on E2EE platforms via metadata

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. This is information that service providers can observe through the provisioning of services, including when, how frequently, how long, and with whom users are communicating. This data, especially in bulk, may give insight into individual and collective behaviour and social network analysis.

Metadata can be used to inform law enforcement investigations or platforms' content moderation without breaking the encryption protection of the communication. However, not all E2EE services collect metadata; and whilst metadata does not contain private communications, it still falls under the protection of the fundamental right to privacy.[21]

Annex 1 – Overview of leading messaging apps offering E2EE

Platforms	Monthly active users	Fully E2E encrypted	"Secret chat" E2EE option
WhatsApp	2 billion monthly active users (April 2020)		
Signal	1-5 million downloads (no specific statistics available);[22] userbase estimate to 20 million active users (end of 2020)[23]		
Line Messenger	84 million monthly active users (2020)[24]		

[20] On that, 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 guarantee that in the future a government won't use access to E2EE beyond the stated purposes 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.
[21] UN OHCHR, The Right to Privacy in the Digital Age, Report of the United Nations High Commissioner for Human Rights.
[22] Lee Micah (2016), Battle Of The Secure Messaging Apps: How Signal Beats WhatsApp, The Intercept.
[23] Greenberg Andy (2020), Signal is Finally Bringing Its Secure Messaging to the Masses, Wired; Singh Manish (2021), Signal's Brian Acton talks about exploding growth, monetization and WhatsApp data-sharing outrage, TechCrunch.
[24] Statista (2020), LINE – Statistics & facts.

Platforms	Monthly active users	Fully E2E encrypted	"Secret chat" E2EE option
Viber	1.2 billion unique users IDs March 2020)[25]		
Wire	Over 1 million installations on Google Play[26]		
Wickr me	Over 5 million installations on Google Play [27]		
Threema	Over 8 million users (including 2 million for Threema Work) [28]		
Element (formerly Riot.im)	Over 100,000 installations on Google Play [29]		
IMessage:	Estimate of 1.3 billion active users (2019) [30]		
Rocketchat	Over 100,000 installations on Google Play [31]		
Telegram	400 million monthly active users (October 2020) [32]		
Conversations	Over 100,000 installations on Google Play. [33]		
Kakaotalk	45 million active users (2020) [34]		
Snapchat	249 million daily active users (2020) [35]		
Session	Over 100,000 installations on Google Play (December 2020) [36]		
Fortknoxster	Over 100,000 installations on Google Play (December 2020) [37]		
Hoop Messenger	Over 500,000 installations on Google Play (December 2020) [38]		

[25] Clement J. (2020a), Viber: number of registered user IDs 2011-2020, Statista.
[26] https://play.google.com/store/apps/details?id=com.wire&hl=en_GB&gl=US
[27] https://play.google.com/store/apps/details?id=com.mywickr.wickr2&hl=en_GB&gl=US
[28] Threema (2020), Cryptography Whitepaper.
[29] https://play.google.com/store/apps/details?id=im.vector.app&hl=en_GB&gl=US
[30] 99Firms (2019), Most Popular Messaging Apps.
[31] Googe Play: Rocketchat
[32] Iqbal Mansoor (2020), WhatsApp Revenue and Usage Statistics (2020), Business of App.
[33] Conversations page on Google Play
[34] Waldeck Yasmin (2020), Number of monthly active users of KakaoTalk in South Korea 2015-2020, Statisita
[35] Clement J. (2020a), Daily active users of Snapchat 2014-2020, Statista.
[36] https://play.google.com/store/apps/details?id=network.loki.messenger&hl=en&gl=US
[37] https://play.google.com/store/apps/details?id=com.fortknoxster&hl=en&gl=US
[38] https://play.google.com/store/apps/details?id=com.magnificus.hoop&hl=en&gl=US