FOR YOUR EYES ONLY?

RANKING 11 TECHNOLOGY COMPANIES ON ENCRYPTION AND HUMAN RIGHTS

AMNESTY INTERNATIONAL

Amnesty International is a global movement of more than 7 million people who campaign for a world where human rights are enjoyed by all.

Our vision is for every person to enjoy all the rights enshrined in the Universal Declaration of Human Rights and other international human rights standards.

We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and public donations.

First published in October 2016
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: POL 40/4985/2016
Original language: English

amnesty.org

Cover photo: Using instant messaging services is part of everyday life for hundreds of millions of people around the world, but their private communications are under real threat from cybercriminals and government surveillance. © iStock

AMNESTY INTERNATIONAL

CONTENTS

EXECUTIVE SUMMARY

Encryption helps protect people's human rights online. By rendering digital data unintelligible, encryption helps ensure that private information sent over the internet stays private. It also allows people to access and operate in safe online spaces where they can speak freely and express their ideas and opinions without fear.

Encryption stops cybercriminals from stealing our personal information, and helps prevent unlawful government surveillance of our communications. It is particularly important for human rights defenders and journalists around the world – whether they are dissidents in China, Bahraini activists in exile abroad, or investigative journalists in Europe. A breach of their data security undermines their vital work, and could result in arrest and detention.

Technology companies play a crucial role in keeping digital information safe. This report ranks 11 companies on whether they are meeting their human rights responsibilities in the way they use encryption to protect users' online security. It focuses specifically on instant messaging services, such as Skype, WhatsApp and WeChat, which hundreds of millions of people around the world use to communicate every day.

Private communications on instant messaging services are under real threat from cybercriminals, malicious hackers, and unlawful interception by state authorities. We ranked the companies on their stated policies and practices, including whether they are deploying a form of encryption that is effective in responding to identified risks to human rights. Amnesty International considers that at minimum, technology companies must deploy end-to-end encryption as a default on instant messaging services – meaning that even the companies themselves cannot access the content of the messages.

The companies that place lowest on our ranking – Blackberry, Snapchat, and Tencent – are failing to apply an adequate level of encryption to their instant messaging services, and as a result are putting their users' rights to privacy and freedom of expression at risk. In addition:

- Only three of the companies assessed – Apple, LINE, Viber Media – apply end-to-end encryption as a default to all of their IM services. Of these, none are fully transparent about the system of encryption they are using.
- In five cases Amnesty International found a gap between policy and practice: for example, Microsoft has a clear stated commitment to human rights, but is not applying any form of end-to-end encryption on its Skype service.
- All of the companies, with the exception of Tencent, have stated publicly that they will not grant government requests to backdoor the encryption on their messaging services.

Many of the companies assessed have taken a strong public stance in support of privacy and security, and have defended their use of encryption tools in the face of pressure from governments. But even the top-ranked companies should do more to show that they are using encryption to respond to human rights threats. All of the companies examined must also be more transparent with their users and the wider public about their use of encryption.

It is now more important than ever to recognize encryption as a human rights issue. There is currently a heated debate between governments, technology companies and privacy advocates over the use of encryption tools online. States have voiced concerns that by protecting the digital data of suspects of crime

and terrorism, encryption is preventing law enforcement and security agencies from being able to carry out investigations – a phenomenon that has become known as 'going dark'.

States have an obligation to protect their populations from crime, including terrorism, and electronic surveillance can legitimately be used for this purpose, if it complies with international law. Encryption does present challenges to law enforcement, because by its very nature, effective encryption must be unbreakable by everyone, even those with legitimate intentions.

However, states also have an obligation to protect the rights to privacy and freedom of expression online. This means that any measures to restrict or circumvent encryption must comply with strict requirements under international law.

Some countries including Pakistan, India, Turkey, and China, have already enacted legislation restricting access to and use of encryption. In seeking to address concerns of 'going dark', some state authorities have proposed requiring technology companies to put 'backdoors' on encryption to provide law enforcement with special access to encrypted information.

However, there is virtual consensus among expert technologists and cryptographers that it is impossible to put in place a system of special access that could only be used by the intended state authorities. If a backdoor exists, others –criminals, malicious hackers, or other governments – will also be able to access it. By undermining digital security for the vast majority of people who rely on encryption for protection, such measures are inherently disproportionate, and do not comply with international law.

Moreover, the encryption debate comes amidst heightened mistrust of governments over their use of surveillance. US intelligence documents disclosed by Edward Snowden in 2013 exposed how US and UK intelligence agencies conducted indiscriminate surveillance on a vast scale – and how companies including Facebook, Google and Microsoft faced secret legal orders to hand over their customers' data. In October 2016, inside sources revealed how Yahoo agreed to a US government demand to scan all of its users incoming emails. In addition to mass surveillance, governments around the world are using targeted invasive surveillance tools to monitor activists and journalists without legitimate grounds.

In this context, technology companies must stand up for the rights of their users by putting in place strong data security protections on their products and services. Companies must resist government efforts to undermine or restrict the use of encryption, while still complying with legitimate requests for information by law enforcement and security agencies when they are able to do so.

The companies assessed in this briefing largely recognize the importance of encryption as a tool for protecting their users' online security. Companies that have publicly refused government attempts to backdoor their services, such as Apple and Facebook, should bolster this position by arguing that encryption tools are vital to the realization of human rights in a digital world. Companies that are lagging behind their peers, either by relying on weaker forms of encryption, or by failing to recognize human rights risks, must catch up.

MESSAGE PRIVACY RANKING

Amnesty International sent letters to all the companies assessed, requesting information about each company's current encryption standards, and details of policies and practices the company has in place to ensure it meets its human rights responsibilities in relation to its instant messaging services. We based our assessment on an analysis of publicly available information and company responses, where applicable.

We ranked the companies across 5 criteria:

- Does the company recognize online threats to freedom of expression and right to privacy as risks to its users through its policies and procedures?
- Does the company apply end-to-end encryption as a default?
- Does the company make users aware of threats to their privacy and freedom of expression and how the company is responding through the use of encryption?
- Does the company disclose details of government requests for user data, and how it responds?
- Does the company publish technical details of its system of encryption?

We awarded up to 3 points per criterion, giving a maximum possible score of 15. For ease of understanding, we scaled the overall score as a total out of 100.

Amnesty International did not assess the overall security of the IM services, and do not endorse any of the named applications as a secure tool for communications. We recommend that journalists, activists, human right defenders and others whose communications may be particularly at risk seek expert digital security advice.

OVERALL RANKING

Ranking position	Company	Instant messaging services	Replied to Amnesty's request for information?	Overall score /100
1	Facebook	FB Messenger, WhatsApp	Yes	73
2	Apple	iMessage, FaceTime	Yes	67
3	Telegram	Telegram Messenger	Yes	67
4	Google	Allo, Duo, Hangouts	No	53
5	Line	Line	Yes	47
6	Viber Media	Viber	Yes	47
7	Kakao Inc	KakaoTalk	Yes	40
8	Microsoft	Skype	Yes	40
9	Snapchat	Snapchat	Yes	26
10	Blackberry	Blackberry Messenger	No	20
11	Tencent	QQ, WeChat	No	0

1. BACKGROUND AND CONTEXT

> **"Encryption protects the identity of dissidents all over the world. It's a vital tool to allow journalists to communicate securely with their sources, NGOs to protect their work in repressive countries, and lawyers to communicate privately with their clients."**
>
> Cybersecurity expert Bruce Schneier, February 2016

In today's digital, globalized world, almost half the world's population have access to the internet, enabling them to communicate with one another through email, instant messaging (IM) and social media.

Companies providing online services have enormous power and control over the ways in which data is shared and stored – and how it is kept safe. Governments have an obligation to respect and protect human rights in the context of digital communications, but all too often states are themselves perpetrating abuses through mass surveillance and censorship. As a result, the world's largest technology companies are now engaged in a political and technological debate with governments and law enforcement agencies about one of the primary means for securing and protecting digital information – encryption.

Technology companies have a responsibility to respect human rights and ensure that they are not contributing to abuses of users' rights to privacy and freedom of expression. Encryption is one of the most effective ways for these companies to protect the security of their users' communications and thereby respond to human rights risks. Amnesty International has previously published a detailed briefing outlining the importance of encryption for protecting human rights online.[1]

This report ranks 11 technology companies based on the extent to which they are approaching encryption as a human rights issue, rather than solely as one of digital security, and whether the companies are applying an adequate level of encryption, specifically in relation to their IM services. These services enable users to communicate via an internet connection to send each other text messages, photos, videos and to make audio and video calls.

Individuals around the world – including human rights activists and journalists and the wider public – face real threats to their rights to privacy and freedom of expression when they use IM services. The risks stem from private communications data being illegitimately obtained as a result of mass or targeted surveillance,

[1] Amnesty International, *Encryption: A Matter of human rights* (Index: POL 40/3682/2016), available at: www.amnesty.org/en/documents/pol40/3682/2016/en/

government requests for user data that do not fulfil requirements under international law, or from malicious hackers or criminals compromising the security of the service.

ENCRYPTION AS A HUMAN RIGHTS ISSUE

Encryption is what makes our data and communications online safe. It is a mathematical process for encoding information to ensure that it can only be accessed by its owner or intended recipient. It is applied in multiple contexts online – such as email, financial transactions and storing medical data. Encrypting data means that if anyone intercepts or obtains this data who is not an intended recipient, they will only see scrambled information.

United Nations experts and human rights groups, including Amnesty International, now consider encryption a vital enabler of human rights, in particular for the rights to privacy and to freedom of expression and opinion.[2] Encryption helps to create a "zone of privacy" online within which people are free to express their beliefs and ideas without fear of interference.[3] Access to encryption, or the lack thereof, may also have an impact on other rights such as the right to peaceful assembly and association.

It is only by securing communications against outside interference that ordinary internet users, human rights defenders, opposition politicians, political activists and investigative journalists can protect themselves from cybercrime as well as from the prying eye of governments all around the world. According to Zeid Ra'ad Al Hussein, UN High Commissioner for Human Rights, "it is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered."[4]

In 2013, the whistle-blower Edward Snowden exposed the existence of global indiscriminate mass surveillance programmes by the US National Security Agency (NSA) and the UK Government Communications Headquarters (GHCQ). These programmes monitor the internet and phone activity of hundreds of millions of people across the world. In addition, many governments carry out more targeted surveillance of individual activists and journalists – for example, the Ethiopian government has used electronic surveillance to spy on opposition activists not only in Ethiopia, but abroad.[5]

Amnesty International has examined the system of secret surveillance in Belarus, which allows the authorities to undertake wide-ranging surveillance with little or no justification.[6] Civil society groups in Belarus generally operate in a restrictive legal environment that violates numerous internationally protected human rights. Belarusian activists regularly face arrest, detention or imprisonment merely for exercising their human rights.[7] Activists and journalists in Belarus who live under fear of surveillance, reported that the use of encryption tools, including encrypted chat programmes, is essential to their work.

DEBATE OVER ENCRYPTION

In the last few years, some technology companies have responded to public concerns around data security by introducing stronger encryption into widely used communications products and services – including end-to-end encryption, where the company itself does not have access to the content of communications data. As a result, a number of states have expressed fears of "going dark". Law enforcement agencies are concerned that encryption will reduce their powers and capability to access the content of communications, meaning they are unable to access information necessary to investigate and prosecute suspected criminals – even where they have legal warrants to do so.

As a result, some governments and legislators have proposed the introduction of regulations to circumvent or restrict encryption, including through mandating service providers to introduce 'backdoors' – technical

[2] D. Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Report to the Human Rights Council*, 22 May 2015, UN Doc A/HRC/29/32, (hereinafter: D. Kaye report 2015) available at: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32
[3] D. Kaye report 2015, p. 5.
[4] Office of the United Nations High Commissioner for Human Rights (OHCHR), *Apple-FBI case could have serious global ramifications for human rights: Zeid*, 4 March 2016.
[5] Human Rights Watch, *Ethiopia: Telecom Surveillance Chills Rights*, 25 March 2014, available at: www.hrw.org/news/2014/03/25/ethiopia-telecom-surveillance-chills-rights
[6] Amnesty International, *"It's enough for people to feel it exists": Civil society, secrecy and surveillance in Belarus* (Index: EUR 49/4306/2016).
[7] Amnesty International, *What is not permitted is prohibited: Silencing civil society in Belarus* (Index: EUR 49/002/2103).

measures that facilitate access by authorities to encrypted information and communications.[8] Moreover, a number of governments, including Pakistan, Turkey and China, have already enacted legislation dramatically restricting access to and use of encryption.[9]

Proposals to backdoor encryption have been strongly criticized by technologists and security experts, who have raised fundamental practical and technical reasons why such measures would seriously undermine digital security.[10] Firstly, such exceptional access would force companies to reverse best practices which are already being deployed to protect digital security. Secondly, building in such access mechanisms also increases system complexity and therefore vulnerability, as there are more opportunities for flaws and loopholes. Thirdly, if a particular body or agency is trusted to hold the key to the backdoor, this actor would become a focused target for cyberattack. Finally, there are fundamental jurisdictional challenges around how such systems would operate in practice in a globalized world.[11]

As a result, it is a "seemingly universal position" among technologists that it is impossible to put in place a system of special access that could only be used by the intended state authorities.[12] If a backdoor exists, it has to be assumed that others – be they criminals, hackers, or other governments – will also be able to access it.

The debate around encryption received greater prominence with the dispute between Apple and the FBI in February and March 2016. The FBI sought to unlock an iPhone used by one of the shooters in a December 2015 attack in San Bernardino, California. Apple resisted the FBI's request on the basis that the government had asked it to build a 'backdoor' which would enable access to not only one specific iPhone, but to all iPhones. Apple's CEO Tim Cook argued that the government's demands constituted a "breach of privacy", and that it would be "dangerous" to create such a backdoor.[13] Numerous independent technology experts, law professors, technology companies and human rights organizations – including Amnesty International – supported Apple's stance on this matter.[14]

The *Apple v. FBI* case concerns device encryption, namely the protections applied to data while it is stored on a phone or computer. However, law enforcement agencies have also expressed concerns over the encryption of communications data while in transit – the focus of this report – and have demanded that companies provide access to encrypted messaging.

In 2014, the FBI criticized Apple's decision to enable end-to-end encryption on iMessage,[15] and there have since been US legal cases where authorities sought access to encrypted communications on iMessage.[16] In April 2016, Facebook's WhatsApp put in place end-to-end encryption for all communications sent through its IM service – the world's largest with over 1 billion users. WhatsApp's use of encryption has led to the company and its parent Facebook becoming involved in a series of legal disputes in Brazil over its inability to hand over data to law enforcement. On three occasions, this has resulted in a temporary nationwide shutdown of WhatsApp in Brazil, following orders by Brazilian judges, and has also led to a Facebook executive being arrested and imprisoned for 24 hours.[17]

---

[8] For example, in September 2015, the Indian government published a draft National Encryption Policy that would have required companies to store decrypted data that could be made available to law enforcement. Following extensive public criticism, the government withdrew the draft policy and is currently redrafting it. See Software Freedom Law Centre, FAQ: Legal Position of Encryption in India, 29 June 2016, available at: http://sflc.in/faq-legal-position-of-encryption-in-india/. In the USA, in April 2016, Senators Richard Burr and Dianne Feinstein released a draft encryption bill that would require companies to be able to provide decrypted data to law enforcement. See D. Feinstein, *Intelligence Committee Leaders Release Discussion Draft of Encryption Bill*, 13 April 2016, available at: www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation

[9] For details, see Amnesty International, *Encryption: A matter of human rights* (Index: POL 40/3682/2016), p. 12., available at: www.amnesty.org/en/documents/pol40/3682/2016/en/

[10] H. Abelson et al, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology, 6 July 2015 (hereinafter: *Keys under Doormats),* available at: www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf

[11] *Keys under Doormats*, p. 2-3.

[12] D. Kaye report 2015, para. 8.

[13] T. Cook, *A Message to Our Customers*, 16 February 2016, available at: www.apple.com/customer-letter/

[14] A list of amicus briefs in support of Apple for the 22 March 2016 hearing available at: www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html

[15] The Guardian (UK), *Apple's encryption means it can't comply with US court order*, 8 September 2015.

[16] The New York Times, *Apple and other Tech companies tangle with U.S. over data access,* 7 September 2015.

[17] The New York Times, *WhatsApp is briefly shut down in Brazil for a third time*, 19 July 2016; Reuters, *Facebook exec jailed over encrypted WhatsApp data says Brazil's police treated him with respect*, 6 March 2016.

SURVEILLANCE AND HUMAN RIGHTS

Surveillance of private communications always entails an interference with human rights, but it can be justifiable if it meets strict requirements under international law. Surveillance is only justifiable when it occurs based on reasonable suspicion, in accordance with the law, is strictly necessary to meet a legitimate aim (such as protecting national security or combatting serious crime) and is conducted in a manner that is proportionate to that aim and non-discriminatory.

Indiscriminate mass surveillance, such as the programmes exposed by Edward Snowden, that is not targeted at specific individuals and is not based on reasonable suspicion will always fail this test because, by its very nature, it constitutes a disproportionate interference with the rights to privacy and freedom of expression.

Strong encryption can pose challenges to accessing information for legitimate law enforcement purposes. Governments have an obligation to protect their populations from crime, including terrorism, and electronic surveillance can be legitimately used for this purpose, if undertaken within the bounds of international law. Yet encryption must be unbreakable by everyone, even those with legitimate intentions, in order for it to be effective against those with illegitimate intentions.[18] It is for this reason that its deployment, promotion and use has become the focus of political debate and the target of legislative measures.

Amnesty International believes that states should facilitate the use of encryption and not interfere with encryption, or permit interferences by others, in an unjustified manner. Government measures to ban or restrict encryption, or that require corporate actors to weaken or backdoor encryption in order to guarantee access by law enforcement to encrypted communications, are inherently disproportionate, and thus impermissible under international law. There is no way to backdoor encryption without undermining the rights of everyone who relies on it.

ROLE OF THE PRIVATE SECTOR

Under international human rights standards, while states have the primary obligation to uphold human rights, all companies should respect human rights. According to the UN Guiding Principles on Business and Human Rights, the responsibility to respect human rights is "a global standard of expected conduct for all business enterprises wherever they operate."[19]

Technology companies can play a critical role in upholding the rights to privacy and freedom of expression in the face of any illegitimate attempts by governments to gain access to individuals' private information and the growing threat of cybercrime.

Companies' responsibility to respect human rights requires that they have adequate measures in place to respond to threats to human rights. The risks of unlawful mass surveillance and large data breaches are well known and technology companies have a responsibility to take measures to protect their users' data, including deploying the strongest encryption possible to their products and services. Encryption plays a critical role in keeping private communications private, thus enabling the enjoyment of, among others, the rights to privacy and freedom of expression. As such, technology companies and service providers could contribute to human rights abuses by governments or other third parties if they have weak encryption in their products or comply with government requests to restrict access to, or use of, encryption.

Much is at stake. There are real reputational risks to companies if they do not do enough to protect their users' digital security, or if they are seen to be collaborating with governments in conducting unlawful surveillance. This is particularly the case in the aftermath of Edward Snowden's revelations about the role of corporations in the USA's PRISM surveillance programme, where companies – including Facebook, Google and Microsoft – faced legal orders to hand over their customers' data to the NSA under secret orders. This is still very much an ongoing concern – in October 2016, inside sources revealed how in 2015 Yahoo agreed to a US government demand to scan all of its users incoming emails.[20]

---

[18] B. Schneier, *iPhone encryption and the return of the crypto wars*, 6 October 2014, available at: www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html
[19] UN GPs principle 11.
[20] Reuters, *Yahoo secretly scanned customer emails for U.S. intelligence–sources*, 4 October 2016, available at: www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT

2. SCOPE AND METHODOLOGY

Amnesty International's 'Message Privacy Ranking' ranks 11 companies based on whether they are meeting their human rights responsibilities in the way they use encryption to protect users' online security. It focuses specifically on companies that provide instant messaging (IM) services.

We chose to focus on IM services for three reasons. Firstly, it is reasonable to expect companies to put in place strong forms of encryption on these services, given the threats to users' human rights.

Secondly, the use of these services by the general population is increasing. The number of people using smartphones around the world is rising rapidly, particularly in emerging and developing economies,[21] and more than half of the world's internet users are on IM every day.[22] Human rights activists around the world are increasingly relying on IM to exchange information and mobilize supporters.[23]

Thirdly, and most importantly, as outlined above, IM services have come into sharp focus in the debate over encryption and national security. In commenting on encryption applied to phones and other devices, and encryption applied to messaging apps, the Director of the US Federal Bureau of Investigations (FBI), James Comey, stated that "The data at rest problem affects non-national security law enforcement overwhelmingly… The data in motion, at least today, overwhelmingly affects our national security work. Terrorists and their fellow travellers are increasingly using end-to-end encrypted apps." [24]

State authorities are demanding access to data held by technology companies about users of these services. In addition to the example of WhatsApp in Brazil, Iran recently passed a regulation ordering providers of IM services to transfer all data and activity they hold about Iranian citizens to servers inside the country.[25]

Companies assessed

There are many different IM applications. In this briefing, we have chosen to focus on companies that develop and run the most popular messaging services worldwide, indicated by the number of users on these services. We have also sought to ensure a balance by including companies headquartered in a number of different countries, as people in different regions often use different services. For example, while WhatsApp is the world's most popular IM app, it has a limited user base in China, where Tencent's WeChat (called Weixin in China) is the dominant service.[26]

---

[21] Pew Research Center, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*, 22 February 2016, available at: www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/
[22] TNS Global, *The new social frontier: Instant messaging usage jumps 12% globally*, 2015, available at: www.tnsglobal.com/press-release/rise-of-im
[23] Y. Atal, former UNESCO Principal Director of Social and Human Sciences, keynote address, in: *Human Rights in Changing Times*, Edited by G.P. Agarwal, S.K. Choudhary and R. Gupta, 2013, p. xix, available at: www.cambridgescholars.com/download/sample/59091
[24] Bloomberg, *FBI has sights on larger battle over encryption after Apple feud*, 11 May 2016, available at: www.bloomberg.com/news/articles/2016-05-11/fbi-has-sights-on-larger-battle-over-encryption-after-apple-feud
[25] Reuters, *Iran orders social media sites to store data inside country* , 29 May 2016, available at: www.reuters.com/article/internet-iran-idUSL8N18Q0IN
[26] Tech In Asia, *WeChat blasts past 700 million monthly active users, tops China's most popular apps,* 18 April 2016, available at: www.techinasia.com/wechat-blasts-700-million-monthly-active-users-tops-chinas-popular-apps

The 11 companies assessed and the instant messaging services that they provide are shown in the table below.

Company	Headquarters	Messaging services	Number of active users
Apple	USA	iMessage, FaceTime	Unknown; 1 billion iPhones sold
Blackberry	Canada	Blackberry Messenger	100 million
Facebook	USA	Facebook Messenger, WhatsApp	1 billion for each app
Google	USA	Allo, Duo, Hangouts	Unknown app-by-app; Google's total user base more than 2 billion
Kakao Inc	South Korea	KakaoTalk	49 million
Line	Japan	Line	218 million
Microsoft	USA	Skype	300 million
Snapchat	USA	Snapchat	200 million
Telegram	Germany	Telegram Messenger	100 million
Tencent	China	QQ, WeChat	WeChat: 697 million; QQ: 853 million
Viber Media	Luxembourg	Viber	250 million

Scope of the assessment

This report uses a human rights framework to assess technology companies based on their stated policies and practices, specifically in relation to the encryption deployed on their IM services. It is not an overall assessment of the companies' human rights performance, or their approach to privacy across all their products and services.

Amnesty International has not carried out a technical evaluation of the specifics of the cryptography used on these services or how it is implemented. The report therefore is limited to assessing the companies only on the form of encryption that they apply to these services, as explained in detail in section 3 below. The form of encryption deployed is an important indication of the strength of the encryption in principle; however, it does not account for the fact that there may still be problems in the way that it is actually implemented in practice.

It is also important to note that although encryption is a primary method for protecting data on an instant messaging service, it is not alone a guarantee of data security. There are numerous other potential flaws and weaknesses in the design and implementation of these services – unrelated to encryption – that could nevertheless make them vulnerable to being compromised.

Moreover, while adequate encryption protects the actual content of communications from being accessed by third parties, it does not generally protect metadata. Metadata is other information associated with communications, such as information about the devices being used, the users of the devices and the manner in which they are being used, such as call times and location records. If cross-referenced with other sources of data, an analysis of metadata can produce an accurate picture of the associations and habits of the participants to a communication.

By focusing only on encryption, the report does not assess the overall security of the IM services, and does not endorse any of the named applications as a secure tool for communications. Amnesty International recommends that journalists, activists, human right defenders and others, whose communications may be particularly at risk, to seek expert digital security advice.

Methodology

Amnesty International initially sent letters to the 11 companies assessed in this report, requesting information about each company's current encryption standards, and details of policies and practices the company has in place to ensure it meets its human rights responsibilities in relation to its online messaging services. Seven companies responded to Amnesty's first letter.

The assessment is based on the companies' responses, together with statements, information and reports that they disclose publicly. Amnesty also assessed the extent to which companies directly inform users of their messaging applications, about the type of encryption used and the extent to which it protects their communications, by downloading and walking through each one and examining what information is made available at each stage.

Amnesty sent follow-up letters to all of the companies, giving them the opportunity to respond to the findings. Six of the companies replied to Amnesty's second letter, and their responses are reflected in the final assessment.

Amnesty did not receive any response from Blackberry, Google, or Tencent.

Amnesty International sought independent expert advice from two cryptographers and cybersecurity specialists, Matthew Green and Frederic Jacobs. Matthew Green is Assistant Professor at the Johns Hopkins Information Security Institute. His research focus is applied cryptography and he also works in the area of cryptographic engineering. Frederic Jacobs is a security engineer who worked as a lead developer on the end-to-end encryption applied to the Signal messaging app. These experts provided explanation of a number of technical issues which informed both our methodology and conclusions. Amnesty would like to express our gratitude for their inputs.

Each company is assessed across five criteria. Amnesty derived the criteria based on an interpretation of international business and human rights standards in the context of encrypted messaging. The criteria are outlined in detail in the following chapter.

Under each criterion, Amnesty gave each company a score between 0 and 3, based on whether the assessment determined that the company met the criterion completely (score 3), substantially but with room for improvement (score 2), only partially (score 1) or not at all (score 0). Each company's overall score is a sum of its rating for each criterion, giving a maximum possible score of 15. For ease of understanding, each companies' overall score was scaled to give a final total out of 100.

3. RANKING CRITERIA

Companies have a responsibility to respect all human rights wherever they operate in the world, as set out in the UN Guiding Principles on Business and Human Rights (UNGPs).[27] This responsibility exists independently of a state's ability or willingness to fulfil its own human rights obligations, and also exists over and above compliance with national laws and regulations.[28]

As part of fulfilling this responsibility, companies need to have a policy commitment to respect human rights, and take ongoing, pro-active and reactive steps to ensure that they do not cause or contribute to human rights abuses – a process called human rights due diligence.

Human rights due diligence requires companies to identify human rights risks linked to their operations, take effective action to prevent and mitigate against them, and be transparent about their efforts in this regard. As the UNGPs make clear, companies "need to know and show that they respect human rights" and "showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders."[29]

Technology companies should ensure that they are adequately addressing the risks their products and services pose to human rights. In the context of IM services, companies should:

- Publicly commit to respect the rights to privacy and freedom of expression, and identify risks to the rights of users of their IM services.
- Take action to respond to human rights risks through the use of encryption on these services.
- Make sure that users of these services, and the wider public, have an accurate picture of the risks in the use of the company's products and services, the measures taken to mitigate those risks, and the actual impact of a company's operations.

Amnesty International has identified the following criteria to assess the extent to which technology companies are meeting their human rights responsibilities in their approach to encrypted messaging.

IDENTIFYING RISKS

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

As the basis for their efforts to meet the responsibility to respect human rights, companies must have a stated commitment to human rights.[30] All of the companies named in this report have a stated commitment

[27] The UNGPs were endorsed by the UN Human Rights Council in 2011. UN Office of the High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011)*, UN Doc HR/PUB/11/04, available at: www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
[28] UNGPs, Principle 11.
[29] UNGPs, Commentary to Principle 21.
[30] UNGPs Principle 16.

to privacy. However, they should also explicitly recognize other rights, including freedom of expression, which may be impacted by their operations.

As a first step in a human rights due diligence process, a company must ensure it knows the human rights risks linked to its activities or its products and services, in order for it to be able to take appropriate action accordingly. This entails identifying any actual or potential adverse impacts on human rights linked to the company's operations.[31]

Risks to the rights to privacy and freedom of expression for users of online communications services are well known, and have been widely recognized in various UN reports, resolutions and decisions.[32] The threat comes from state surveillance of communications, when this is carried out in a manner that does not meet requirements under international law, including necessity and proportionality – including for example, government requests for companies to backdoor encryption. The threat also comes from criminals, malicious hackers and private actors seeking to compromise data in order to defraud or extort money, or to blackmail and harass people.

Technology companies must recognize these threats to people's rights to privacy and freedom of expression through the use of their online services, including their IM services. The companies should have public policies in place designed to support the rights to privacy and freedom of expression. These policies should state what specific measures the company takes to protect users and how it responds to the threats – including the use of encryption.

TAKING ACTION TO RESPOND TO RISKS

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Under international business and human rights standards, after companies identify the risks to human rights associated with their operations, or their products or services, they must take "appropriate action" to address these threats.[33]

Encryption is an important and effective tool for protecting the security of private communications online, and therefore one of the principal actions that these companies can take to respond to human rights risks is to deploy strong encryption on its services. As cybersecurity expert Bruce Schneier makes clear, "Security is more than encryption, of course. But encryption is a critical component of security."[34]

Companies should deploy encryption at a level that is effective against and commensurate to identified risks. This criterion considers whether companies are deploying a form of encryption to their IM services that in principle is effective to prevent and mitigate against the established threats to users privacy and freedom of expression.

END-TO-END ENCRYPTION

All of the messaging apps named in this report have at least a basic form of encryption called transport encryption, in which communications are encrypted between the user and the company's servers. This is largely effective to protect against most interception of internet traffic – for example unsophisticated forms of criminality – and also makes state surveillance more difficult. With transport encryption, the company does have access to the decrypted content of communications.

However, to respond to the human rights risks posed by unlawful state surveillance and cybercrime, Amnesty International considers that at a minimum, companies providing IM must put in place a stronger form of encryption on these services – namely end-to-end encryption. End-to-end encryption exists when the keys to decrypt communications are held exclusively by the sender and recipient of the communication.

---

[31] UNGPs principle 18.
[32] Amnesty International, *Encryption: A Matter of human rights* (Index: POL 40/3682/2016), pp. 13-14, available at: www.amnesty.org/en/documents/pol40/3682/2016/en/See Amnesty International
[33] UNGPs Principle 19.
[34] B. Schneier, *The importance of strong encryption to security*, 25 February 2016, available at: www.schneier.com/blog/archives/2016/02/the_importance_.html

When end-to-end encryption is deployed, any intermediate device or service provider with access to the electronic communications, or any entity attempting to intercept the communications, is unable to read their contents. [35]

If implemented properly, end-to-end encryption is a very effective way for companies to significantly strengthen the security of IM applications, and thereby prevent or mitigate against adverse impacts on users' rights to privacy and freedom of expression. It protects users' communications against interception, not only by government mass surveillance programmes, but also cybercriminals and malicious hackers.

Moreover, by ensuring that companies themselves do not have access to the content of communications, end-to-end encryption is the only way for technology companies to guarantee that they will not be forced to fulfil government requests for access to users' data that are not in line with international human rights standards. It also means that the content of communications are not at risk if the service providers' own systems are compromised by malicious hackers or surveillance – which has happened on numerous occasions in the past.[36] When end-to-end encryption is in place, the content of communications can still be stolen or monitored, but only by compromising one of the 'endpoints', that means, the mobile phone or device of one of the parties to the conversation.

"End-to-end encryption is pretty much the gold standard for securing messaging data."

Matthew Green, cryptographer and Professor of Computer Science, John Hopkins University

There are multiple technical reasons why it is relatively straightforward for companies to put in place end-to-end encryption on messaging applications, particularly on mobile services.[37] For example, unlike communications sent by email, these systems are typically "closed". This means that the developer controls the software that will be used on both sides of the connection, and can put in place strong encryption that seamlessly integrates into the product, and does not have to "interoperate with hundreds of diverse software clients". [38] Expert Matthew Green confirms it is "relatively inexpensive, widely-deployed technology. If you're deploying a messaging technology, the question should be: why are you not using end-to-end encryption?"[39]

APPLIED AS A DEFAULT

However, it is not sufficient for companies just to put in place end-to-end encryption on these services; the way in which the encryption is applied has important implications for security. One of the critical factors is whether companies choose to set end-to-end encryption as an automatic default for all messages sent through the service – or whether this is an option which users must explicitly choose to apply, while the default option is a weaker form of encryption (such as transport encryption).

Privacy advocates have criticized companies which have chosen to make end-to-end encryption an 'opt-in' on their messaging services. In response to Google's announcement of the launch of its new messaging apps Allo and Duo, Edward Snowden said, "Google's decision to disable end-to-end encryption by default in its new Allo chat app is dangerous, and makes it unsafe. Avoid it for now".[40]

Requiring users to 'opt-in' to use end-to-end encryption means that in practice the majority of the users of the service are likely to use a weaker form of encryption, and therefore will remain vulnerable to mass surveillance and cybercrime. Ensuring that end-to-end encryption is put in place as a default is an important action companies can take to respond to threats to users' rights on these services.

Companies have various reasons for choosing not to deploy end-to-end encryption as a default, depending on both the nature of the particular product or service, and on the company's business model. Many

---

[35] Transport encryption and end-to-end encryption both use mathematically strong encryption, which cannot easily be broken without the decryption keys. But with end-to-end, the service provider doesn't hold the key – meaning it is more effective to protect against threats to privacy on instant messaging apps.
[36] See for example, The Financial Times, *'State-sponsored actor' stole data from 500m Yahoo users*, 23 September 2016; Washington Post, *Chinese hackers who breached Google gained access to sensitive data, U.S. officials say*, 20 May 2013; Keys under Doormats pp. 9-10.
[37] Email correspondence with cryptographers and cybersecurity specialists Matthew Green, Assistant Professor at Johns Hopkins Information Security Institute, and security engineer Frederic Jacobs, August 2016
[38] Email correspondence with Frederic Jacobs and Matthew Green, August 2016.
[39] Email correspondence with Matthew Green, August 2016.
[40] ZDNet, *NSA whistleblower Snowden: Google Allo without default encryption is 'dangerous',* 20 May 2016.

technology companies rely substantially on advertising as their primary source of revenue and the ability to tailor advertising to specific users requires the company to be able to access and track the content of the users' communications. A group of security and policy experts have stated that "implementing end-to-end encryption by default for all, or even most, user data streams would conflict with the advertising model and presumably curtail revenues."[41] Furthermore, several companies have added or are planning to add artificial intelligence powered services to their IM apps, which require access to the content of messages.[42]

In the context of instant messaging applications, any business case against deploying end-to-end encryption as a default would not be sufficient to outweigh the need to prevent or mitigate the risks to the rights to privacy and freedom of expression of the users of IM services which are not end-to-end encrypted. This does not preclude the inclusion of services that cannot function with end-to-end encryption, like artificial intelligence powered assistants, or the ability to back up the content of messages to the cloud; however, these should require users to knowingly opt out of end-to-end encryption.

There are also legitimate technical reasons why it is more difficult for some companies to apply end-to-end encryption as a default to their instant messaging services. For example, if the messaging service is already being used on an existing legacy system, particularly if it is used through a web browser like Facebook Messenger, there are challenges for putting in place end-to-end encryption.[43] Cryptographer Matthew Green explains: "If you use [Facebook] Messenger from the web browser there's just no way to do encryption reliably."[44] In addition, on many existing IM services users are accustomed to simultaneously being able to use different devices – that means, seeing the same messages and chat history on their phone, computer and tablet. On such services, it is harder to deploy end-to-end encryption (although it is not impossible).[45] In such cases, as a first step it may be more realistic for companies to add end-to-end encryption as an option rather than as a default, at least until they have overcome the technical challenges.

For the purposes of this assessment, Amnesty International takes the position that companies providing instant messaging services should deploy end-to-end encryption as a default unless they face technical challenges in doing so because of the nature of their service. However, companies should work towards overcoming these challenges and ultimately deploy end-to-end encryption as a default, and should clearly state their intention to do so and a clear timeline.

TRANSPARENCY AND DISCLOSURE

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Companies providing messaging services should inform users on their website and when they sign up about how their rights could be at risk through sharing communications on the service. It should be made clear within the app's user interface what level of encryption is applied and to which messages specifically. Where a stronger form of encryption – such as end-to-end encryption – is an option, there should be clear warnings to users when they switch to the less secure mode that there are greater risks to their private data.

In order to show that they are carrying out adequate human rights due diligence, technology companies should be transparent about the risks to their users' rights to privacy and freedom of expression and how they are addressing these risks, including by deploying encryption to protect security.

---

[41] J.L. Zittrain, M.G. Olsen, D. O'Brien, and B. Schneier, *Don't Panic: Making progress on the "Going Dark" debate*, Berkman Center for Internet & Society, 1 February 2016, p. 11, available at: https://cyber.harvard.edu/pubrelease/dont-panic/
[42] Tech Crunch, *Facebook launches Messenger platform with chatbots*, 12 April 2016; Wired, *Google's New Allo messaging app gets its edge from AI*, 18 May 2016.
[43] Email correspondence with Matthew Green, August 2016.
[44] Motherboard, *Why it's harder to encrypt Facebook Messenger than WhatsApp*, 8 July 2016.
[45] Email correspondence with Matthew Green, August 2016.

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

One particular area where technology companies can and should ensure the maximum level of transparency is over specific government requests for information. Many government requests for users' data will be perfectly legal and in line with requirements under international human rights law. However, if a company is subjected to a demand from a government which is illegal under local law, or complies with local law but would risk breaching international human rights standards, they should challenge such requests and do everything that they can to respect human rights to the greatest extent possible in the circumstances.

There are often limits to the amount of information that technology companies are legally permitted to disclose about government requests for data. For example, in the USA, when companies receive national security orders from the government, there are strict rules about the way that these can be reported, and in many instances companies are forbidden from disclosing the fact they have received such requests.[46] Companies should disclose this data to the fullest extent possible within the law, including the type of request received and whether the company complied with the request.

Importantly, companies should also commit to notifying the specific individual affected that a request has been made for their data. Companies should make clear that those situations where it would not inform users are exceptional and detail the specific circumstances where this would apply.

In the ongoing debate around encryption and governments' fears of 'going dark', technology companies are likely to come under significant legal and political pressure to agree to government requests to circumvent encryption through the use of 'backdoors'. Such requests could be in relation to a specific product or service – such as the FBI's request for a backdoor to the iPhone.[47] There have also been calls by government officials and authorities for regulation to mandate backdoors enabling law enforcement to be able to circumvent encryption across the board. Companies should make a public commitment not to provide a backdoor to their messaging services.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

To meet their responsibility to respect human rights, all companies must be able to demonstrate that they are taking effective steps to prevent and mitigate against adverse human rights impacts linked to their operations. This includes disclosing information that allows key stakeholders and the wider public to evaluate the adequacy of the actions that the company has taken to respond to identified threats to human rights.

In this context, as outlined above, one of the primary actions that a company providing instant messaging services can take to mitigate against violations of the rights to freedom of expression and privacy is to put in place strong encryption.

Companies should therefore ensure that the system of encryption used on these services is disclosed as fully as possible. Such disclosure is important to allow cryptographers and cybersecurity researchers to carry out detailed analyses and audits to determine whether the encryption applied is sound, and to identify any security vulnerabilities or bugs that should be fixed.

At a minimum, companies should publish a technical specification providing details such as the cryptographic algorithms and protocols used, and outlining the process for generating and exchanging keys. However, to provide a fuller guarantee of the security and reliability of the encryption used, companies should go a step further by using an open source encryption protocol. This means publicly disclosing those portions of the application's source code related to encryption. Using an open source protocol enables third-party audits of how the encryption is implemented.

---

[46] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, section 505, Pub. Law No 107-56, 115 Stat. 272 (2001); Electronic Frontier Foundation, *Ruling Unsealed: National Security Letters upheld as constitutional*, 21 April 2016, available at: www.eff.org/press/releases/ruling-unsealed-national-security-letters-upheld-constitutional

[47] Apple, *A Message to Our Customers*, 16 February 2016, available at: www.apple.com/customer-letter/

Cryptographer Matthew Green told Amnesty International that "open source encryption is not only a good move from a transparency point of view, it's also the right move from a security point of view."[48]

SIGNAL

Signal is an IM app developed by Open Whisper Systems (OWS), a non-profit group; it is powered by the Signal Protocol an open source encryption protocol developed by OWS. The protocol has become widely recognized by cryptographers and security experts as the current "gold standard" for encryption applied to IM services.[49] Edward Snowden has endorsed the Signal app, saying that "they do strongly protect your content from precisely this type of in-transit interception".[50] Major IM providers including Facebook, WhatsApp, and Google have also adopted the Signal Protocol for end-to-end encryption in their IM apps. In September 2016, it was revealed that Hillary Clinton's presidential campaign team were using the Signal messenger app.[51]

Amnesty International did not include OWS in its ranking as the report focuses on apps with the largest numbers of users; and while the Signal Protocol is now deployed in apps used by more than one billion users, OWS' own Signal app has a relatively small user base.

[48] Email correspondence with cryptographer and cybersecurity specialist Matthew Green, Assistant Professor at Johns Hopkins Information Security Institute, August 2016.
[49] Email correspondence with Matthew Green, August 2016.
[50] The Daily Dot, *Edward Snowden tells you what encrypted messaging apps you should use*, 6 March 2016.
[51] The Financial Times, *Hillary Clinton adopts start-up's encryption app,* 4 September 2016.

4. COMPANY RANKING

Amnesty International ranked 11 companies against the above criteria, based on an analysis of information publicly disclosed by the company, the company's response, if any, to Amnesty's written request for information, and other sources. The ranking of each company is summarized in the table below, and detailed company-by-company assessments are included in the annex.

Overall assessment

All of the companies assessed apply at least a basic form of encryption to their messaging apps. However, it is evident from Amnesty's assessment that end-to-end encryption has now become best practice for these services. Only three companies (Microsoft, Snapchat and Tencent) do not offer any form of end-to-end encryption to users of their IM services (although Blackberry only offers end-to-end encryption as a paid subscription service).

However, only three of the companies assessed apply end-to-end encryption as a default to all of their IM services. Most of the companies also do not disclose full technical information about how they implement encryption, making it more difficult for security experts to confirm that the encryption is sound. None of the companies deploys end-to-end encryption as a default to all of its instant messaging services, while also using an open source encryption protocol. Amnesty International considers that this is a minimum requirement for the system of encryption applied to IM services. Notably, while Facebook's WhatsApp meets both criteria, its other IM app, Facebook Messenger, does not.

All of the companies have a stated commitment to privacy. Some have been at the forefront of the recent debate around encryption, arguing that government proposals to undermine the security of their products and services pose grave risks to privacy. Although Apple has been most visible in resisting state authorities' attempts to backdoor encryption, most of the companies assessed have either supported Apple's position or have otherwise spoken out publicly on the importance of privacy and security.[52]

However, in five cases – most starkly Microsoft – there was a gap between the company's stated commitment to privacy and recognition of the threats to human rights, and the level of encryption applied to their IM service. Also, the majority of those assessed do not have a stated commitment to freedom of expression.

On transparency, eight out of the 11 companies responded to Amnesty International's request for information, thereby showing a willingness to engage on these critical issues. It is disappointing that Amnesty did not receive a response from Blackberry, Google or Tencent.

Very few of the companies assessed provide adequate information within the user interface of their messaging apps about the risks to human rights and the level of encryption applied to the service. WhatsApp is the only app where users are explicitly warned when end-to-end encryption is not applied to a particular chat or conversation. On the apps where end-to-end encryption is only applied as an option (Facebook Messenger, Google's Allo, KakaoTalk, Telegram), or that combine IM with regular SMS messages

[52] *Amicus Briefs in Support of Apple*, available on Apple's website at: www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html

(iMessage), there is insufficient information to ensure users fully understand the different levels of security applied – and how their rights are at greater risk when using the weaker option.

Half of the companies surveyed are transparent in providing details of the number of requests they receive from governments for their users' personal data. It is unsurprising that all of the US-based companies now publish transparency reports containing this information, given the Snowden revelations about the role of corporations in the US's PRISM surveillance programme. However, government surveillance is by no means exclusively a US concern; all companies around the globe must disclose as much information as possible to shed light on the extent to which they are being asked to give up data about their users, and the nature of these requests.

In this vein, it is encouraging that all of the companies, with the exception of Tencent, have stated publicly that they will not grant government requests to backdoor the encryption on their messaging services.

Message Privacy Ranking: How the companies scored

COMPANY	IM SERVICES ASSESSED	1. RECOGNISES ONLINE THREATS TO HUMAN RIGHTS?	2. DEPLOYS END-TO-END ENCRYPTION AS A DEFAULT?	3. INFORMS USERS OF RISKS AND ENCRYPTION USED?	4. DISCLOSES GOVERNMENT REQUESTS FOR USER DATA?	5. PUBLISHES TECHNICAL DETAILS OF ENCRYPTION?	OVERALL SCORE /100
FACEBOOK	**FB MESSENGER, WHATSAPP**	Yes, but only committed to freedom of expression through participation in multi-stakeholder initiative. **Score 2**	Yes, but only on WhatsApp, not on Messenger. **Score 2**	Inadequate notification within the apps, no warning in Messenger when using weaker encryption. **Score 1**	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. **Score 3**	Yes, both apps use open source Signal protocol, provide specification. **Score 3**	**73**
APPLE	**IMESSAGE, FACETIME**	Yes, but no policy commitment to freedom of expression. **Score 2**	Yes. **Score 3**	Inadequate notification within the apps. **Score 1**	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. **Score 3**	Some specification of encryption, but protocol not open source. **Score 1**	**67**
TELEGRAM	**TELEGRAM MESSENGER**	Yes, stated commitment to rights and recognition of online threats. **Score 3**	Has end-to-end encryption, but not set as a default. **Score 1**	Inadequate notification within the apps; no warning when using weaker encryption. **Score 1**	Commitment not to share user data, but no transparency report with details of requests received. Has taken public stance against encryption backdoors. **Score 2**	Yes, app is open source, although encryption implementation criticised. **Score 3**	**67**
GOOGLE	**ALLO, DUO, HANGOUTS**	Yes, but only committed to freedom of expression through participation in multi-stakeholder initiative. **Score 2**	Yes on Duo; but only as an option on Allo, Hangouts not at all. **Score 1**	Inadequate notification within the apps; no warning in Allo when using weaker encryption. **Score 1**	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. **Score 3**	Allo uses open source Signal, but not published specification yet. **Score 1**	**53**
LINE	**LINE**	Commitment to rights, but no policy recognition of threats. **Score 1**	Yes. **Score 3**	Inadequate notification within the app. **Score 1**	No, does not publish transparency report. Has taken public stance against encryption backdoors. **Score 1**	Provides specification of encryption, but not open source protocol. **Score 1**	**47**
VIBER MEDIA	**VIBER**	No commitment to freedom of expression, no policy recognition of threats. **Score 1**	Yes. **Score 3**	Inadequate notification within the app. **Score 1**	No, does not publish transparency report. Has publicly rejected encryption backdoors. **Score 1**	Provides specification of encryption, but not open source protocol. **Score 1**	**47**
KAKAO INC	**KAKAO TALK**	Commitment to rights, but no policy recognition of threats. **Score 1**	Has end-to-end encryption, but not set as a default. **Score 1**	Inadequate notification within the apps; no warning when using weaker encryption. **Score 1**	Publishes transparency report. Has taken public stance against encryption backdoors. **Score 3**	Only basic information on system of encryption. **Score 0**	**40**
MICROSOFT	**SKYPE**	Yes, clear commitment to rights and recognition of online threats. **Score 3**	Skype does not have end-to-end encryption. **Score 0**	No information or warnings within app about level of encryption on Skype. **Score 0**	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. **Score 3**	No specification of Skype system of encryption. **Score 0**	**40**
SNAPCHAT	**SNAPCHAT**	No commitment to freedom of expression, no policy recognition of threats. **Score 1**	Snapchat does not have end-to-end encryption. **Score 0**	No information given to users on website or in app about level of encryption. **Score 0**	Yes, and notifies affected user. Refuses to backdoor encryption. **Score 3**	No specification of Snapchat system of encryption. **Score 0**	**26**
BLACKBERRY	**BLACKBERRY MESSENGER**	No commitment to freedom of expression, no policy recognition of threats. **Score 1**	No, only offers end-to-end encryption as separate paid service. **Score 0**	Explanation on website, but no reference to encryption within app itself. **Score 1**	No, does not publish transparency report. Has publicly rejected encryption backdoors, but alleged cases where not done so in practice. **Score 0**	Provides specification of encryption, but not open source protocol. **Score 1**	**20**
TENCENT	**QQ, WECHAT**	No recognition of threats, no commitment to freedom of expression. **Score 0**	WeChat not end-to-end encrypted, QQ encryption unclear. **Score 0**	No information given to users on website or in app about level of encryption. **Score 0**	No. Does not publish transparency report, does not publically refuse to backdoor encryption. **Score 0**	No specification about encryption. **Score 0**	**0**

5. CONCLUSION AND RECOMMENDATIONS

In the digital age, encryption is a bulwark against online threats to human rights. It helps protect human rights activists from being targeted by authorities because of their work, and helps protect everyone from the threats of cybercrime and of private communications being harvested by intelligence agencies. Encryption provides a space within which people are free to express themselves and share opinions without fear.

Technology companies have a responsibility to apply encryption in response to risks to the rights to privacy and freedom of expression. Amnesty International's ranking shows that the 11 technology companies assessed all have room for improvement. It also exposes a gap between the companies that are taking a lead in protecting users' data security through encrypted messaging and the companies lagging behind their peers.

There is no excuse for not putting in place end-to-end encryption on instant messaging services. Companies that are still entirely relying on a weaker form of encryption, such as Blackberry, Microsoft, Snapchat and Tencent, are putting the personal communications of the millions of people using their services at greater risk. As such, they are failing to meet their responsibility to respect the human rights to privacy and freedom of expression.

Yet all of the companies must increase their transparency, so that people are fully informed about the extent to which they are protected against these threats when they use IM services.

Technology companies face increasing pressure from state authorities to provide access to their users' data – not only through lawful requests for information about specific individuals, but through measures that would systemically weaken and undermine encryption. How the companies choose to respond will affect the rights to privacy and freedom of expression of everyone.

Many of the companies assessed have so far taken a public position in support of privacy and security. To bolster this position and to demonstrate their commitment to act in the interests of their users, the wider public, and those around the world whose rights online are most at threat, companies must now show that they are adopting a human rights approach.

Recommendations for the companies are implicit in the ranking criteria themselves. Overall, Amnesty's three key recommendations for all companies providing instant messaging services are as follows:

1. Deploy end-to-end encryption as a default on all instant messaging services, and publish as open source all parts of the app's source code relevant to encryption.

2. Clearly inform users of its instant messaging services about the level of encryption applied to the service and how this mitigates against risks to users' human rights.

3. Publish regular transparency reports outlining – in as much detail as legally permitted – the number and nature of government requests for user data the company has received and how the company responded, and challenge government restrictions on disclosure of such data that don't comply with international law.

ANNEX: COMPANY-BY-COMPANY ASSESSMENT

APPLE

Apple's instant messaging services are iMessage, for sharing text, photo and videos, and FaceTime, its video calling app. There are few figures available of the number of users on these services, but given the company has sold a total of almost 1 billion iPhones, it is reasonable to assume that millions of people use the services daily.[53]

Apple is a powerful advocate for privacy and security and is applying a strong form of encryption to its services. However, Amnesty International found that the company could do more to tackle these issues from a human rights perspective and inform its users about the threats to their human rights and the way that the company is responding.

Apple replied to Amnesty International's second letter, providing information in response to our assessment.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Apple as 2 for this criterion.

Apple has a strong stated commitment to privacy and data security and provides information on what actions it takes to protect privacy. In its 'Approach to Privacy' statement, the company says it builds "powerful safeguards into our operating systems, our apps and the devices themselves", and outlines the encryption applied to particular products and services, including iMessage and FaceTime.

Through its participation in the Reform Government Surveillance coalition of technology companies, Apple recognizes threats to the rights to privacy and freedom of expression posed by state surveillance and argues for governments to strengthen legal protections of these rights in the context of surveillance.[54]

However, the company's publicly available policies do not have a stated commitment to the right to freedom of expression. The company only refers explicitly to human rights in the context of its supply chain, rather than in relation to its own products and services. For this reason, Amnesty was unable to give Apple the highest ranking marks for this criterion.

In response to Amnesty International, Apple pointed to public statements made by its CEO Time Cook, defending the right to free speech. For example, in a March 2016 interview, Cook said, "When I think of civil liberties, I think of the founding principles of this country. The freedoms that are in the First Amendment, but also the fundamental right to privacy." He added that "… you don't take away the good for that sliver of bad. We've never been about that as a country. We make that decision every day, right? There are some times

[53] The Financial Times, *Apple iPhone sales set to pass 1bn milestone*, 24 July 2016, available at: www.ft.com/cms/s/0/3e2b61a2-500a-11e6-8172-e39ecd3b86fc.html
[54] Reform Government Surveillance website: www.reformgovernmentsurveillance.com/

that freedom of speech, we might cringe a little when we hear that person saying this and wish they wouldn't. This, to us, is like that. It's at the core of who we are as a country."[55]

CRITERION 2: DOES THE COMPANY DEPLOY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Apple as 3 for this criterion.

Apple applies end-to-end encryption as a default to both iMessage and FaceTime, meaning in principle it has put in place a strong form of encryption on these services, and the company itself does not have access to the content of users' communications.

However, iMessage is an important example of how the form of encryption applied to a messaging service does not guarantee security. A team of researchers from John Hopkins University carried out an analysis of iMessage to determine the security of the protocol against a variety of attacks. They found "significant vulnerabilities" that could be used by an attacker to decrypt communications on iMessage.[56] Apple has taken steps to mitigate against these flaws in the latest version of its software – nevertheless, this demonstrates that even when end-to-end encryption is applied as default, there can still be important vulnerabilities in the way the encryption is actually implemented in practice.

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Apple as 1 for this criterion.

Apple has publicly asserted its commitment to privacy and to protecting the digital security of its users. On its website it outlines in accessible terms the encryption that it applies to iMessage and FaceTime, how this protects users' communications, and that Apple "wouldn't be able to comply with a wiretap order even if we wanted to."

However, the company does not do enough to inform users within the apps themselves about risks to human rights and encryption. iMessage uses the same interface as standard text messages, and although the two are distinguished by colour (blue and green respectively), it is not made clear to users the different security standards applied to each one. This is especially important given that standard text messages are not protected by any form of encryption.

When Amnesty International raised this issue with Apple, the company responded by publishing new guidance on its website explaining the difference between iMessage and SMS, including the level of encryption.[57] This is a welcome step, but Apple should make this clear within the messaging services themselves. There is no notification within iMessage or FaceTime telling users what level of encryption is applied to the service, and how this addresses threats to human rights.

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Apple as 3 for this criterion.

Apple publishes a Transparency Report twice a year outlining details concerning the number of requests for information it has received from governments. The company says that for government information requests, "we report as much detail as we are legally allowed." It also publishes guidelines for law enforcement outlining how it responds to requests.

Apple has called for governments to allow companies to be more transparent about government demands for user information. In September 2016 the company filed a legal brief supporting Microsoft in its case against the US government on this issue (see Microsoft section below).[58]

---

[55] TIME, *Inside Apple CEO Tim Cook's Fight with the FBI,* 17 March 2016.
[56] C. Garman, M. Green, G. Kaptchuk, I. Miers, M. Rushanan, John Hopkins University, *Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage*, 2016, (hereinafter: *Dancing on the Lip of the Volcano*) available at: https://isi.jhu.edu/~mgreen/imessage.pdf
[57] Apple, *About iMessage and SMS/MMS*, available at: https://support.apple.com/en-us/HT207006
[58] *Brief as Amici Curiae by Apple, Lithium Technologies, Mozilla and Twilio in support of Microsoft Corporation's opposition to defendant's motion to dismiss*, 2 September 2016, in *Microsoft Corporation v. The United States Department of Justice*, case number 2:16-cv-00538, available at: https://blog.mozilla.org/wp-content/uploads/2016/09/Mozilla-Brief-of-Joint-Amicus-in-MSFT-v.-DOJ.pdf

The company also has a policy to notify users if a request has been made concerning their personal data, unless it is explicitly prohibited from doing so, and in certain exceptional cases.

Apple has made a strong public commitment not to backdoor its encryption. In a statement on the company's website, CEO Tim Cook states "we have never worked with any government agency from any country to create a backdoor in any of our products or services. We have also never allowed access to our servers. And we never will."[59] Amnesty International could find no evidence nor public suggestion that Apple has, in practice, contravened this position. Moreover, as outlined above, Apple has defended this position in court.

Amnesty concluded that Apple has a high level of transparency about government requests for user information.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Apple as 1 for this criterion.

In its iOS Security Guide, Apple publishes a specification of the encryption applied to both iMessage and FaceTime.[60] This provides a brief overview of the process for generating and exchanging keys. However, the encryption protocol applied to these apps is not open source. The analysis of the iMessage cryptography by John Hopkins researchers found that this overview, taken together with previous efforts to identify Apple's encryption, still omit "key details of the encryption mechanism, as well as the complete key registration and notification mechanisms."[61] The researchers recommended that Apple adopt a different, more open protocol.

In response to Amnesty International, Apple stated that "we are extremely transparent in relation to how end to end encryption works within iMessage and FaceTime, including in our Security Whitepaper."

BLACKBERRY

Blackberry is a Canadian-based company. Although best known as a developer of smartphones, the company also provides an instant messaging app, Blackberry Messenger (BBM), which is reported to have 100 million users.[62]

Blackberry's CEO John Chen has been a public voice in the debate over encryption. He has rejected proposals to ban or disable encryption, while arguing that technology companies should not refuse "reasonable, lawful access requests" made by governments, stating that Blackberry's privacy commitment "does not extend to criminals."[63]

Blackberry did not respond to Amnesty International's request for information, therefore our assessment is based on our review of publicly available information.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Blackberry as 1 for this criterion.

Blackberry has a human right policy which includes the company's commitment to privacy. This is further elaborated in its Privacy Policy.

However, the company's human rights policy does not include a commitment to the right to freedom of expression. The company also does not explicitly recognize the threats to users' privacy and freedom of expression posed by government surveillance.

---

[59] *Apple's commitment to your privacy*, available at: www.apple.com/uk/privacy/
[60] Apple, *iOS Security Guide*, pp. 41-42, May 2016, www.apple.com/business/docs/iOS_Security_Guide.pdf
[61] *Dancing on the Lip of the Volcano*, p. 3.
[62] Statista, *Leading social networks worldwide as of September 2016, ranked by number of active users,* September 2016, available at: www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
[63] J. Chen, Executive Chairman and CEO of Blackberry, *The Encryption Debate: a Way Forward,* 15 December 2015, (*The Encryption Debate: a Way Forward*) available at: http://blogs.blackberry.com/2015/12/the-encryption-debate-a-way-forward/

Blackberry's Privacy Policy provides general information about how it safeguards users' information, stating only that "BlackBerry continues to evolve our physical, organizational and technological measures used to protect your personal information." It does not make any reference to encryption.

Amnesty concluded that although Blackberry has a stated commitment to the right to privacy, its policies do not recognize what the threats to users' privacy are, or what actions the company takes to respond. It also does not recognize how its product and services pose a risk to other human rights, such as the right to freedom of expression.

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Blackberry as 0 for this criterion.

Messages sent through BBM are sent using Transport Layer Encryption; there is no option for end-to-end encryption. This means that the company does have access to the decrypted content of users' communications.

Blackberry offers a secure messaging service, BBM Protected, in which messages are end-to-end encrypted. However, this is primarily targeted at Blackberry's corporate clients, and requires a paid subscription.[64] It is not otherwise available as an option for users of the BBM app. It is troubling that Blackberry acknowledges the importance of stronger encryption, and has the capability to apply it to its messaging service, but has decided to provide different levels of protection to users based on an ability to pay. Amnesty concluded that Blackberry is not meeting its responsibility to respect the rights of regular users of its BBM app.

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Blackberry as 1 for this criterion.

In the user support pages of its website, Blackberry outlines how BBM and BBM Protected protect messages, including the form of encryption applied to both apps.[65]

However, the company does not inform users about the threats to their human rights when using its messaging services, either on its website or when signing up to the service.

Within the BBM app itself, there is no information given to users about threats to privacy or other human rights, or on the level of encryption applied to the service. This means that users are unaware how the company is protecting their communications when they use BBM.

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Blackberry as 0 for this criterion.

Blackberry does not disclose figures regarding government requests for information that it has received. A Blackberry spokesperson also publicly stated that it does not have plans to publish a transparency report in the near future.[66]

Blackberry's CEO has publicly stated that "BlackBerry has refused to place backdoors in its devices and software. We have never allowed government access to our servers and never will."[67] In November 2015, the company decided to pull out of Pakistan after demands from the government for open access to its servers.[68] This decision was welcomed by digital rights groups.[69]

---

[64] Blackberry, Overview of BBM Protected, available at: http://support.blackberry.com/kb/articleDetail?ArticleNumber=000035648)
[65] Blackberry, *BBM security*, available at: http://help.blackberry.com/en/bbm-security; *BBM Protected security*, available at: http://help.blackberry.com/en/bbm-protected-security
[66] Z. Whittaker, ZDNet, *BlackBerry, once a security pioneer, falls behind on privacy, transparency*, 19 November 2015, available at: www.zdnet.com/article/blackberry-has-no-plans-for-locking-out-feds-from-data-demands/
[67] *The Encryption Debate: a Way Forward*.
[68] M. Beard, Chief Operating Officer, Blackberry, *Why BlackBerry is Exiting Pakistan,* 30 November 2015, available at: http://blogs.blackberry.com/2015/11/why-blackberry-is-exiting-pakistan/
[69] Access Now and 10 other NGOs, *Open letter to BlackBerry on rejecting backdoors and protecting human rights*, 22 December 2015, available at: https://www.accessnow.org/13354-2/

However, Blackberry's consumer messaging service uses a shared global encryption key, and an April 2016 investigation by Motherboard and Vice News reported that Blackberry had given its global encryption key to the Royal Canadian Mounted Police in connection with a criminal investigation.[70] This would essentially amount to giving a 'front door' to law enforcement, enabling access to all messages sent through BBM (although only consumer messages, as the company's business service allows companies to generate their own keys).

Blackberry CEO responded to the allegations stating "regarding BlackBerry's assistance, I can reaffirm that we stood by our lawful access principles. Furthermore, at no point was BlackBerry's BES server involved. Our BES continues to be impenetrable – also without the ability for backdoor access – and is the most secure mobile platform for managing all mobile devices."[71] However, this statement was not adequate, as it pointed only to the company's business service, which would anyway not have been affected. The CEO did not make any assurances about the security of BBM's consumer service. The company's 'lawful access principles' do not provide any assurances that the company will only comply with requests for information related to specific individuals or accounts, rather than indiscriminate access to all communications.

Between 2008 and 2013, Blackberry was also involved in a long-running dispute with the Indian government over law enforcement access to its services. Blackberry ultimately refused to give the Indian government access to communications under the company's corporate services, but stated that it did provide an "appropriate lawful access solution" to its consumer services, including BBM.[72] It remains unclear what this entailed and whether Blackberry gave the Indian authorities encryption keys for these services.

Amnesty concluded that Blackberry is not transparent about how it responds to government requests for user information. Although it is welcome that the company has stated it does not provide backdoor access to its encryption, there are alleged cases where the company has not met this commitment in practice. If the company did provide state authorities with access to all encrypted communications, this would disproportionately affect the privacy of its users.

In both instances, the company's public response provided reassurance of the security of its corporate services, while failing to provide details of how the company protects individuals using its consumer services. Amnesty International gave Blackberry the opportunity to provide further comment on these specific cases, but the company had not responded at the time of publication.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Blackberry as 1 for this criterion.

Blackberry publishes whitepapers that provide a specification of the encryption applied to both BBM and BBM Protected.[73] However, the company does not use an open source encryption protocol.

FACEBOOK

The US-based social media company Facebook controls the two instant messaging services with the most number of users worldwide: Facebook Messenger and WhatsApp, which each have 1 billion active users.[74]

Facebook responded to Amnesty International's request for information on behalf of both Facebook and WhatsApp.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Facebook as 2 for this criterion.

---

[70] J. Ling and J. Pearson, Vice News and Motherboard, *How Canadian Police Intercept and Read Encrypted BlackBerry Messages,* 14 April 2016, available at: http://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada
[71] J. Chen, *Lawful Access, Corporate Citizenship and Doing What's Right,* 18 April 2016, available at: http://blogs.blackberry.com/2016/04/lawful-access-corporate-citizenship-and-doing-whats-right/#disqus_thread
[72] Reuters, *RIM: BlackBerry security not compromised in India*, 2 August 2012, available at: http://in.reuters.com/article/rim-india-blackberry-idINDEE87101A20120802
[73] Blackberry, *BBM Protected Security Note*, June 2016; *BBM Security Note*, May 2015.
[74] Facebook, *Thank You Messenger*, 20 July 2016; WhatsApp, *One Billion*, 1 February 2016.

Facebook has made a commitment to the rights to privacy and freedom of expression through its participation in the Global Network Initiative (GNI).[75] This includes a commitment to "employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of users." The 'Privacy Basics' section of its website indicates the measures Facebook puts in place to protect privacy, including encryption.

The company has recognized the threat to human rights posed by state surveillance through its membership of the Reform Government Surveillance coalition of technology companies.

Through the GNI, Facebook is subject to a regular independent assessment of the company's relevant internal systems, policies and procedures. The first assessment of Facebook published in July 2016 found that Facebook has "established policies and procedures to implement the GNI Principles into daily operations", and concluded the company was in compliance with the principles.[76]

However, the GNI Assessment process is confidential, meaning Amnesty International is unable to verify this conclusion. Facebook's publicly available policies include a clear commitment to privacy, but do not state Facebook's commitment to freedom of expression, which is only reflected in the company's participation of GNI. As a result, Amnesty scored the company as 2 for this criterion.

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Facebook as 2 for this criterion.

There are different levels of encryption applied to Facebook's Messenger and WhatsApp services.

In April 2016, WhatsApp announced that it had put in place end-to-end encryption across its entire service, meaning that it is applied to all communications, including text messages, photos, videos, and voice calls, and to both one-on-one messaging and group chats.[77] WhatsApp also deploys end-to-end encryption as a default, meaning that it is automatically applied to all communications (provided users are using the latest version of the software). Given the large number of people worldwide using the app, this decision was welcomed by privacy advocates as a significant step in strengthening online security.[78]

Facebook subsequently announced that it has started testing end-to-end encryption on its Messenger app, based on the same encryption protocol applied to WhatsApp.[79] However, unlike WhatsApp, end-to-end encryption is not set as a default on Messenger, and is only applied to messages and photos sent through a 'Secret Conversations' option. For regular messages, Messenger "uses secure communications channels like HTTPS with forward secrecy" – that means Transport Layer Security.[80] This means that messages are encrypted between the user and Facebook, but the company does have access to the unencrypted content.

Facebook's decision to introduce end-to-end encryption as an option rather than a default on Messenger has been criticized by privacy advocates. Nate Cardozo, a senior attorney with the Electronic Frontier Foundation, said: "The fact that it is not on by default means that Messenger can't and shouldn't be treated as a secure platform."[81]

---

[75] The Global Network Initiative (GNI) is a multi-stakeholder group of companies, NGOs, academics and investors set up to address issues of privacy and freedom of expression linked to the ICT sector. GNI participants commit to a set of principles, as well as a governance structure. The GNI has been criticized by some civil society organizations, including Amnesty International. In February 2016, the NYU Center for Business and Human Rights resigned its membership, citing concerns including weaknesses in the GNI's accountability mechanisms. In 2013, the Electronic Frontier Foundation resigned from GNI, citing a fundamental breakdown in confidence that the group's corporate members are able to speak freely about their own internal privacy and security systems in the wake of the Snowden revelations. For more information see Global Network Initiative website: http://globalnetworkinitiative.org/
M. Posner and S. Labowitz, *NYU Center for Business and Human Rights resigns its membership in the Global Network Initiative*, 1 February 2016, available at: http://bhr.stern.nyu.edu/statement/cbhr-letter-of-resignation-gni
EFF, *EFF Resigns from Global Network Initiative*, 10 October 2016, available at: www.eff.org/press/releases/eff-resigns-global-network-initiative

[76] GNI, *Public Report on the 2015/16 Independent Company Assessments*, pp. 21-22, 7 July 2016.

[77] WhatsApp blog, *End-to-end encryption*, 5 April 2016, available at: https://blog.whatsapp.com/10000618/end-to-end-encryption

[78] For example, security researcher Kenneth White, Director of the Open Crypto Audit Project, quoted in Threatpost, *WhatsApp Encryption A Good Start, But Far From a Security Cure-all,* 6 April 2016, available at: https://wp.me/p3AjUX-uuO

[79] Facebook, *Messenger starts testing end-to-end encryption with eecret conversations*, 8 July 2016.

[80] Facebook letter to Amnesty International, 3 August 2016 (Facebook letter).

[81] Quoted in Buzzfeed, *You'll have To Turn On Encryption To Protect Your Facebook Messages*, 8 July 2016.

Facebook claims the reason behind its decision is that "secret conversations are designed to enable these conversations to be read only on the sending and receiving devices".[82] This means Messenger users cannot see secret conversations when switching between multiple different devices such as phone, tablet and laptop, and the company says this experience "may not be right for everyone".[83] Facebook's Chief Security Officer Alex Stamos said "FBM is multi-device, and we'd like to see E2E usability improve to support this".[84]

This argument does not entirely hold up. The Signal protocol used by Facebook for Secret Conversations and WhatsApp already supports multi-device, and both WhatsApp and the Signal app allow the use of different devices. But another reason given by Stamos is that, "Hundreds of millions use Messenger from a web browser. No secure way to verify code or store keys without routing through mobile."[85] Amnesty International consulted a technical expert who advised that it is true that there may be real technical challenges to deploying end-to-end encryption across a web browser.[86] This makes it difficult for Facebook to integrate Secret Conversations into the Facebook website or the browser-based version of Messenger. As a result, Secret Conversations only currently work through the Messenger app on phones or tablets.

Taking into consideration the various factors, Amnesty International has ranked Facebook as 2 for this criterion. WhatsApp already has end-to-end encryption as a default, and although Facebook should aim to achieve the same for Messenger, it does face legitimate implementation challenges that do not apply to other IM services. Introducing end-to-end encryption as an option is a good first step, but Facebook should commit to deploy end-to-end encryption as a default on Messenger in future and provide a clear timeline for doing so.

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Facebook as 1 for this criterion.

Facebook provides resources on its website which give clear and accessible information outlining its privacy policy, how it protects user data including through encryption on Messenger and WhatsApp, and how it deals with government requests for information.

Within the apps themselves, WhatsApp sends a notification informing users when messages sent between individuals or in group chats are end-to-end encrypted and users can check whether specific conversations are encrypted. The app also sends a clear notification when messages are not end-to-end encrypted.

However, WhatsApp does not do enough to warn users about the privacy implications of backing up messages to the cloud. Like many messaging apps, WhatsApp has an option that allows users to back-up their chat histories to Google Drive, iCloud, or a local backup. This enables messages to be restored if the phone is lost or stolen, and so is clearly a feature that many find useful. But because by their nature, these messages must be capable of being decrypted when retrieved from the cloud, the content of backed-up chats are no longer end-to-end encrypted between only the recipients, and are capable of being accessed by the cloud provider. The notification WhatsApp sends to users about the backup feature does not make this clear.

Messenger has a link to user-friendly tools and information about Facebook's Data Policy, including how the company responds to legal requests for data. There is a clear option to switch to 'Secret Conversations' when opening any new message, and it is then differentiated with a lock symbol. However, Messenger does not warn users when switching to regular conversations that this is a lower level of encryption, and what the implications are for their data security and human rights.

Facebook should do more to inform users how their rights to privacy and freedom of expression are under threat when they communicate through Facebook's IM services. Although the company recognizes the threat posed by government surveillance, it does not make this clear on the WhatsApp or Messenger

[82] Facebook letter.
[83] Facebook letter.
[84] Tweet by Alex Stamos, 8 July 2016, available at: https://twitter.com/alexstamos/status/751416166032117760
[85] Tweet by Alex Stamos, 8 July 2016, available at: https://twitter.com/alexstamos/status/751416491317161984
[86] Email correspondence with cryptographer and cyber-security specialist Matthew Green, Assistant Professor at Johns Hopkins Information Security Institute, August 2016.

websites. The company also does not clearly state – either on its website or within its messaging apps – its commitment to all internationally-recognized human rights, including freedom of expression.

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Facebook as 3 for this criterion.

Facebook's Global Transparency Report provides figures of the number of requests it has received from governments on a country-by-country basis. The figures relate to its products and services including Messenger and WhatsApp and include a percentage of requests where some data is produced. Facebook's policy is to notify users of requests for their information prior to disclosure "unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when providing notice would be counter-productive."[87] Facebook has also stated that it will notify users "whose account has been targeted by an attacker suspected of working on behalf of a nation-state."[88]

The company provides guidance for law enforcement officials seeking records from Facebook and says that "our team carefully evaluates each request for compliance with applicable law, appropriate jurisdiction, and consistency with internationally recognized standards."

Facebook states in its response to Amnesty International that "we do not provide 'back doors' into our systems."[89] As outlined above, WhatsApp has been also involved with public disputes with law enforcement agencies including the Brazilian authorities and the FBI, indicating that these countries do not have exceptional access to the service.[90] There has been no evidence nor public suggestion that Facebook has breached its policy commitment in these cases.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Facebook as 3 for this criterion.

Messenger's 'Secret Conversations' and WhatsApp both use the Signal encryption protocol, which is open source and has been extensively reviewed by cryptography experts. Facebook has also published whitepapers for both apps providing a technical specification of how the encryption is deployed.[91]

Regular conversations through Messenger (that means, not Secret Conversations) rely on different encryption protocols. The Messenger app uses MQTT protocol.[92] Messages sent through a browser are encrypted as a default through the HTTPS protocol.[93]

GOOGLE

Until recently, the primary instant messaging service of the US-based internet company Google (now a subsidiary of Alphabet Inc.) was Google Hangouts. Hangouts enables messaging, voice and video calls via mobile phone apps as well as through a web browser. However, Google recently launched two new messenger apps for mobile – Allo, an app for sharing text messages, videos and photos, and Duo, a video calling app – which were released in August and September 2016 respectively.

Google has not reported specific user statistics for Hangouts, however independent estimates have put Google's total user base to be more than 2 billion.[94] Duo was downloaded more than 5 million times on Android in the first week after it launched.[95]

---

[87] Facebook, *Information for law enforcement authorities*, available at: https://en-gb.facebook.com/safety/groups/law/guidelines/
[88] Facebook letter.
[89] Facebook letter.
[90] The New York Times, *WhatsApp encryption said to stymie wiretap order*, 12 March 2016, available at: www.nytimes.com/2016/03/13/us/politics/whatsapp-encryption-said-to-stymie-wiretap-order.html
[91] WhatsApp, *Encryption Overview: Technical Whitepaper*, 4 April 2016; Facebook, *Messenger Secret Conversations: Technical Whitepaper*, 8 July 2016.
[92] L. Zhang, Facebook software engineer, *Building Facebook Messenger*, 12 August 2011, available at: www.facebook.com/notes/facebook-engineering/building-facebook-messenger/10150259350998920
[93] Facebook, *Secure browsing by default*, 21 July 2013.
[94] Stone Temple Consulting, *Hard Numbers for Public Posting Activity on Google Plus*, 14 April 2015, available at: www.stonetemple.com/real-numbers-for-the-activity-on-google-plus/ (accessed September 2016)
[95] Android Police, *Google Duo has been downloaded 5 million times on Android since its release*, 25 August 2016.

Amnesty International has engaged with Google on encryption; however, Google did not provide information in response to Amnesty International's letter, therefore our assessment is based on a review of publicly available information.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Google as 2 for this criterion.

Like Facebook and Microsoft, Google has made a commitment to the rights to privacy and freedom of expression through its participation in the Global Network Initiative. The company also recognizes threats to human rights posed by state surveillance through its membership of the Reform Government Surveillance coalition of technology companies. The company's Privacy Policy lists some of the actions that the company takes to protect privacy, including encryption.

Google did not respond to Amnesty International's letter requesting details of its policies and procedures. Google's publicly available policies include a commitment to privacy, but do not state the company's commitment to freedom of expression, which is only reflected through the company's participation in GNI. As a result, Amnesty ranked the company as 2 for this criterion.

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Google as 1 for this criterion.

Google Hangouts currently use transport encryption, meaning that communications are not end-to-end encrypted but are encrypted between the user and Google's servers.[96]

Duo applies end-to-end encryption as a default for all video calls, but in Allo, end-to-end encryption is only offered as an option and is only applied when users choose the 'Incognito' mode.[97]

Putting in place end-to-end encryption on Hangouts would present some technical challenges, given that it would need to be deployed to a legacy client, and users are already accustomed to its functioning on multiple different devices including through a web browser.

However, these challenges do not apply to the new Allo and Duo apps, which have been developed from scratch and which are only available through mobile apps. Google has indicated that its decision not to apply end-to-end encryption to all messages as a default on Allo was because other features – specifically its Google Assistant, an artificial intelligence bot – would otherwise not be able to function.[98] This decision was strongly criticized by privacy advocates when Allo was announced in May 2016. When the app was launched in September 2016, the company came under renewed criticism for failing to include other privacy protections it had previously promised to add to Allo.[99]

To adequately respond to well-known human rights risks posed by third parties, Google should deploy end-to-end encryption as a default on all its messaging services. This would enable it to meet its responsibility to respect human rights. It is a fact that it is technically challenging to combine artificial intelligence with end-to-end encryption.[100] However, if the company decides to include another mode with additional features but a lower level of encryption, this should not be set as the default option, and users should be given clear warnings about the risks to their human rights when switching to the less secure mode.

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Google as 1 for this criterion.

As outlined above, Google has a clear public commitment to privacy. Overall, it has a variety of tools and materials showing how users can manage privacy settings and personal data across Google's entire range of

---

[96] Google, *How Hangouts encrypts information*, available at: https://support.google.com/hangouts/answer/6046115
[97] Google blog, *Saying 👋 to Allo and Duo*, 18 May 2016, available at: https://googleblog.blogspot.co.uk/2016/05/allo-duo-apps-messaging-video.html?_sm_au_=iVVS4PDKVHPkqLQ5
[98] E. Nakashima and H. Tsukayama, Los Angeles Times, *Google chat app Allo boasts strong encryption – if you turn it on*, 23 May 2016.
[99] Fortune, *Everything You Need to Know About Google Allo's Privacy Backlash*, 22 September 2016, available at: http://fortune.com/2016/09/22/google-allo-nope/
[100] Email correspondence with security engineer Frederic Jacobs, August 2016.

products and services, but there is little information that is specifically tailored to users of its messaging apps.

The company has information about the level of encryption applied to its messenger services available on its website. However, within the apps themselves, the company does not do enough to make clear to users the encryption applied to the service, or how it is deployed to respond to threats to their human rights. In both Duo and Hangouts, there is no reference to encryption, only a link to the company's privacy policy. In Allo, there is a message when starting an 'Incognito' chat saying that it is kept "top secret with encryption". However, there is no explanation about the different levels of encryption applied to incognito chats, or a warning of how users' communications are less protected when using the default setting.

The Electronic Frontier Foundation (EFF) states, "While Allo does expose more users to end-to-end encrypted messaging, this potential benefit is outweighed by the cost of Allo's mixed signals about what secure messaging is and how it works."[101]

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Google as 3 for this criterion.

Google's transparency report provides details of the number of requests it has received from governments and the percentage of requests where some data was produced, both as an overall figure and on a country-by-country basis. The company's policy is to notify the affected user via email before any information is disclosed.[102]

In 2015, senior Google staff members stated that the company does not give governments backdoor access to its services,[103] although neither the company itself nor its CEO have recently taken a clear public stance on backdoors in the way that other technology companies have done. Amnesty International asked the company whether it has placed backdoors to encryption on its messaging services, but Google had not responded to the letter at the date of publication. However, Amnesty could find no evidence nor public suggestion that it has, in practice, contravened this position.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Google as 1 for this criterion.

Allo uses the Signal encryption protocol, which is fully open source. When Allo was announced in May 2016, Open Whisper Systems, the company behind Signal, said it would "provide more technical details and a summary of the integration when the app is available."[104] At the time of writing, these had not yet been published. Duo uses a new protocol developed by Google called QUIC. The company has published a specification of the cryptography on QUIC, but has not yet published a whitepaper outlining how the protocol is implemented on Duo.[105]

Google provides a very brief specification on the transport encryption that it applies to Hangouts.[106]

It is welcome that Google is using an open source encryption protocol on Allo; however, for all its messaging apps the company should be more transparent about how encryption is implemented.

KAKAO CORPORATION

Kakao Corporation (Kakao) is a South Korean technology company. Among its various products and services is the messaging application KakaoTalk. The app reportedly has more than 49 million active monthly

[101] EFF, *Google's Allo Sends The Wrong Message About Encryption*, 3 October 2016, available at: www.eff.org/deeplinks/2016/09/googles-allo-sends-wrong-message-about-encryption
[102] Google Transparency Report, available at: www.google.com/transparencyreport/userdatarequests/legalprocess
[103] Speech by Rachel Whetstone, Google's Senior Vice President Communications and Public Policy, 13 February 2015, available at: http://googlepolicyeurope.blogspot.co.uk/2015/02/privacy-security-surveillance-getting.html
Statement by Rob Salgado, Google's Director for law enforcement and information security, 8 May 2015, available at: www.reddit.com/r/IAmA/comments/35b6bt/we_are_senior_members_of_googles_public_policy/cr2sd65
[104] Open Whisper Systems, *Open Whisper Systems partners with Google on end-to-end encryption for Allo*, 18 May 2016.
[105] Google, *QUIC Crypto Specification*, 26 May 2016, available at: https://docs.google.com/document/d/1g5nIXAIkN_Y-7XJW5K45IblHd_L2f5LTaDUDwvZ5L6g/edit
[106] Google, *How Hangouts encrypts information.*

users.[107] KakaoTalk is widely used in South Korea – in 2014, Kakao's CEO claimed that 93% of smartphone owners in the country used the app.[108]

In October 2014, the company came under significant public pressure following reports that it had complied with orders by the South Korean government to provide information about KakaoTalk users who had criticized the government's handling of the Sewol ferry disaster.[109] In response, the company's CEO announced that it would stop accepting any "prosecution warrants to monitor our users' private conversions".[110] The company subsequently took steps to strengthen its level of encryption and improve transparency.

Kakao sent a response to Amnesty International's request for information.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Kakao as 1 for this criterion.

Kakao has a stated commitment to privacy set out in its privacy policy. On its website, the company outlines some of the measures it has in place to protect privacy, including encryption.[111] In its response to Amnesty International, Kakao states that it is committed to the right of freedom of expression of its users. In a letter to NGO Access Now in May 2016, the company stated that it will "soon start to institutionalize our commitments to users' freedom of expression at the same level as our commitments to privacy. We expect to finish our work by 3Q 2016." [112]

In its response to Amnesty International, the company provided details of some of the procedures it carries out to protect privacy and freedom of expression. The company states that, "Based on various data and prior experiences, Kakao carefully examines the messaging service through its self-established checklist and the risk management model."[113] The company also has a security operation service centre that identifies any symptoms of concern or potential threats from hackers.

However, the company does not explicitly recognize how state surveillance and online criminality pose a threat to the human rights of users of its IM services. Kakao challenged this assessment, pointing to a statement on its official privacy web page: "We at Kakao will never neglect our obligation to protect our users' personal information, which is protected by law, as well as our users' privacy-related information from third parties."[114] Although this statement does indicate the company's commitment to privacy, Amnesty International does not consider it sufficient recognition of the source of online threats to users' rights.

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Kakao as 1 for this criterion.

Kakao deploys end-to-end encryption to KakaoTalk, but it is not set as a default. To apply end-to-end encryption, users must select the app's 'Secret Chats' feature. Other messages on KakaoTalk are encrypted with transport layer encryption, meaning that decrypted content is accessible on Kakao's servers.

Kakao responded to Amnesty International stating that the 'Secret Chat' feature is a default option together with the two other default modes (open chat, and regular chat). It is the case that these three different options are presented side by side when starting a new conversation through the 'Chats' tab – however, the 'regular chat' mode is automatically used when a user starts a new conversation through the 'Friends' tab. It is clear that regular chat is the default mode.

---

[107] Statista, *Number of monthly active KakaoTalk users from 1st quarter 2013 to 2nd quarter 2016*, available at: www.statista.com/statistics/278846/kakaotalk-monthly-active-users-mau/
[108] Keynote speech by Lee Sir-goo, CEO of KakaoTalk, at the Mobile World Congress, 24 February 2014, available at: www.koreaherald.com/view.php?ud=20140224001578 (accessed September 2016)
[109] Y. Lee, Associated Press, *S. Korea rumor crackdown jolts social media users,* 5 October 2014.
[110] Korea Times, *Kakao defies prosecution's monitoring*, 14 October 2014, available at: www.koreatimesus.com/kakao-defies-prosecutions-monitoring/
[111] Kakao, *Privacy Policy: Technical Measures*, available at: http://privacy.kakaocorp.com/en/protection/tech
[112] Kakao letter to Access Now, 2 May 2016, available at: https://business-humanrights.org/sites/default/files/documents/Kakao%20response.pdf
[113] Kakao letter to Amnesty International, 12 July 2016.
[114] Kakao letter to Amnesty International, 4 October 2016.

The company has not provided a detailed explanation for its decision not to apply end-to-end encryption to all messages sent on KakaoTalk. In its letter to Access Now, the company states that "although we have had some functional and technical issues related to employing end-to-end encryption on all chats in KakaoTalk, it is something we are giving serious consideration."[115]

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Kakao as 1 for this criterion.

Kakao has user-friendly materials on its website outlining its approach to privacy, how it collects and uses personal information, and its 'Secret Chats' feature.

However, the company also does not make users aware of the threats to their human rights when using KakaoTalk, including through clear warnings that individuals' private communications are at greater risk when using the default chat mode.

When using the app, there is a clear option for using 'Secret Chats' when starting any new conversation. However, there is no explanation within the app about what encryption is or what the difference is between 'secret chats' and 'regular chats'. There is also no warning about the potential risks to users' rights when using the lower level of encryption.

In its response to Amnesty International, Kakao stated that the company "decided to promote and explain [the 'Secret Chats' feature] through our website, official blog, media reports and various online contents, rather than explaining within app which we believe is highly likely to interrupt the seamless use of KakaoTalk service."

Amnesty International considers that it is important for companies to make clear to users within the app itself how their rights are protected through encryption, particularly when there are different modes with different levels of security.

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Kakao as 3 for this criterion.

Since January 2015, the company has published a transparency report that provides figures dating back to 2013 of the number of information requests it has received from the South Korean government, the nature of the requests, and the number of user accounts affected. Kakao says it is the first company in South Korea to issue transparency reports.

Under South Korean law, investigation agencies are supposed to notify users subject to communications surveillance within 30 days after deciding whether or not to institute and prosecute against them.[116] In most cases involving the content of communications, a company that has provided the information will be unable to inform the affected user itself.[117] On this issue, Kakao told Amnesty International that "we have tried to participate in discussions about enhancement of users' rights including such user notification, and we have tried to find a legitimate solution within the boundary of current laws… Hence, we are in a position that this user notification issue remains to be resolved by lawmakers."[118]

However, it is not clear whether or not Kakao notifies the affected users when it receives a request for their personal information. The company only states that under South Korean law the prosecutor or police must send a written notification to the user concerned, and that Kakao will "actively participate in critical discussions about making practical improvements surrounding user notification".[119]

In its letter to Amnesty International, Kakao states that there are no backdoors to encryption on its messaging services, and it has not received "any requests from any government to place backdoors on its messaging

---

[115] Kakao letter to Access Now, July 2016
[116] Korea Internet Transparency Report, section on Surveillance, available at: http://transparency.kr/surveillance?ckattempt=1
[117] K.S. Park, Professor, Korea University Law School, *Communications Surveillance in Korea*, August 2014, section 4, available at: http://opennetkorea.org/en/wp/main-privacy/internet-surveillance-korea-2014?ckattempt=2#_ednref1
[118] Kakao letter to Amnesty International, 4 October 2016.
[119] Kakao Privacy Policy, Frequently Asked Questions, available at: http://privacy.kakaocorp.com/en/faq/report/page1 .

services." It also states that "Kakao does not in any way respond to requests from state authorities demanding access to communication data or the restriction in offering end-to-end encryption." Amnesty International could find no evidence nor public suggestion that it has, in practice, contravened this position since the company strengthened its privacy protections in response to public pressure in 2014.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Kakao as 0 for this criterion.

In its response to Amnesty International and on its website, Kakao provides only basic specifications of how it encrypts messages on KakaoTalk. Amnesty could not find a detailed specification of how the company implements encryption. The company uses its own custom LOCO communications protocol.

LINE

LINE Corporation is a Japan-based company whose core business is its LINE mobile messaging service. It is a subsidiary of South Korean internet company Naver Corporation. The LINE app has more than 200 million active daily users, with the majority from Japan, Indonesia, Thailand and Taiwan.[120]

LINE sent a response to Amnesty International's request for information.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored LINE as 1 for this criterion.

In its privacy policy, LINE states that it is committed to protecting users' personal information. On its website, the company also states its commitment to freedom of expression through its compliance with Japanese law.[121] It also provides details of measures it takes to protect user information, including deploying encryption. The company carries out security inspections prior to application disclosures or updates which include "inspections on suitability of encryption strength, countermeasures against third-party account hijackings".[122]

However, LINE does not state explicitly how its users' human rights are under threat from surveillance, or that measures such as encryption have been put in place in response to these threats. The company does state that censorship is a threat to users by saying that "LINE Corporation does not cooperate whatsoever with unilateral requests for information disclosure in relation to acts of state censorship".

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored LINE as 3 for this criterion.

In July 2016, LINE extended end-to-end encryption to apply as a default to text, location messages, VoIP and video calls sent through the LINE app.[123] End-to-end encryption had previously only been available as an option on the service.

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored LINE as 1 for this criterion.

In LINE's response to Amnesty International, the company states that "we continuously update information about privacy and security practices in what we consider is on par with the best practice available in the industry." LINE's website provides some guidance for users to protect their own privacy and security, and states the level of encryption deployed on the app and how this means that communications are "hidden from browsing not only by third parties but also by LINE server managers".[124]

---

[120] The Financial Times, *Line app looks to export Asian popularity to new markets*, 4 June 2016.
[121] LINE, *LINE Corporation's Compliance with Applicable Laws*, section on Telecommunications Business Act–Communication secrecy., available at: https://linecorp.com/en/security/article/34
[122] LINE, *Secure Programming*, available at: https://linecorp.com/en/security/article/38
[123] LINE, *Hidden Chat users to enjoy "Letter Sealing" from July*, 30 June 2016.
[124] LINE, *Data Security*, available at: https://linecorp.com/en/security/article/37

However, the company does not make users aware of the threats to their human rights posed by government surveillance or online criminality. There is no information or notifications provided to users within the messaging app itself indicating what level of encryption is applied to the service, or how the company is deploying encryption to prevent and mitigate against risks to users rights.

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored LINE as 1 for this criterion.

LINE does not publish a transparency report outlining details of the number of information requests it has received from state authorities. On its website the company states that "LINE plans to continue to implement initiatives that will enhance the transparency of how we treat and handle user information."

LINE provides only some brief details of how it handles government requests, stating that "the person in charge at LINE will only cooperate with criminal investigations in accordance with strict information handling rules, and only when a thorough verification confirms the legalities and propriety of the investigation." It does not say that it notifies affected individuals if a request has been made for their personal data.

The company has indicated that it does not backdoor its encryption. In its response to Amnesty International, the company states that no backdoors exist in its services, and that it has not received any request, "nor would we respond to any request from authorities to build a backdoor to our service."

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored LINE as 1 for this criterion.

LINE provides an overview of the encryption applied to its app on its website.[125] In September 2016, the company published a technical whitepaper for security engineers and developers with technical details about the encryption protocols and algorithms used.[126] However, the company has used its own encryption protocol which is not open-source.

MICROSOFT

Skype is a communications platform that operates through both desktop-based software as well as a mobile phone app. Skype has been a division of the multinational technology company Microsoft since 2011. Skype is used for voice and video calling, as well as text messaging and has 300 million active users.[127]

Skype has been a major target of government surveillance, and access by governments to Skype communications has been exposed in the past. An internal NSA document released by Edward Snowden showed that the agency was carrying out "sustained Skype collection" through its PRISM programme, including access to audio, video, messages and file transfers.[128] In 2013, the *New York Times* reported that, before it was acquired by Microsoft, Skype developed a secret programme for making calls available to US intelligence agencies and law enforcement officials.[129] In the past, Skype has also come under criticism over surveillance and censorship by the Chinese government targeting services operated by its former Chinese joint venture TOM-Skype.[130] In 2013, Microsoft ended its partnership with TOM Group and strengthened privacy protections for users in China.[131]

Microsoft has a strong public commitment to human rights and is relatively transparent about the policies and procedures it has in place to respect human rights. However, given Skype's history around issues of

---

[125] LINE, *New generation of safe messaging: "Letter Sealing"*, 13 October 2015, available at: http://developers.linecorp.com/blog/?p=3679#more-3679
[126] LINE, *Encryption Overview: Technical Whitepaper*, 29 September 2016, available at: https://scdn.line-apps.com/stf/linecorp/en/csr/line-encryption-whitepaper-ver1.0.pdf
[127] Statista, *Leading social networks worldwide as of September 2016, ranked by number of active users,* September 2016.
[128] Spiegel, *Inside the NSA's War on Internet Security*, 28 December 2014, available at: www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
[129] The New York Times, *Web's Reach Binds N.S.A. and Silicon Valley Leaders*, 19 June 2013, available at: www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html?_r=1
[130] See for example: N. Villeneuve, P. Fellow, the Citizen Lab, *Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform,* 1 October 2008; Reuters, *Skype says China JV partner stores text messages*, 2 October 2008; TechCrunch, *Skype Must Be More Transparent, Says Activists And Advocacy Groups*, 24 January 2013.
[131] Reuters, *Microsoft blocks censorship of Skype in China: advocacy group*, 27 November 2013.

surveillance, it is particularly disappointing that the company is still deploying a weak form of encryption on Skype. The company must follow through on its stated commitments by strengthening encryption on Skype, as well as do more to inform Skype users about how it is using encryption to protect their human rights.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Microsoft as 3 for this criterion.

Microsoft has made a clear public commitment to respect human rights, including privacy and freedom of expression, reflected in the company's Global Human Rights Statement with explicit reference to international human rights standards.[132] The company has six 'privacy principles' indicating how it protects privacy, including that it will "protect the data you entrust to us through strong security and encryption".[133]

The company recognizes online threats to the rights to privacy and freedom of expression through its participation in the Global Network Initiative, and the Reform Government Surveillance Coalition of companies.

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Microsoft as 0 for this criterion.

In its letter to Amnesty International, Microsoft states that Skype software utilizes "industry standard encryption", and that it "applies end-to-end industry standard encryption to all Skype calls". However, the company does not provide any details, including clarification of how encryption keys are generated and exchanged for Skype calls and – crucially – whether Skype holds the encryption keys itself. The company only states that – as with any app that enables calls to be made to ordinary phone numbers – the part of the call that takes place through the telephone network rather than the internet is not encrypted.[134]

In relation to instant messages, Microsoft clearly indicates on its website that these are not end-to-end encrypted, but are encrypted between the client and Skype's servers.[135] In response to Amnesty International, Microsoft and Skype pointed to the difficulty of reconciling end-to-end encryption with aspects of product functionality, such as translation tools.

Based on the information available, Microsoft does not deploy any end-to-end encryption to Skype in a way that prevents the company itself from being able to access the content of communications. Amnesty concluded that the company is not using an adequate level of encryption on this service.

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Microsoft as 0 for this criterion.

Microsoft's Privacy Statement on its website provides information about how it collects, uses and shares personal information, including on Skype.

In response to Amnesty International, Microsoft says that "Skype has an online support channel for its customers which hosts a series of Frequently Asked Questions (FAQs) concerning all aspects of the Skype product offering", and provided a link to an FAQ with an explanation of the encryption applied to Skype. However, as outlined above, this explanation does not clarify what form of encryption is applied to Skype calls, the process of how keys are generated and shared, or whether the company has access to the content of communications. It is therefore not sufficient for demonstrating how encryption protects users' privacy and other rights.

Within the Skype app itself, there is no information given to users on encryption. Users are also not informed about the level of encryption applied to different communications (for example, voice calls and instant messages). This is particularly concerning given Skype's weak level of encryption and the fact that there have been well-documented threats to Skype's communications through surveillance.

---

[132] Microsoft, *Global Human Rights Statement*, available at: www.microsoft.com/about/csr/DownloadHandler.ashx?Id=03-01-01
[133] Statement by Microsoft CEO Satya Nadella, *Privacy at Microsoft*, available at: https://privacy.microsoft.com/en-US/
[134] Microsoft, *Does Skype use encryption?*, available at: https://support.skype.com/en/faq/FA31/does-skype-use-encryption
[135] Microsoft, *Does Skype use encryption?*

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Microsoft as 3 for this criterion.

Microsoft publishes bi-annual reports on the Transparency Hub section of its website which provide details of the requests it has received from law enforcement agencies worldwide, and the legal demands made by the US government under national security laws. This covers all of its services, including Skype. In its response to Amnesty International, the company states that "if a government wants customer data, it needs to follow applicable legal process – meaning, it must serve us with a warrant or court order for content or a subpoena for subscriber information or other non-content data. We require that any requests be targeted at specific accounts and identifiers."

The company also has a policy to give "prior notice to users whose data is sought by a law enforcement agency or other governmental entity", except when prohibited by law or under exceptional circumstances. Microsoft has also taken action to try to increase transparency over government requests for its users' information. The company has filed four lawsuits against the US government related to the right to privacy and transparency – the most recent lawsuit, filed in April 2016, challenges the government's use of secrecy orders preventing companies from disclosing certain types of legal demands for information.[136]

In response to Amnesty International, Microsoft states that it "does not place any backdoors to encryption on its messaging services… Microsoft does not provide any government with direct and unfettered access to our customers' data, and we do not provide any government with our encryption keys or the ability to break our encryption." As outlined above, there have in the past been allegations that Skype has provided disproportionate access to users' communications; Microsoft has consistently said that it only ever complies with orders for requests "about specific accounts or identifiers".

For this criterion, we concluded that overall Microsoft demonstrates a high level of commitment to being transparent about the requests it receives from governments. However, the only way to provide real reassurance to users that their human rights are protected when using Skype is for the company to put in place stronger encryption.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Microsoft as 0 for this criterion.

Microsoft only discloses basic details of the encryption algorithms that it applies to Skype.[137] It is not clear what system of encryption is applied to Skype calls and Microsoft does not provide a specification of how it implements encryption on the service.

SNAPCHAT

Snapchat is a US-based company whose primary product is the Snapchat mobile application. The app allows users to send each other photos and video messages ('Snaps'), as well as text messages ('Chat'). Unlike most other IM services, these messages disappear from the app's interface once they have been viewed. More than 100 million people use Snapchat per day, and the app is particularly popular among young people.[138]

Snapchat sent a response to Amnesty International's request for information.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Snapchat as 1 for this criterion.

---

[136] B. Smith, Microsoft's President and Chief Legal Officer, *Keeping secrecy the exception, not the rule: An issue for both consumers and businesses*, 14 April 2016, available at: http://blogs.microsoft.com/on-the-issues/2016/04/14/keeping-secrecy-exception-not-rule-issue-consumers-businesses/#EwUCXsXzTmxiu6qG.99

[137] Microsoft, *Does Skype use encryption?*

[138] Snapchat letter to Amnesty International, 11 July 2016 (Snapchat letter); Statista, *Distribution of Snapchat users worldwide as of 2nd quarter 2015, by age,* 2016, available at: www.statista.com/statistics/315398/snapchat-user-age-distribution/

In its letter to Amnesty International, the company states that "privacy and security are foundational values at Snapchat".[139] This commitment is reflected in its Privacy Policy. However, the company does not have a policy commitment to all human rights including freedom of expression.

Snapchat also states that "we strongly oppose any initiative that would deliberately weaken the security of our systems", and "backed up our words with action" by intervening to support Apple's case against the FBI. In a blog post about the case, Snapchat's CEO Evan Spiegel raised concern that the FBI's request for a "backdoor" to the iPhone poses a threat "to the security of your information and communications."[140]

It is positive that Snapchat took action in support of Apple's position, and publicly recognized the threats posed by encryption backdoors. However, in its publicly available policies the company does not otherwise acknowledge how human rights – including both right to privacy and freedom of expression – may be adversely impacted as a result of governments or other third parties gaining access to its users' private information.

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Snapchat as 0 for this criterion.

Snapchat states that "we employ strong encryption for all communication with our servers and use certificate pinning for added security over HTTPS. What's more, Snaps and other sensitive data are encrypted at rest on the mobile device and on our servers."[141] This indicates that the company uses transport encryption. The company does not deploy end-to-end encryption, evidenced by the fact that the company acknowledges that "in certain limited circumstances it may be possible for Snapchat to retrieve the content of sent messages".[142]

In March 2016, Snapchat was reported to be working on a secure messaging system.[143] In response to Amnesty International, the company said "we regularly evaluate new ways to improve security for Snapchatters, including possibly implementing end-to-end encryption. But needless to say, we cannot share the specifics of our product development roadmap."

By failing to deploy end-to-end encryption, Snapchat is failing to respond to well-known threats to its users' rights to privacy and freedom of expression.

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Snapchat as 0 for this criterion.

Snapchat's model is that messages sent through the app disappear once they have been viewed, giving users an impression that messages are 'ephemeral', despite the fact that the content is stored temporarily on the company's servers. However, the risk that this will give users a false sense of privacy and security means that there is a greater onus on the company to ensure users are fully informed about possible risks to their rights to privacy and freedom of expression, and the way that the company is responding through encryption.

Snapchat's privacy policy is available on its website and via a link in the app itself. The company also gives warnings to users that content sent through the app can be retained and stored through various means, including "screenshots, in-app functionality, or any other image-capture technology".[144]

However, Snapchat does not make clear to users the threats to their rights posed by state surveillance and criminality. The company also does not make any reference, either in its public policies or within the app itself, to the level of encryption it deploys on the service, or how the company is using encryption to protect users' security.

---

[139] Snapchat letter, 11 July 2016.
[140] Snapchat, *Why we're standing with Apple*, 3 March 2016, available at: www.snap.com/en-US/news/post/why-were-standing-with-apple/
[141] Snapchat letter, 11 July 2016.
[142] Snapchat Law Enforcement Guide, 16 October 2015, p. 6.
[143] The Guardian, *Facebook, Google and WhatsApp plan to increase encryption of user data*, 14 March 2016.
[144] Snapchat Privacy Policy, available at: www.snapchat.com/privacy

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Snapchat as 3 for this criterion.

Since April 2015, Snapchat has published a transparency report twice a year which provides details of the number of government requests for its users' information, the nature of these requests, and a percentage of requests where some data was produced.

Since November 2015, Snapchat's policy has been to notify users when the company "receives legal process seeking their records, information, or content", with exceptions "where we are legally prohibited from doing so, or when we believe there are exceptional circumstances (like child exploitation or an imminent risk of death or bodily injury)."

In its response to Amnesty International, Snapchat states that "to date we have not received any formal government demands for a "backdoor." If that day were ever to come, we would oppose it across the board – just as we would oppose any measure that would compromise the security of our platform." Amnesty International could find no evidence nor public suggestion that it has, in practice, contravened this position.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Snapchat as 0 for this criterion.

On its website, Snapchat does not provide any specification of the encryption it uses. In its response to Amnesty International, the company only said that, "We employ strong encryption for all communication with our servers and use certificate pinning for added security over HTTPS."

TELEGRAM

Telegram is a company headquartered in Germany that develops Telegram Messenger, a messaging app that can be used across smartphones and other devices. Telegram is financially supported by Russian entrepreneur Pavel Durov, and the company states that it is a non-commercial project.[145] In February 2016, the company stated that it has 100 million monthly active users.[146]

Telegram sent a response to Amnesty International's request for information.

Telegram brands itself as a secure messaging app, and takes a strong stance on protecting users' privacy, yet the company does not put in place end-to-end encryption as a default.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Telegram as 3 for this criterion.

Telegram's public image as a secure messaging app means that it clearly recognizes threats to privacy online and how these can be addressed through the use of encryption. On its website, the company states that "at Telegram we think that the two most important components of Internet privacy should be: Protecting your private conversations from snooping third parties, such as officials, employers, etc. Protecting your personal data from third parties, such as marketers, advertisers, etc."[147]

Its Privacy Policy outlines how the company protects its users' privacy, including through the use of encryption. The company also expresses its commitment to protecting freedom of speech and freedom of opinion on its website.[148]

In the wake of the armed attacks in Paris in November 2015, Telegram was thrust into the centre of the debate around encryption after media reports named it as a popular tool among supporters of the armed

[145] Telegram FAQ, available at: https://telegram.org/faq#q-how-are-you-going-to-make-money-out-of-this
[146] TechCrunch, *Encrypted messaging app Telegram hits 100M monthly active users, 350k new users each day*, 23 February 2016.
[147] Telegram FAQ, *What are your thoughts on internet privacy*, available at: https://telegram.org/faq#q-what-are-your-thoughts-on-internet-privacy .
[148] Telegram FAQ, *Do you process take-down requests from third parties?,* available at: https://telegram.org/faq#q-wait-0-o-do-you-process-take-down-requests-from-third-parties

group calling itself Islamic State (IS).[149] In response, the company announced that it had blocked public channels related to IS, but stated that it maintained a commitment to privacy, with Durov quoted as saying that "as for private chats, they were and remain sacred to us. There will be no shift in attitude there."[150]

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Telegram as 1 for this criterion.

Telegram has been applying end-to-end encryption for messages and media since October 2013. However, end-to-end encryption is not applied to all communications on the app as a default, but only when users select the 'Secret Chats' mode, while all other messages are sent through the 'Cloud Chats' mode. 'Cloud chats' use server-client encryption, meaning that messages are encrypted between the user and Telegram's servers – so in principle Telegram can access the decrypted content of communications.

In its response to Amnesty International, Telegram states that the reason that end-to-end encryption is not applied to all messages by default is that "Telegram offers its users the ability to use the company's own secure cloud for backup and seamless synchronization of message history (Cloud Chats). This is advantageous compared to forcing the majority of users to use third-party solutions from Apple and Google (as some of our competitors do, most notably, WhatsApp)." The company also says that if it made all chats "Secret", meaning that users were unable to back up to the cloud, this would push users to third-party client apps. Telegram concludes that "the current separation of chats into Cloud and Secret represents the most secure solution currently possible for a mass-market messaging application in real-life conditions."[151]

Although it is legitimate for messaging apps to offer users alternative options that allow functionality not compatible with end-to-end encryption, there is no legitimate reason why Telegram has not made Secret Chats the default setting for the majority of communications sent through its service. This is particularly the case given that Telegram explicitly identifies itself as a secure messaging app.

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Telegram as 1 for this criterion.

Telegram's FAQ on its website explains the company's stance on internet privacy and on the encryption used on its service in layman terms. In its privacy policy, it emphasizes that there is no way for the company to access the content of Secret Chats.[152]

Within the app itself, Telegram indicates to users that 'Secret Chats' are encrypted with end-to-end encryption, and differentiates them from regular chats by highlighting them in green and marking them with a lock symbol. However, it does not warn users of how and why their communications could be at greater risk when using the default 'Cloud Chats' option that relies on a weaker form of encryption.

This is particularly problematic given that the app is branded as being secure, meaning people could assume that the strongest form of encryption is being applied throughout.

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Telegram as 2 for this criterion.

Telegram's privacy policy states simply that it "never shares data with anyone". In its response to Amnesty's question on what the company's policy for responding to requests from state authorities is, Telegram said:

"To protect the data that is not covered by end-to-end encryption, Telegram uses a distributed infrastructure. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from different jurisdictions

[149] See for example: CNN, *An app called Telegram is the 'hot new thing among jihadists'*, 17 November 2015.
[150] Quoted in TechCrunch, *After Paris Attacks, Telegram Purges ISIS Public Content*, 19 November 2015, available at: https://techcrunch.com/2015/11/19/telegram-purges-isis-public-channels/
[151] Telegram email to Amnesty International, 4 October 2016.
[152] Telegram, *Secret Chats*, available at: https://telegram.org/privacy#secret-chats

are required to force us to give up any data. Thanks to this structure, we can ensure that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression. Telegram can be forced to give up data only if an issue is grave and universal enough to pass the scrutiny of several different legal systems around the world."[153]

This clearly indicates that Telegram rarely, if ever, provides any personal information about its users in response to requests from governments or law enforcement agencies. Telegram confirms that to date it has disclosed "0 bytes of user data to third parties, including governments."[154]

However, the company has not published a transparency report detailing all of the government requests it has received. It should also outline in more detail what its process is for responding to such requests, including what circumstances it would consider providing user data, and whether it would notify the affected users.

In its response to Amnesty International, Telegram said, "We can confirm that we have not introduced any backdoors to Telegram and will not do so in the future. We oppose anti-encryption laws that are proposed in various countries and publicly refused and will refuse even to consider implementing backdoors to our service."[155] Amnesty International could find no evidence nor public suggestion that it has, in practice, contravened this position.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Telegram as 3 for this criterion.

Telegram's app is open-source, and the company provides details of its encryption protocol on its website. We therefore ranked the company as 'green' for this criterion.

However, there has been debate over vulnerabilities in the security of Telegram's messaging app, including in relation to the encryption applied to the service. One of the main criticisms of Telegram's encryption is that the company decided to use 'homebrew' cryptography, meaning that it invented its own custom cryptographic protocol.[156] This approach has been long recognized by cryptographers to be less secure than relying on a standard protocol which has been publicly vetted and withstood broad cryptanalysis.[157]

Telegram responded to this issue by stating that "to this day, not a single way of breaking Telegram's encryption has come to light. We are continuously working with our worldwide community of developers and security specialists to ensure that Telegram remains impenetrable."[158]

TENCENT

Tencent is a Chinese internet company that is the developer of the two most popular messaging apps in China, WeChat (known as Weixin in China) and QQ Messenger.[159] Tencent reports that Weixin/WeChat has 697 million monthly active users worldwide, while QQ Messenger has 853 million active users.[160] WeChat/ Weixin is the most popular app in China and is used not only for instant messaging, but has numerous other functions including paying for goods, ordering deliveries and gaming.[161]

Tencent did not respond to Amnesty International's request for information, and it does not publish many details of measures to address issues around privacy or other human rights. The company does not appear to put in place strong forms of encryption on its messenger services. However, because China's laws and regulations strictly control the internet, this would be legally and politically very difficult for Chinese companies.

---

[153] Telegram email to Amnesty International, 28 July 2016.
[154] Telegram, *Do you process data requests?,* available at: https://telegram.org/faq#q-do-you-process-data-requests
[155] Telegram email to Amnesty International, 28 July 2016.
[156] See for example, The Atlantic, *The Flaw in ISIS's Favorite Messaging App*, 4 January 2016; J. Jakobsen and C. Orlandi, Aarhus University, *On the CCA (in)security of MTProto*, 8 Dec 2015, last revised 31 Mar 2016, available at: https://eprint.iacr.org/2015/1177
[157] Cybersecurity expert B. Schneier, *Amateurs Produce Amateur Cryptography,* 12 May 2015, available at: www.schneier.com/blog/archives/2015/05/amateurs_produc.html
[158] Telegram email to Amnesty International, 4 October 2016.
[159] China Internet Watch, *Top 6 China mobile social networking apps*, 7 April 2016.
[160] Tencent, *About Tencent*, available at: www.tencent.com/en-us/at/abouttencent.shtml
[161] The Financial Times, *Overloaded China users battle 'WeChat fatigue'*, 16 April 2016.

In July 2015, Citizen Lab reported on how WeChat's blogging feature was subject to censorship by the Chinese authorities.[162] It cited a number of reported instances where the platform has been the target of official scrutiny, including cases of both censorship and surveillance.[163]

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Tencent as 0 for this criterion.

Tencent has one set of policies that apply to users within China and Chinese citizens and another that applies to international users of its services. There are also specific policies for WeChat and QQ.

Under both sets of policies, the company's privacy policy has a stated commitment to privacy.[164] However, the company does not make a commitment to freedom of expression. It also does not make clear what action its takes to protect privacy, stating only that "we use a variety of security technologies and procedures for the purpose of preventing loss, misuse, unauthorized access or disclosure of Information."

Tencent has five Corporate Social Responsibility commitments, however none of these recognize the threats to its users' privacy or freedom of expression.[165]

The company did not respond to our letter and Amnesty International could not find evidence of any other policies and practices that the company has in place that recognize online threats to the rights to privacy and freedom of expression linked to its services.

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Tencent as 0 for this criterion.

Tencent applies transport encryption to WeChat so that communications are encrypted between the user and the company's servers.[166] It does not deploy end-to-end encryption.

Amnesty International was unable to find any information about the encryption applied to QQ Messenger.

A March 2016 Citizen Lab report found that another Tencent service, a web browser called QQ Browser, transmits personally identifiable data without encryption or with easily decryptable encryption.[167]

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Tencent as 0 for this criterion.

As outlined above, Tencent provides limited information to its users or the wider public about threats to privacy and freedom of expression, or the level of encryption deployed to its messaging services. On WeChat's international website, there is a security FAQ with some basic information about encryption applied to the service.[168] There is a link to the company's privacy policy and terms of service when users first register for the QQ and WeChat, but within the apps themselves there is no link to the privacy policy and no reference to encryption.

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Tencent as 0 for this criterion.

---

[162] J. Q. Ng, University of Toronto's Citizen Lab, *Politics, Rumors, and Ambiguity: Tracking Censorship on WeChat's Public Accounts Platform*, 20 July 2015, available at: https://citizenlab.org/2015/07/tracking-censorship-on-wechat-public-accounts-platform/

[163] J. Q. Ng, University of Toronto's Citizen Lab, *Politics, Rumors, and Ambiguity: Tracking Censorship on WeChat's Public Accounts Platform*, 20 July 2015, Appendix: Documented Cases of WeChat Restrictions.

[164] Tencent Privacy Policy (outside China), available at: www.tencent.com/en-us/zc/privacypolicy.shtml; Tencent Privacy Policy for users within China and Chinese citizens, available at: www.qq.com/privacy.htm

[165] Tencent letter to Business and Human Rights Resource Centre, 2015, available at: https://business-humanrights.org/en/tencent-0

[166] Tencent, *How secure are my chat messages and conversations on WeChat? Can third-parties snoop or read my messages?*, available at: https://help.wechat.com/cgi-bin/micromsgbin/oshelpcenter?opcode=2&plat=1&lang=en&id=1208117b2mai1410243yyQFZ&Channel=helpcenter

[167] J. Knockel, A. Senft, R. Deibert, Citizen Lab, *WUP! There It Is: Privacy and security issues in QQ browser*, 28 March 2016, available at: https://citizenlab.org/2016/03/privacy-security-issues-qq-browser/

[168] Tencent, *How secure are my chat messages and conversations on WeChat? Can third-parties snoop or read my messages?*

Tencent's international Privacy Policy specifies that by using its services "you agree that we or our affiliate companies may be required to retain, preserve or disclose your Personal Information: (i) in order to comply with applicable laws or regulations; (ii) in order to comply with a court order, subpoena or other legal process; (iii) in response to a request by a government authority, law enforcement agency or similar body (whether situated in your jurisdiction or elsewhere); or (iv) where we believe it is reasonably necessary to comply with applicable laws or regulations."[169]

Tencent does not publish transparency reports or details of specific requests it has received for users' personal information. Amnesty International was unable to find any statements made by Tencent in relation to backdoors to encryption on its services.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Tencent as 0 for this criterion.

As stated above, Amnesty International could find limited or no details about the encryption applied to WeChat and QQ.

VIBER MEDIA

Viber Media is the developer of Viber, a messaging app primarily used on mobile phones, which enables text, video, and photo sharing as well as voice and video calls. Viber Media is legally based in Luxembourg, with its main office in Israel, and is a subsidiary of Japanese internet company Rakuten Inc.[170] Viber has 700 million registered users, and almost 250 million active daily users.[171]

Viber Media sent a response to Amnesty International's request for information.

CRITERION 1: DOES THE COMPANY RECOGNIZE ONLINE THREATS TO FREEDOM OF EXPRESSION AND RIGHT TO PRIVACY AS RISKS TO ITS USERS THROUGH ITS POLICIES AND PROCEDURES?

Amnesty International scored Viber Media as 1 for this criterion.

In its response to Amnesty International, the company said that "Viber believes user privacy and security are paramount." The company's privacy policy outlines some of the privacy safeguards it has in place, including firewalls and encryption.

However, Amnesty International could not find any evidence of any other policies and practices that the company has in place that recognize threats to the rights to privacy and freedom of expression linked to its services.

Viber does not have any stated commitment to freedom of expression. The company did not respond to our request for information on what policies and practices the company has in place to identify, prevent and mitigate against human rights abuses.

CRITERION 2: DOES THE COMPANY APPLY END-TO-END ENCRYPTION AS A DEFAULT?

Amnesty International scored Viber Media as 3 for this criterion.

In April 2016, Viber Media announced that it started fully encrypting its messaging service with end-to-end encryption. All chats, including group chats, and calls within Viber are end-to-end encrypted, unless one of the participants is using an older version of the app. Viber's 'Viber Out' feature also allows users to make calls to regular landline and mobile phone numbers – as with any communications over the telephone network, these calls are not end-to-end encrypted.

CRITERION 3: DOES THE COMPANY MAKE USERS AWARE OF THREATS TO THEIR PRIVACY AND FREEDOM OF EXPRESSION, AND HOW THE COMPANY IS RESPONDING THROUGH THE USE OF ENCRYPTION?

Amnesty International scored Viber Media as 1 for this criterion.

---

[169] Tencent Privacy Policy (International).
[170] Rakuten website, available at: http://global.rakuten.com/corp/about/company/digital.html
[171] Viber letter to Amnesty International, 12 July 2016 (Viber letter); Statista, *Leading social networks worldwide as of September 2016, ranked by number of active users.*

Viber has a Security FAQ on its website providing information in a digestible form about the encryption that it applies to its app, how it functions and how it protects users' security. Within the app itself, the company has a system of indicating the level of encryption applied to specific messages and conversations, using a colour-coded lock icon. However, the only way to tell if a chat is not encrypted is if the icon is missing – there is no clear warning to users that they are using a weaker form of encryption. It is also not made clear, either on the app or on Viber's website, that end-to-end encryption does not apply to Viber Out calls through the telephone network.

The company also does not inform users of how their human rights may be at risk through the use of its app. In its letter, Viber says it agrees that governments are "increasing pressure in this area". But the company does not make users aware of the threat posed by government surveillance.

CRITERION 4: DOES THE COMPANY DISCLOSE DETAILS OF GOVERNMENT REQUESTS FOR USER DATA, AND HOW IT RESPONDS?

Amnesty International scored Viber Media as 1 for this criterion.

Viber does not publish a transparency report or provide any details of the requests it receives from governments for users' private information. The company's privacy policy states that "we may disclose information about you if we determine that for national security, law enforcement, or other issues of public importance that disclosure of information is necessary." It does not make clear whether or not it will notify the affected individuals.

In its response to Amnesty International, Viber Media stated that it has not given any governments a "backdoor" to break its encryption.[172] In April 2016, a spokesperson was also quoted as stating that "Viber will not grant backdoor access under any circumstance and in any country. We agree with the stance both Apple and WhatsApp have taken."[173] Amnesty International could find no evidence nor public suggestion that it has, in practice, contravened this position.

CRITERION 5: DOES THE COMPANY PUBLISH TECHNICAL DETAILS OF ITS SYSTEM OF ENCRYPTION?

Amnesty International scored Viber Media as 1 for this criterion.

The company provides a technical overview of how it implements encryption on its app.[174] Viber says that its protocol uses the same concepts of the "double ratchet" protocol used in Open Whisper Systems Signal application, but that "Viber's implementation was developed from scratch and does not share Signal's source code."

However, the encryption protocol is not open source. In response to criticism that the company had not provided enough details of its system of encryption, the company confirmed that "our encryption protocol was based on an open source protocol concept, with an extra level of security developed in-house."[175]

[172] Viber letter, 12 July 2016.
[173] TechCrunch, *Viber defends new end-to-end encryption protocol against criticism*, 20 April 2016, available at: https://techcrunch.com/2016/04/20/viber-defends-new-end-to-end-encryption-protocol-against-criticism/
[174] Viber Encryption Overview, available at: www.viber.com/en/security-overview
[175] TechCrunch, *Viber defends new end-to-end encryption protocol against criticism*, 20 April 2016.

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

Contact us


info@amnesty.org


+44 (0)20 7413 5500

Join the conversation


www.facebook.com/AmnestyGlobal


@AmnestyOnline

FOR YOUR EYES ONLY?

RANKING 11 TECHNOLOGY COMPANIES ON ENCRYPTION AND HUMAN RIGHTS

Encryption helps protect people's human rights online. By rendering digital data unintelligible, encryption helps ensure that private information sent over the internet stays private.

Encryption stops cybercriminals from stealing our personal information and helps prevent unlawful government surveillance of our communications. It is particularly important for human rights defenders and journalists around the world – whether they are dissidents in China, Bahraini activists in exile abroad, or investigative journalists in Europe. A breach of their data security undermines their vital work and could result in their arrest and detention.

Technology companies play a crucial role in keeping digital information safe. In this report, Amnesty International ranks 11 technology companies on whether they are meeting their human rights responsibilities by using encryption to protect users' right to privacy online. It focuses specifically on instant messaging services, such as Skype, WhatsApp and WeChat, which hundreds of millions of people around the world use to communicate every day.

Amnesty is asking all technology companies to deploy end-to-end encryption as a default on all instant messaging services. Amnesty International found that all of the companies it assessed need to be more transparent about the extent to which they protect users' rights to privacy and freedom of expression online.

INDEX: POL 40/4985/2016
OCTOBER 2016
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL