SECURING PRIVACY: Privacy International on End-to-End Encryption

September 2022

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

SECURING PRIVACY:

Privacy International on End-to-End Encryption

September 2022

CONTENTS

INTRODUCTION

End-to-end encryption (E2EE) contributes significantly to security and privacy. For that reason, Privacy International (PI)[1] has long been in favour of the deployment of robust E2EE.

Encryption is a way of securing digital communications using mathematical algorithms that protect the content of a communication while in transmission or storage. It has become essential to our modern digital communications, from personal emails to bank transactions. End-to-end encryption is a form of encryption that is even more private. It ensures that only the "ends" of the communication, usually the person who sent the message and the intended recipient(s), can decrypt and read the message.

> As described in more detail in this paper, E2EE attempts to recreate, in the digital world, the guarantees of privacy that have traditionally applied in private face-to-face conversations.

As more of people's lives are lived in the digital realm, communication security tools, such as E2EE, are increasingly important to the protection of human rights, including the right to privacy. E2EE gives us access to safe and private spaces for personal development where we can communicate without interference. It protects us from criminals. It protects us from unnecessary and disproportionate surveillance. This secure space is also essential for those who seek to challenge powerful interests, including journalists, protestors, political opposition and human rights defenders. E2EE thereby facilitates the exercise of human rights beyond privacy, including freedom of expression and opinion. Such a space is necessary for all of us.

But E2EE is not universally applauded. Governments see the expansion of E2EE as a threat to their ability to access our communications. Governments may occasionally have legitimate reasons to seek this access, including for targeted law enforcement investigations. An E2EE communication, however, is not as easy to access as other forms of digital communications. Indeed, allowing governments to obtain the content of the communication while in transit would destroy its end-to-end encrypted nature. For that reason, governments have put forth a variety of proposals for how to access E2EE communications while, purportedly, retaining their security. We briefly address some of the most prominent of these proposals in this paper.

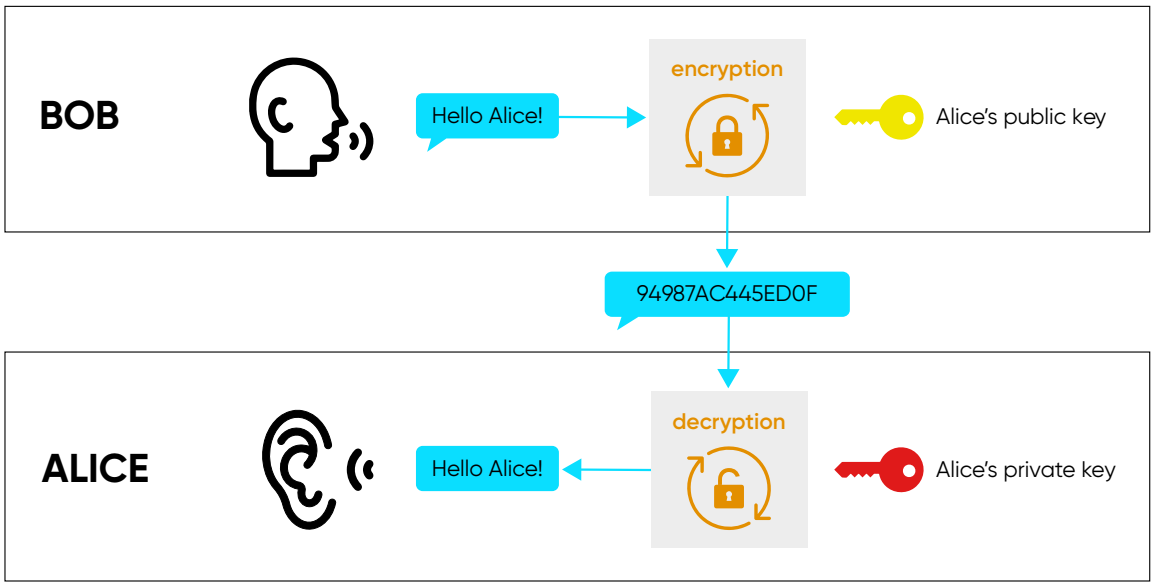
> To date, no proposal has successfully preserved E2EE while also providing government authorities the access they seek. Other less intrusive investigative techniques, such as targeted surveillance of communications subject to robust safeguards, remain open to governments, however.

On balance, PI remains strongly in favour of the continued expansion of E2EE to secure our communications. Breaking E2EE puts our privacy, security and freedom at risk.

WHAT IS END-TO-END ENCRYPTION?

All that was once necessary for two or more people to have a private conversation was for them to walk into a field – away from eavesdroppers – where they could simply talk.[2] We will refer to this as the "field model". The intention of end-to-end encryption (E2EE) is to restore the benefits of two or more people talking privately in a field – but in a world of digital communication where participants may be physically or virtually separated from each other. This goal requires the exclusion of message content from all entities who are not participants in the conversation – where, exactly as in the field model – participation is defined as one who is apparent as being within earshot of the speaker.

Encryption is a way of securing communications using mathematical algorithms that protect content of the communication while in transmission or storage.[3] A common modern method of encryption relies on the generation of mathematically related numbers, unique for each recipient. Those two numbers, called 'keys', are used to cipher and decipher a message. For each communication, one of the two keys, the 'public' one is distributed to anyone who can send a message to the recipient, while the corresponding 'private' key is exclusively used by the recipient. The 'private' key must be kept secure, and not shared with anyone. Advanced applications used for communications in modern devices, such as mobile phones, generate this pair of keys for their user. By relying on this "public-key cryptography" technique, anyone can send an encrypted message that only the recipient can unscramble.[4]



Encryption, hence, relies on the process of merging a message ('plaintext' – the content of the message, which could include text, multimedia or arbitrary data) with a passphrase or other data such as a file (the 'encryption key' described above) to produce a 'ciphertext' that is indecipherable to users who do not have the encryption key. In order to make the message coherent, an individual must use a correct key to decrypt the ciphertext and convert it back to readable plaintext. In other words, the sender of the message uses their encryption key

to turn a readable message into scrambled, unreadable text. In return, the message's recipient uses an encryption key to make the message readable. If the message is intercepted in transit, it will be unreadable.

One of the most robust methods of encryption is E2EE. With E2EE, a user encrypts the contents of a message on their own device and the messaging service or application sends an encrypted version of that message to a final recipient who then decrypts the message on their own device.[5] As the encryption and decryption of messages sent and received occurs on users' devices, E2EE provides only the intended recipients – not even the communications service provider – with access to the content of the message, making it secure.[6] This is how E2EE replicates the field model. It excludes any unknown participants from the conversation. E2EE can secure not only instant messages between two or more people, but interactions between systems, such as sharing passwords or sensitive health data between devices, and many other forms of communication.

Additional, security enhancing features of some E2EE systems

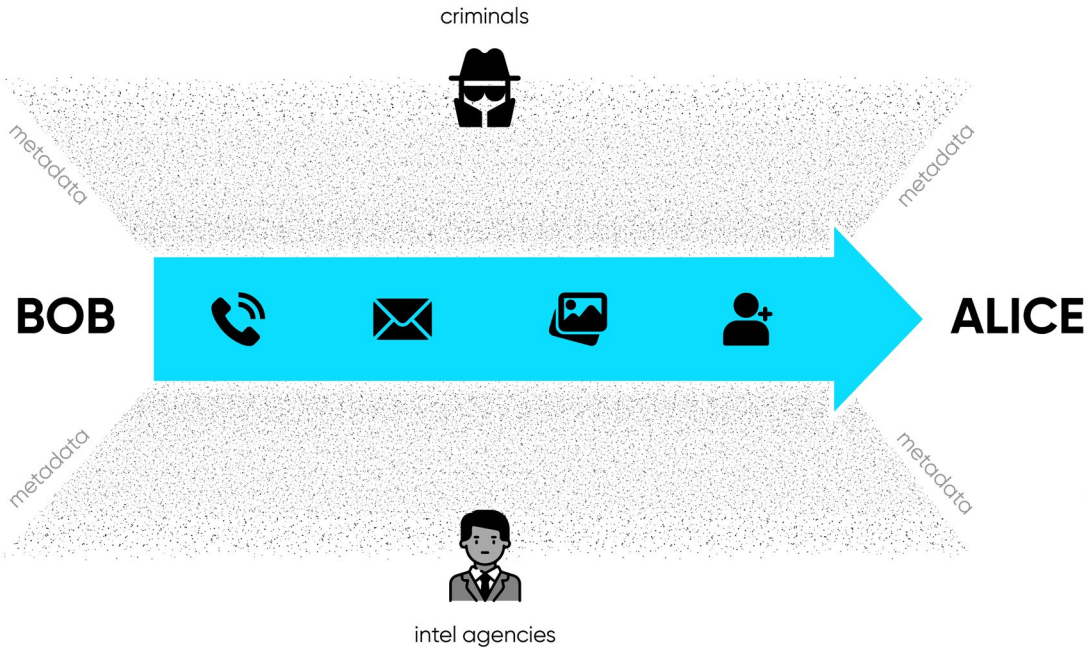
Several messaging service providers, including WhatsApp and Signal, have implemented '**forward secrecy**',[7] which requires that the private keys for a connection are kept in an ephemeral storage. This basically means that every time a certain number of messages is sent, or a certain time period has elapsed, a new key is generated.[8] Accordingly, the key used to encrypt a previous message cannot be reconstructed once this has been transmitted or received. This provides users of E2EE messaging services with an additional layer of security, because, if a single key is compromised, the third party will only have access to a limited number of messages. In fact, not even the communications services provider will be able to retroactively decrypt past messages, due to the nature of E2EE as mentioned above.

A further layer of security on messaging services is the use of '**safety numbers**' in two- or multi-party communications. This ensures that

a person is communicating only with the intended parties, such as a reporter communicating with a source. This authentication mechanism is, for example, called a "safety number" in Signal and a "security code" in WhatsApp.[9] They are long strings of numbers that are derived from the public keys of the two parties of the conversation, which can be compared between them – via some other verifiable communications channel such as in person– to confirm that the strings match. Because the safety number is per pair of communicators — more precisely, per pair of encryption keys — a change in the value means that a key has changed, and that can mean that it's a different party entirely on the other end of the communication.

Public encryption keys can change on messaging services for legitimate reasons, for instance, when an app is reinstalled on a phone, the user gets a new phone or when a phone number changes on a device, the messaging client will generate a new key and notify the recipient of a key change. On WhatsApp, for example, users may see a message on a chat saying "Your security code with XXX has changed. Tap here to learn more."[10] People can thus choose to be notified when these safety numbers change, to ensure that they can maintain this level of authentication.

An important caveat with respect to E2EE is it protects only the content of electronic messages. The communication service provider, such as WhatsApp, can still see the metadata accompanying the messages, like dates, sender, and recipient.[11] While securing content is very important in protecting privacy, metadata can be equally -or, at times, even more- revealing,[12] so E2EE is not a completely private communications solution. Any user considering E2EE should be aware of what the accompanying metadata can reveal, and who may have access to it, including the service provider, governments who can compel the service provider to turn over such data, and criminals who may try to obtain it by unlawful means.[13]



E2EE, as conceptualised in this paper, encompasses the idea of having end-to-end integrity in private communications in transit. Thus, as will be discussed in more detail below, the privacy and security of E2EE may be interfered with not only when the technical features of encryption are broken, but also by other attempts to systemically access the content of the communication such as through client-side scanning.[14]

This paper does not, however, focus on encrypted data at rest, such as that which exists on a mobile phone protected by a passcode. This is another fundamentally important form of encryption,[15] which can complement E2EE by protecting the "end" of the communication, such as the user's device where data is stored. Many of the legal and policy arguments articulated below may nonetheless apply in the context of encrypted data at rest.

THE HUMAN RIGHTS IMPLICATIONS OF E2EE

Modern communication is increasingly digital. Over the internet, using mobile phones, via email, text message, social media platform or video sharing service, we now have so many ways to talk to each other without being face to face. This comes with many benefits and some challenges.

> One of those challenges is that many other entities are involved in facilitating our communications, which means they may also be privy to them. E2EE helps 'take out' any spying intermediary, making our communications more secure.

Governments have long recognized the role of encryption in securing the digital economy, including in vital services like banking, credit card purchases and other online business transactions that require secrecy.[16] More recently, the use of encryption generally, although not E2EE[17] specifically, has been recommended by governments and government departments tasked with securing our data and communications, such as the Netherlands[18], the UK Information Commissioners Office, the UK[19] National Cyber Security Centre (NCSC)[20], the European Data Protection Supervisor (EDPS)[21], and the EU Agency for Cybersecurity[22]. Several data protection laws, such as the EU General Data Protection Regulation (GDPR), impose obligations on entities responsible for the processing of personal data to take security measures such as applying encryption[23]. The EU Article 29 Data Protection Working party considers encryption a necessity, which "should ideally always cover the entire communication, from the device of the sender to that of the recipient (end-to-end encryption)."[24] The European Data Protection Board (EDPB) and EDPS agree, recently opining that "end-to-end encryption ('E2EE') is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider."[25]

Governments also rely on E2EE.[26] When the Covid-19 pandemic forced many people into remote work, the US National Security Agency (NSA) published guidance for US government employees and military service members which heavily promoted the use of E2EE. The first question under the guide's "Criteria to Consider When Selecting a Collaboration Service" is "[d]oes the service implement end-to-end encryption (E2EE)?"[27] In the current conflict in Ukraine, the encryption of Russian military communications reportedly failed, leading to significant vulnerabilities, although whether these systems were fully end-to-end encrypted is up for debate.[28]

Numerous UN resolutions adopted by consensus of all UN member states have highlighted the vital importance of encryption in safeguarding human rights. In an often cited and thorough analysis of the benefits of encryption from 2015, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, wrote:

> *Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression.*[30]

Everyone benefits from having a private sphere in which to communicate and develop our opinions and beliefs, as well as to enable economic activity.[31] Some people, as the above examples illustrate, may have heightened duties of confidentiality or be at increased risk of unlawful surveillance, making the protections of E2EE essential. These people include law enforcement and government officials, journalists,[32] researchers, lawyers, civil society, activists, human rights defenders, marginalised and vulnerable groups (including based on gender, religion, ethnicity, national origin or sexuality), and artists. PI has also recommended E2EE for protestors.[33]

Who benefits from E2EE?

E2EE helps to protect everyone against unlawful interference with privacy by governments, companies and criminals. Some who are at particular risk are:

- **Journalists** reporting on a political activist in a country that strongly disapproves of that activist's cause. An E2EE mode of communication allowed the journalist to engage with his source when authorities in the country shutdown all his other methods of communication.[34]
- **Human rights defenders and political activists** opposing an authoritarian regime. E2EE may protect human rights defenders' and political activists' communications from being seized by the government, which might otherwise use such communications to justify abuse such as detention and torture.[35]
- **Protestors** demonstrating against government policies or practices. E2EE channels of communication allow protestors to organise in-person gatherings, as well as associate and assemble virtually. In countries that crack down heavily on dissent, such virtual assembly one of the only available options.[36]

- **Members of the LGBTQIA+ community** in a country where homosexuality is criminalised. Members of the community are subject to violence and imprisoned. Due to its ownership of the country's major telecommunications company, the government could easily identify LGBTQIA+ activists using SMS messages. E2EE allows them to communicate safely.[37]

Who are all these users of E2EE protecting themselves from? Without E2EE, companies, criminals, and governments, whether acting pursuant to legal process or not, have easier access to our communications.

Because E2EE protects a communication throughout its entire journey from sender to recipient, even the company providing the communication service – such as Meta providing WhatsApp or Whisper Systems providing Signal – is not able to read or store the content of the communication. The content of our communications is thus removed from the scope of data which companies can exploit.[38] With services that are not E2EE, companies may store the unencrypted content of the communication on their internal servers before passing it on to the intended recipient(s). These companies can then put that data to other uses.

E2EE not only protects the content of our communications from commercial exploitation by service providers, it also helps secure it from malicious actors who could gain access to company data. As an example of that abuse, a former Twitter employee has been accused of misusing his access to unencrypted Twitter data, "gathering the personal information of political dissidents and passing it to Saudi Arabia in exchange for a luxury watch and hundreds of thousands of dollars."[39]

Service providers are also subject to hacking[40] and data breaches. When content is stored on company servers or traversing unprotected over company networks, that provides one more place for criminals and ill-intentioned third parties to attack. Company data troves are also often appealing, as large amounts of content on many people can be obtained all at once.

More frequently, states may seek access to service provider content directly through legal process. This can include warrants or orders served on service providers requiring them to turn over the content of communications.[41] It can also take the form of pressure on service providers to provide direct access to that content.[42] Use of E2EE means service providers will not have any content to turn over in response to such requests. While this can be frustrating to law enforcement agencies that follow human rights standards in issuing targeted warrants, this frustration must be weighed against the protection provided by E2EE against many other governments that would seek to abuse such process to harass, censor or persecute. There is no way to adopt separate and secure solutions depending on the governance in place.

What is more, some governments also engage in mass surveillance, which can include intercepting the content of all of the communications flowing through a major communications cable or requiring a service provider to turn over all of the data it holds.[43] E2EE can reduce the reach of mass surveillance by encrypting message content in transit, making it essentially useless in the context of mass interception, and by removing it from company servers, leaving no content to turn over to a government if it seeks bulk access to company content.

In all of these contexts, E2EE helps protect the privacy of the content of our communications. By keeping them secure, it allows us a safe space in which to develop our autonomy and dignity.

E2EE AND THE RIGHT TO PRIVACY

The privacy of our correspondence is a core component of the right to privacy as enshrined in numerous international and regional instruments. These include Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant of Civil and Political Rights (ICCPR), Article 8 of the European Convention on Human Rights (ECHR), Articles 7 and 8 of the European Union Charter of Fundamental Rights (EU Charter), and Article 11 of the American Convention on Human Rights. The reference to correspondence is usually explicit. For instance, the ICCPR Article 17(1) states, "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." It is established case law of the European Court of Human Rights (ECtHR) that "[t]apping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence" (Kruslin v. France, App. No. 11801/85, § 33; Huvig v. France, App. No. 11105/84, § 32; Kopp v. Switzerland, App. No. 23224/94, § 72). At a basic level, by protecting the privacy of our correspondence – our digital communications – E2EE engages these rights. Put another way, any attempt to remove or undermine E2EE would constitute an interference with the right to privacy.

Privacy extends beyond correspondence, however. The ECtHR has repeatedly held that "Article 8 protects, inter alia, the right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world" (Breyer v. Germany, App. No. 50001/12, ECtHR §73). In Barbulescu v. Romania (App. No. 61496/08), the Grand Chamber of this Court affirmed that the broad interpretation given to the notion of private life ought to encompass "the right to lead a "private social life", that is, the possibility for the individual to develop his or her social identity" (ECtHR §70). By protecting the privacy of these relationships and social interactions, E2EE also engages the right.

Any attempt by a government to restrict or impede encrypted communications, therefore, must meet at least the narrow requirements established for permissible interferences with privacy. The UN General Assembly has declared "that any

interference with the right to privacy is consistent with the principles of legality, necessity and proportionality."[44] Taking the ECHR right as an example, privacy may only be interfered with if the interference is "in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[45]

In order to be "in accordance with law", any interference with E2EE must be governed by a national legal regime that is clear, foreseeable and adequately accessible (Big Brother Watch and Others v. The United Kingdom, Apps Nos 58170/13, 62322/14 and 24960/15, ECtHR § 8), among other requirements.[46] This can be a hurdle for states that wish to undermine E2EE as they cannot use vague laws to hide their intent. When laws that more clearly engage encryption have been opened for public debate, they often receive significant pushback. For instance, in the 1990s, a small group of technical experts, privacy advocates (including PI), and industry leaders successfully pushed back on US government proposals to introduce the "Clipper Chip" into telephones using encryption - a hardware encryption chip with a deliberate mathematic backdoor allowing law enforcement to easily decrypt all messages encrypted with it.[47] More recently, proposals by the EU[48] and UK[49] which could weaken or effectively ban E2EE are also facing robust criticism.

An even higher hurdle for proposals to undermine E2EE, however, are the necessity and proportionality requirements. The ECtHR has applied a heightened standard of 'strict necessity' to interferences with the right to privacy in the when using "cutting-edge" technologies in a secret surveillance context.[50] Similarly, the Court of Justice of European Union (CJEU) requires that "derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary. In addition, an objective of general interest may not be pursued without having regard to the fact that it must be reconciled with the fundamental rights affected by the measure, by properly balancing the objective of general interest against the rights at issue." (Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others (C-623/17), Grand Chamber, CJEU § 67). When determining whether an interference with the right to

privacy is "necessary in a democratic society", the ECtHR also examines whether that interference was proportionate to the aims pursued (Catt v. The United Kingdom, App. No. 43514/15, ECtHR § 109).

> Considering the vital role encryption plays for individuals' modern communication[51] and the risks inherent in the measures that seek to undermine it allowing for secret surveillance, any attempt to tamper with E2EE constitutes a serious interference with privacy.

As will be discussed in more detail in the next section, the current proposals to allow law enforcement access to E2EE either (1) introduce vulnerabilities in E2EE systems, such as inserting 'silent listeners' to conversations, or (2) seek to monitor the content of communications at the "ends" of the E2EE conversation through bulk surveillance mechanisms such as searching every message for potentially incriminating content.[53] Both forms of access interfere with the privacy of E2EE users. They are also indiscriminate as they cannot be applied only to specific users, which might, for instance, present a threat to national security or be engaging in serious crime. Instead, they become a "feature" of the E2EE system that compromises the privacy and security of the millions or billions of users of that service.

Such blanket or indiscriminate measures that seriously interfere with privacy are neither necessary nor proportionate. In S. and Marper v. the United Kingdom (App. Nos. 30562/04 and 30566/04), the ECtHR held that the collection and retention of DNA and fingerprints of innocent people was contrary to Article 8. In particular, the Court was "struck by the blanket and indiscriminate nature of the power of retention in England and Wales" (§ 119), concluding that "the blanket and indiscriminate nature of the powers of retention…fails to strike a fair balance between the competing public and private interests" (§ 125). It held that the UK had "overstepped any acceptable margin of appreciation in this regard" even though the DNA database was undoubtedly a valuable tool for detecting and prosecuting serious criminals (§ 125).

The CJEU has also condemned indiscriminate forms of surveillance. In Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others (Case C-623/17), the Court held that EU law precluded a requirement on service providers to "carry out the general and indiscriminate transmission of traffic data and location data" to the UK intelligence agencies (§ 82). In Data Protection Commissioner v. Facebook Ireland Ltd. ("Schrems II") (Case C-311/18), the Court similarly declared disproportionate US laws allowing for bulk collection of data (§§ 183-184).

In light of such precedent, it is hard to see how the generalised and indiscriminate proposals to undermine E2EE could be considered lawful and proportionate. The UN High Commissioner for Human Rights agrees, opining that weakening encryption "jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks. Such a widespread and indiscriminate impact is not compatible with the principle of proportionality."[54] The Commissioner recently reiterated that "the impact of most encryption restrictions on the right to privacy and associated rights are disproportionate, often affecting not only the targeted individuals but the general population."[55]

In addition to being indiscriminate, it is not clear that these proposals to undermine E2EE are strictly necessary in the sense that there are no other less intrusive means of obtaining the content sought (Szabó and Vissy v. Hungary, App No 37138/14, ECtHR § 21 (12 January 2016)). Modern law enforcement agencies have a wide array of investigative techniques available to them, including ways to access the "ends" of the E2EE communication. According to the UN High Commissioner for Human Rights, "[g]overnments seeking to limit encryption have often failed to show that the restrictions they would impose are necessary to meet a particular legitimate interest, given the availability of various other tools and approaches that provide the information needed for specific law enforcement or other legitimate purposes."[56] Breaking E2EE, with its general and indiscriminate impact, does not appear to be the least intrusive option in such circumstances.

STATES' PRIVACY OBLIGATIONS

Furthermore, under international human rights law states are subject to the duty to affirmatively protect the right to privacy against abuses by public and private actors including taking measures to protect the enjoyment of rights. As noted by the UN High Commissioner for Human Rights, that duty includes "to adopt legislative and other measures to give effect to the prohibition of and protection against unlawful or arbitrary interference and attacks, whether they emanate from State authorities or from natural or legal persons."[57] The Commissioner, in promoting encryption, has similarly called on states to "to enact policies that protect the privacy of individuals' digital communications."[58]

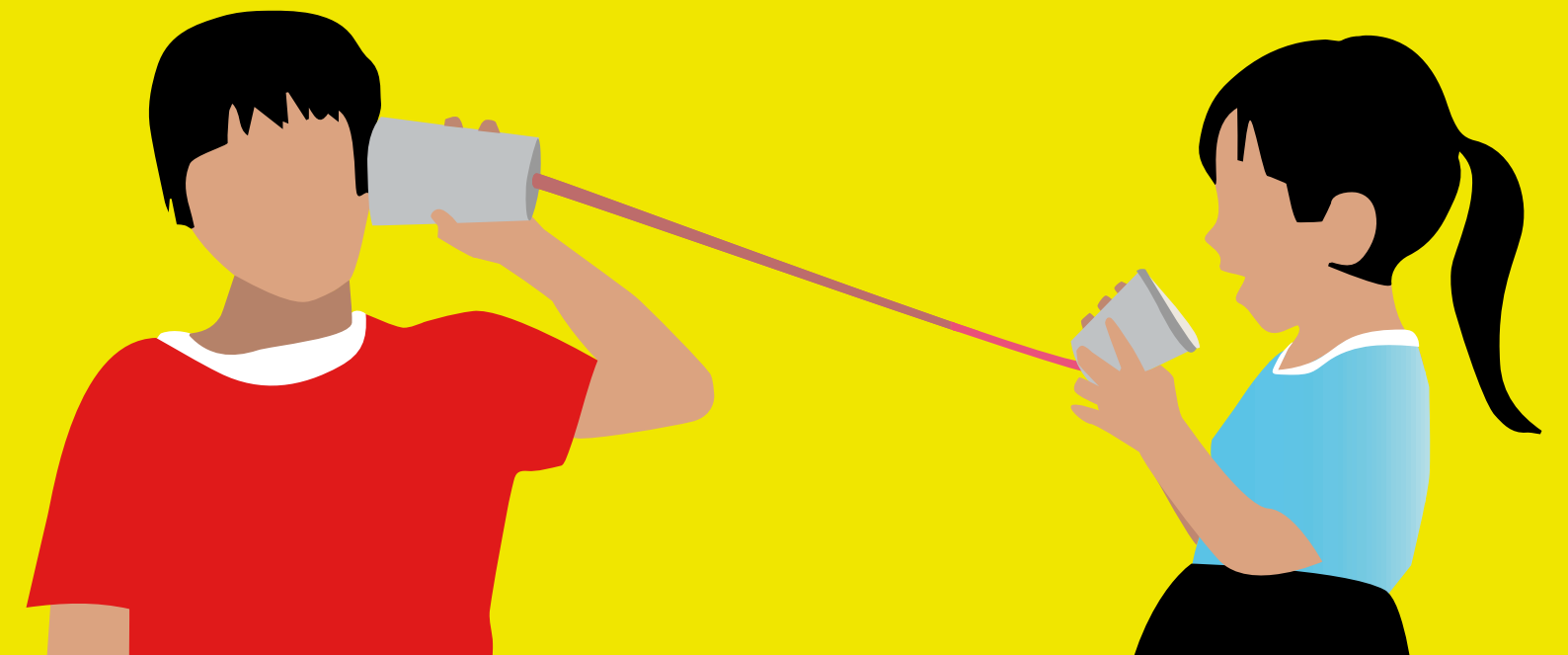
EU law similarly imposes a series of obligations on states to guarantee the privacy and confidentiality of communications, as well as the security and integrity of information technology systems.[59] In particular, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 establishes rules for the processing of personal data, also in the context of a criminal investigation.[60] Among others, the Directive underlines a series of obligations for law enforcement authorities to ensure the security, integrity and confidentiality of personal data by implementing relevant measures.[61] Finally, the EU Directive on security of network and information systems (the NIS Directive) provides legal measures to boost the overall level of cybersecurity among member states.[62]

The fifty-five states party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data are also subject to certain obligations to affirmatively protect privacy.[63] The European Court of Human Rights recognises that, to protect privacy, "[w]hile the essential object of Article 8 of the Convention is to protect individuals against arbitrary interference by public authorities, it may also impose on the State certain positive obligations to ensure effective respect for the rights protected by Article 8" (Barbulescu v. Romania, App. No. 61496/08, ECtHR § 108 (5 September 2017)).

By requiring states to secure our communications from unlawful or arbitrary interference, these duties counsel in favour of the application of E2EE.

Thought Experiment

In our attempts to understand digital security, techniques like E2EE are sometimes given physical world analogues. Encryption is often represented as a lock. Taking that analogy further, E2EE is like a lock that cannot be picked. While this parallel is far from perfect, it does help illustrate the state's duty regarding such a power. Should the state promote an unpickable lock, even if it might hamper its own investigative capabilities? We say the above precedents say it should. Yet many states are leaning toward banning the unpickable lock, preventing us from having access to this peak of security technology, relegating us to a world of lesser, pickable locks. Common sense, as well as the law, suggest that is an untenable position.



E2EE AND THE RIGHTS TO FREEDOM OF EXPRESSION AND OPINION

Because E2EE also provides a private space in which to express views, organise collective action, and form opinions, among other things, it also implicates the right to freedom of expression and opinion.

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression argued persuasively that both rights protect encryption.[64] The right to freedom of expression is subject to narrow exceptions very similar to those for privacy. The analysis above thus applies equally. Indeed, with regard to encryption generally, the Special Rapporteur concluded:

> *"The regulation of encryption often fails to meet freedom of expression standards in two leading respects. First, restrictions have generally not been shown to be necessary to meet a particular legitimate interest. This is especially the case given the breadth and depth of other tools, such as traditional policing and intelligence and transnational cooperation, that may already provide substantial information for specific law enforcement or other legitimate purposes. Second, they disproportionately impact the rights to freedom of opinion and expression enjoyed by targeted persons or the general population."*[65]

This analysis is even more salient with regard to E2EE as most proposed methods of accessing E2EE communications would require the breaking or removal of encryption for all users of the system, which is inherently disproportionate. The Special Rapporteur on freedom of expression agrees, stating that when States seek to mandate backdoor access to encrypted communications, "[g]iven its widespread and indiscriminate impact, [such] access would affect, disproportionately, all online users."[66]

CORPORATE OBLIGATIONS AND E2EE

Many companies also have obligations that counsel in favour of deploying E2EE.

Companies have responsibilities to respect human rights, as authoritatively outlined in the UN Guiding Principles on Business and Human Rights. These responsibilities include specific steps to mitigate risks of human rights abuses, including carrying out human rights due diligence and putting in place processes and safeguards to prevent and mitigate potential privacy and other human rights harms.[67]

With regard to encryption more broadly, the UN Human Rights Council

> *"[e]ncourages business enterprises, including communications service providers, to work towards enabling solutions to secure and protect the confidentiality of digital communications and transactions, including measures for encryption, pseudonymization and anonymity, and to ensure the implementation of human-rights compliant safeguards..."*[68]

Article 32(1) of the EU's General Data Protection Regulation (GDPR) requires data controllers and processors to implement appropriate technical measures to ensure the security of the data they process. Article 32 cites encryption as an example of an appropriate technical measure. The European Data Protection Supervisor (EDPS) calls it "one of the main tools to guarantee the security of our information."[69] National data protection authorities, including the Irish Data Protection Commission (DPC), similarly promote using encryption.[70] In the UK, the ICO also encourages encryption under the UK GDPR.[71]

Under Article 4 of the EU's e-Privacy Directive, providers of electronic communications services must protect the security of those communications.[72] And under Article 5 of the e-Privacy Directive, EU member states must ensure the communications' confidentiality. In their joint response to the EU's Proposal for a Regulation to prevent and combat child sexual abuse (CSAM), the EDPS and the European Data Protection Board (EDPB) note that the proposal conflicts with those provisions, and that "end-to-end encryption ('E2EE') is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong

technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider."[73]

E2EE also helps fulfill the fundamental data protection principle of data minimization (GDPR Art. 5(1)(c)). If communication service providers have no legitimate purpose for accessing and storing the content of communications, they should not do so. E2EE removes the possibility of such access and storage.

ACCESSING E2EE COMMUNICATIONS?

Given the manifest benefits of E2EE for privacy, security, freedom of expression and other rights, what are the arguments against the deployment of E2EE? Most prominently, they come from governments who seek to access our communications. Some governments, like the United States,[74] United Kingdom,[75] and the EU[76] have pushed for access for the purpose of law enforcement and intelligence agency use to facilitate investigations into crimes such as terrorism, child sexual abuse and drug offenses. Other governments, such as Russia, China and Egypt, have sought effectively to ban encryption entirely[77] to preserve access, often for illegitimate purposes such as cracking down on dissent.

> The prevention of serious crimes such as terrorism and child exploitation may constitute important and compelling reasons to access communications. The problem arises because technologists seem to be in almost universal agreement that there is no way to allow only law enforcement and other legitimate government access to E2EE communications of individuals suspected of serious crimes.[78] Any weakening of the security of E2EE communications creates a vulnerability that could be accessed by a sufficiently sophisticated actor, including criminals and states with illegitimate aims. Making matters worse, most proposals to provide access to E2EE communications would "break" the security for all users of the service, not just those who are the targets of a specific investigation, which would render such proposals disproportionate as a solution for combatting crime.

The possibility of security flaws designed to give exceptional access to law enforcement being exploited by hostile actors is far from theoretical.[79]

Between 1996 and 2006, it appears that insiders at Telecom Italia enabled the wiretapping of 6,000 people, including business, financial, and political leaders, judges, and journalists.[80] From 2004 to 2005, the cell phones of 100 senior members of the Greek government, including the Prime Minister, the head of the Ministry of National Defence, the head of the Ministry of Justice, and others were wiretapped by unknown parties through lawful access built into a telephone switch owned by Vodafone Greece.[81] Similar vulnerabilities have also been exploited by third parties with onerous consequences for millions of individuals globally. WannaCry ransomware attack, for example, was developed by hackers who effectively managed to exploit software vulnerabilities stockpiled by the United States National Security Agency (NSA),[82] and seriously impacted European infrastructure operators in the sectors of health, energy, transport, finance, and telecoms.[83]

A new generation of proposals, such as client-side scanning, attempt to avoid these vulnerability concerns by searching the content of an E2EE communication before it is encrypted or after it is decrypted.[84] Remembering the field model introduced earlier, these proposals are no more palatable, however, as they break E2EE by revealing the content of the E2EE communication and raise a myriad of other security and human rights concerns.

In this section, we briefly describe some of the most prominent proposals regarding access to E2EE communications and why those proposals would break E2EE, thereby undermining our human rights.

BACKDOORS

A backdoor is an umbrella term to describe several known methods that ultimately decrypt communications for any actor other than the sender and intended recipient(s), thus breaking the field model discussed previously. Backdoors allow third-party access to communications without the sender's or recipient's knowledge or permission. This can be done by obtaining the private keys of participants, by holding secret knowledge about the encryption algorithm which make its solution easier than intended – such as an otherwise

unseen mathematical flaw[85], or by finding innovative ways to make factoring large primes mathematically easier than the current approach of brute-forcing, such as through the potential of Quantum Computing. Once a private key has been compromised, or a weakness discovered by "solving" the maths in the algorithm, this can be discovered by others and exploited, and therefore introduces a security vulnerability in an entire system that could have wider and unforeseeable consequences beyond those initially intended, including use by criminals and other adversaries.

KEY ESCROW

Key escrow is one type of backdoor. In the mid 1990s, much as today, law enforcement expressed fears of encryption.[86] Computers were less powerful at that time. The typical modern smartphone dwarfs any "supercomputer" of the period, and one consequence of this was that cryptography was used sparingly. Keys were generated infrequently, leading to proposals of 'key recovery' or 'key escrow'. The idea was that any time that data was encrypted with a key, they would be obliged to register (to permit recovery, or to otherwise escrow) that key with some "trusted" third party authority in case the government wanted in future to access what had been sent. This breaks E2EE, in violation of human rights obligations explained above, and the field model[87], because a third party with the key will be able to access the content of the communications.

The key escrow has become a much less practical idea, however, now that newer and more powerful computers – and better algorithms[88] – mean that new encryption keys are generated and used every time that someone presses the send key on their messenger, or a dozen times every time a webpage is refreshed, rather than when you move university or employer and get a new email address. Governments which continue to pursue key escrow proposals might therefore require the generation and use of fewer encryption keys, undermining these security innovations as well as breaking E2EE.

DOWNGRADE ATTACKS

A downgrade attack is forcing the use of a less secure method of encryption, such as one trivially easy to break with modern computing power. Typically, the longer an encryption key, the harder it is to break in order to decrypt to communication.[89] Understanding as much, some countries such as China have specified the number of characters that can be used in an encryption key.[90] For example, a key length of 64 characters (or "bits") as opposed to the standard 2048-bit key length means the private key "equation" could be more easily solved in less time and with less computing power. This is a downgrade attack, forcing users to use more insecure methods of communicating by obtaining the private key with ease and as a result creating a backdoor.

GHOST PROTOCOL

In a 2018 Lawfare blog post,[91] representatives of the UK spy agency GCHQ proposed a new twist on key escrow: that service providers should be obliged, when hosting an E2EE conversation, to splice an additional and invisible participant – referred to by some as a ghost[92] – into the conversation. Then at some later time, if surveillance of the conversation was required, law enforcement could access the content by viewing it as the invisible participant.

This method, often called the ghost protocol, introduces a potential vulnerability into the E2EE system.[93] Injecting an invisible user would bypass significant protections put in place by service providers, including forward secrecy and authentication through methods like safety numbers.[94] This means users would no longer be able to verify who is participating in their conversation. The ghost protocol might be used by human-rights respecting law enforcement for targeted investigations, as intended. But it could also potentially be exploited by criminals or co-opted by states with illegitimate aims.[95] The ghost protocol thus breaks E2EE by exposing the content of the communication to an unintended third party, the ghost.

MESSAGE HASH ESCROW

The Indian Government is greatly concerned by E2EE, and especially wants to be able to trace the 'originator' of much-forwarded viral content within an E2EE system such as WhatsApp.[96] It has proposed applying a 'hash function' to each message a person composes, where the 'hash' is an irreversible digital fingerprint of the message's plaintext content, while also separately encoding and storing the identity of the person who initially composed that message.[97] The hash-and-identity originator information would be left unmodified if the message was merely forwarded to other users.

There are several problems with this scheme, including that the act of saving-and-resending an image may create a new hash.[98] Thus, there is no guarantee that the originator of the message being pursued is the actual originator. The government's purpose in imposing the system is also ultimately to understand who sent certain content, which breaks E2EE by revealing the content of the E2EE communication.[99]

Furthermore, this mechanism can leak message content, breaking the field model and E2EE.[100] Someone wanting to discover the content of the message, especially a plain text message, could potentially do so either by guessing the plaintext content of the hash or synthesising it using the platform. As service providers are required to save the hash of every message sent, the government could then demand a search of the database for senders who have previously sent a message with that hash.

CLIENT-SIDE SCANNING

Client-side scanning (CSS) describes the scanning of content on a device at one end of a communication, prior to its encryption or after it has been decrypted. The content is scanned to identify anything that is deemed problematic. Currently, the debate around CSS mainly focuses on detecting child sexual abuse material (CSAM).[101] Client-side scanning could be used to detect any type of content, however, so if implemented could be used to look for evidence

of other serious crimes like terrorism or for illegitimate aims such as censorship of political speech. Proponents argue CSS does not break E2EE because the scanning happens on the device where the message is decrypted (the "end"), not during the encrypted message transmission.[102]

Client-side scanning can be implemented in a variety of ways, including by hashing content on the device and comparing it with hashes stored on a remote server.[103] Despite the assurances of CSS proponents, almost all these CSS methods, especially those meant to notify a third party of the detection of content deemed problematic, break E2EE by revealing the content of the E2EE communication.[104] CSS thus breaks the field model if a third party, such as Meta, is sent an alert every time problematic content is identified.

CCS is also general and indiscriminate surveillance, and thus disproportionate, in that it scans all the material being sent over an E2EE service, from all users, in order to identify the small amount deemed problematic. The UN High Commissioner for Human Rights agrees that "[i]mposing general client-side scanning would constitute a paradigm shift that raises a host of serious problems with potentially dire consequences for the enjoyment of the right to privacy and other rights. Unlike other interventions, mandating general client-side scanning would inevitably affect everyone using modern means of communication, not only people involved in crime and serious security threats."[105]

Such scanning also faces significant technical problems and potential false positives.[106] As the UN High Commissioner for Human Rights notes, "frequent false positives cannot be avoided, even if accuracy rates are high, thereby implicating numerous innocent individuals. Given the possibility of such impacts, indiscriminate surveillance is likely to have a significant chilling effect on free expression and association, with people limiting the ways they communicate and interact with others and engaging in self-censorship."[107] The CSS system could also be abused, causing further significant freedom of expression harms, depending on the type of content it was set to search for, such as political discussions.[108]

Other problems with CSS include that it may be easily circumventable through minor modification of the content to avoid a match (this depends on how

sophisticated the filtering system is)[109]; and if a device is more than a few years old or less powerful, CSS will probably not be able to function because of the amount of computing resources it would require. For a thorough discussion of the problems with client-side scanning, see "Bugs in Our Pockets: The Risks of Client-Side Scanning".[110]

METADATA ANALYSIS

Given that E2EE does not protect the metadata connected with a communication, government and company proposals have increasingly focused on examining the metadata of an E2EE communication to preserve investigative capabilities while also protecting E2EE.[111] Examining the metadata attached to a communication does not break the field model, as theoretically third parties could observe who is in the field and where they are located (the 'metadata of the field'), without knowledge of the content of their discussion.

As noted previously, however, metadata can be as revealing as content, especially when collected in bulk.[112] Bulk metadata collection or analysis is another form of general and indiscriminate surveillance that is inherently disproportionate.[113] Using it as an alternative to breaking E2EE is no better from a human rights perspective. Targeted requests for metadata, however, if they respect all the necessary human rights safeguards, could be a legitimate investigative alternative.

HACKING

Hacking one of the end points of an E2EE is another way to obtain communications' contents either before they are encrypted or after decryption. Governments increasingly use hacking as an investigative technique.[114] Hacking raises significant human rights concerns of its own, which we have written extensively about before.[115] Even when used in a targeted fashion, hacking for investigative purposes must meet stringent safeguards to avoid disproportionately interfering with privacy and security.[116]

PI'S POSITION ON E2EE

E2EE protects our privacy and security, and provides a space in which to exercise other human rights such as freedom of expression and opinion. Breaking E2EE violates those rights. So far, no proposal to provide access to E2EE content has managed to reconcile these concerns and ensure human rights are protected in the process. For these reasons:

- PI supports the expansion of end-to-end encryption and would like to see end-to-end encryption be the default in devices, messaging services, networks and platforms for data in-transit. This not only creates more secure communications but reduces the potential for data exploitation by companies who will no longer have access to the content of the E2EE communications.
- PI encourages the use of end-to-end encryption because it protects the security of our communications and raises the cost of modern, intrusive forms of surveillance like mass surveillance of the content of communications. This helps restore the balance between increasingly powerful forms of technological surveillance and our human rights.
- PI recommends end-to-end encryption be legally available for use by everyone, and especially by human rights defenders, journalists and others at risk around the world. But such use must come with the caution that encryption secures the content of communications but rarely secures the metadata of communications. Some states also place restrictions, including criminal sanctions, on the use of encryption, so prospective users should be aware of their local law.
- PI opposes current proposals by governments, intelligence agencies and law enforcement agencies for access to the content of or the banning of end-to-end encrypted communications. PI opposes the imposition of requirements for mandatory general client-side scanning. Such proposals take away important security protections and are disproportionate, threatening multiple human rights, including privacy and freedom of expression. Breaking encryption for one government breaks it for everyone.

ENDNOTES

1 Privacy International, Encryption, https://privacyinternational.org/learn/encryption (last visited 8 September 2022).

2 Whitfield Diffie & Susan Landau, Privacy on the Line, Introduction (1998) ("But before the electronic era conversing in complete privacy required neither special equipment nor advanced planning. Walking a short distance away from other people and looking around to be sure that no one was hiding nearby was sufficient. Before tape recorders, parabolic microphones, and laser interferometers, it was not possible to intercept a conversation held out of sight and earshot of other people."); A Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 Univ. of Pa. Law Rev. 709, 845 (1995) ("Under current law, a person communicating via new media is less able to ensure her privacy than were speakers in the late eighteenth century. If Thomas Jefferson wanted to speak privately to John Adams, they could go for a walk in an open field where they could see any potential eavesdroppers from a mile away.").

3 Danielle Kehl, Encryption 101, Slate (24 February 2015), http://www.slate.com/articles/technology/safety_net/2015/02/what_is_encryption_a_nontechnical_guide_to_protecting_your_digital_communications.html.

4 Privacy International, Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages (29 May 2019), https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted messages.

5 Nicole Perlroth, What Is End-to-End Encryption? Another Bull's-Eye on Big Tech, NY Times (19 November 2019), https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html.

6 See, for example, Signal Support, How do I know my communication is private?, https://support.signal.org/hc/en-us/articles/360007318911-How-do-I-know-my-communication-is-private (last visited 8 September 2022); WhatsApp, About end-to-end encryption, https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption (last visited 8 September 2022).

7 Signal, Forward Secrecy for Asynchronous Messages (22 August 2013), https://signal.org/blog/asynchronous-security/; WhatsApp, WhatsApp Encryption Overview: Technical white paper (Version 6, 15 November 2021), page 3, https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-5&_nc_sid=2fbf2a&_nc_ohc=ciRO7AcIdu8AX_Mi-3r&_nc_ht=scontent.whatsapp.net&oh=6fc894bb719bdaf871c1c7f5464a9554&oe=61AE7799

8 See Signal, Forward Secrecy for Asynchronous Messages (22 August 2013), https://signal.org/blog/asynchronous-security/

9 Signal Support, What is a safety number and why do I see that it changed?, https://support.signal.org/hc/en-us/articles/360007060632-What-is-a-safety-number-and-why-do-I-see-that-it-changed (last visited 9 September 2022); WhatsApp Help Center, About Security Code Change Notifications, https://faq.whatsapp.com/2974126929583030/?locale=en_US (last visited 9 September 2022).

10 WhatsApp Help Center, About Security Code Change Notifications, https://faq.whatsapp.com/2974126929583030/?locale=en_US (last visited 9 September 2022).

11 Surveillance Self-Defense, A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work? (29 November 2018), https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work

12 See, for example, Big Brother Watch and Others v. The United Kingdom, Apps Nos 58170/13, 62322/14 and 24960/15, ECtHR Grand Chamber § 342 (2021) ("While the content might be encrypted and, in any event, may not reveal anything of note about the sender or recipient, the related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted.")

13 For further information about metadata, see Electronic Frontier Foundation, Surveillance Self-Defense: Why Metadata Matters (12 March 2019), https://ssd.eff.org/en/module/why-metadata-matters

14 For a definition of client-side scanning, see Section IV, subsection "Client-side scanning".

15 See Brief of Privacy International and Human Rights Watch as Amici Curiae Supporting Apple, In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus, Cal. License Plate 35KGD203 (C.D. Cal. 22 March 2016) (No. CM 16-10 (SP)), https://privacyinternational.org/sites/default/files/2018-03/Amicus%20Brief%20-%20PI%20and%20HRW.pdf

16 See, for example, OECD, Guidelines for Cryptography Policy (1997), https://www.oecd.org/digital/ieconomy/guidelinesforcryptographypolicy.htm; European Central Bank, Recommendations for the security of internet payments (January 2013), https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf.

17 See Section II for a definition of E2EE.

18 Letter from The Netherlands Minister of Security and Justice and Minister of Economic Affairs to the President of the House of Representatives of the States General (4 January 2016), https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption

19 See Information Commissioner's Office, For Organisations/ Guide to Data Protection/ Guide to the General Data Protection Regulation (GDPR)/ Security/ Encryption, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption (last visited 12 September 2022).

20 See National Cyber Security Centre, Cloud security guidance, Principles 1 & 2, https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles (last visited 12 September 2022); see also National Cyber Security Centre, Protecting Bulk Personal Data, https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data/further-information (last visited 12 September 2022); National Cyber Security Centre, Device Security Guidance, https://www.ncsc.gov.uk/collection/device-security-guidance/security-principles/protect-data-at-rest-and-in-transit (last visited 12 September 2022).

21 European Data Protection Supervisor, Encryption, https://edps.europa.eu/data-protection/our-work/subjects/encryption_en (last visited 12 September 2022)

22 European Union Agency for Cybersecurity, Recommended cryptographic measures – Securing personal data (4 November 20213), https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data

23 GDPR, Article 32.

24 Article 29 Data Protection Working Party, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU (11 April 2018), https://ec.europa.eu/newsroom/article29/items/622229/en

25 EDPB-EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, § 97 (adopted 8 July 2022), https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

26 National Security Agency, Cybersecurity Information: Selecting and Safely Using Collaboration Services for Telework – UPDATE (November 2020), https://media.defense.gov/2020/Aug/14/2002477670/-1/-1/0/CSI_%20SELECTING_AND_USING_COLLABORATION_SERVICES_SECURELY_SHORT_20200814.PDF

27 Ibid.

28 Stephen Bryen, The fatal failure of Russia's ERA cryptophone system, Asia Times (26 May 2022), https://asiatimes.com/2022/05/the-fatal-failure-of-russias-era-cryptophone-system/

29 See UN Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (16 December 2020); Human Rights Council Resolution on the Safety of Journalists, UN Doc A/HRC/RES/39/6 (27 September 2018); Human Rights Council Resolution on the Freedom of Opinion and Expression, UN Doc A/HRC/RES/44/12 (16 July 2020); Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021).

30 David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32, § 12 (22 May 2015), http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

31 See, for example, Article 29 Data Protection Working Party, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU (11 April 2018), https://ec.europa.eu/newsroom/article29/items/622229/en ; Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, § 21 (4 August 2022).

32 See also, UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/74/157 (18 December 2019)("Emphasizes that, in the digital age, encryption and anonymity tools have become vital for many journalists to freely exercise their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use of such technologies and to ensure that any restrictions thereon comply with States' obligations under international human rights law.")

33 Privacy International, How the police can access your digital communications at a protest (5 May 2021), https://privacyinternational.org/explainer/4505/how-police-can-access-your-digital-communications-protest

34 This hypothetical is based on the account of journalist Jamie Barlett. Jamie Bartlett: Encryption is for everyone, not just extremists, Index on Censorship (25 Aug 2017), https://www.indexoncensorship.org/2017/08/jamie-bartlett-encryption-extremists/

35 This hypothetical is based on the experiences described in Vernon Silver & Ben Elgin, Torture in Bahrain Becomes Routine With Help From Nokia Siemens, Bloomberg (Aug. 22, 2011)

36 This hypothetical is based on the scenario reported in BSR, Human Rights Impact Assessment: Meta's Expansion of End-to-End Encryption 46 (2022), https://www.bsr.org/reports/bsr-meta-human-rights-impact-assessment-e2ee-report.pdf37

37 This hypothetical is based on the scenario reported in BSR, Human Rights Impact Assessment: Meta's Expansion of End-to-End Encryption 64 (2022), https://www.bsr.org/reports/bsr-meta-human-rights-impact-assessment-e2ee-report.pdf

38 For instance, in its Privacy Policy, Yahoo! States it "analyzes and stores all communications content, including email content from incoming and outgoing mail. This allows us to deliver, personalize and develop relevant features, content, advertising and Services." Yahoo, Welcome to the Yahoo Privacy Policy (Updated April 2022), https://legal.yahoo.com/us/en/yahoo/privacy/index.html ; see also Privacy International, Challenging Corporate Data Exploitation, https://privacyinternational.org/strategic-areas/challenging-corporate-data-exploitation (last visited 12 September 2022)

39 Kate Conger, Twitter Worker Accused of Spying for Saudi Arabia Heads to Trial, New York Times (20 July 2022), https://www.nytimes.com/2019/11/06/technology/twitter-saudi-arabia-spies.html

40 Daniel Boffey, British spies 'hacked into Belgian telecoms firm on ministers' orders', The Guardian (21 Sep 2018), https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report

41 See, for example, Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2523 (2018) (providing a framework for US law enforcement to obtain warrants to intercept or access stored content held by companies); see in particular the section known as the CLOUD Act, Electronic Communications Privacy Act, 18 U.S.C § 2523 (providing a framework whereby law enforcement from other countries can serve warrants directly on US companies); Investigatory Powers Act 2016, c. 25 (UK), §§ 15-43, https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (providing a framework for UK law enforcement and intelligence agencies to serve interception warrants on companies, including extraterritorially); German Code of Criminal Procedure (Strafprozeßordnung – StPO), Articles 100a-100j, https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.

42 See Global Network Initiative, Defining Direct Access: GNI calls for greater transparency and dialogue around mandatory, unmediated government access to data (3 June 2021), https://globalnetworkinitiative.org/defining-direct-access-2/; see also Privacy International, Direct Access, https://privacyinternational.org/learn/direct-access (last visited 12 September 2022); Zakharov v Russia, App. No. 47143/06, ECtHR , § 270 (4 December 2015)("... the Court considers that a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great.")

43 See, for example, Investigatory Powers Act 2016, c. 25 (UK), Chapter 6 (allowing for bulk interception of communications); Investigatory Powers Act 2016, c. 25 (UK), Chapter 7 (allowing for the collection of bulk personal datasets from companies, which may contain content); amaBhungane Centre for Investigative Journalism and Sole v. Minister of Justice and Correctional Services and others, Constitutional Court of South Africa, Case CCT 278/19, https://privacyinternational.org/legal-action/amabhungane-and-sole-case-south-africa (describing the South African bulk surveillance regime).

44 UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (16 December 2020); see also numerous citations to the necessity and proportionality standard as articulated by international and regional bodies in PI's Guide to International Law and Surveillance (December 2021), https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance

45 ECHR, Article 8(2)

46 Other international and regional instruments bodies impose a similar standard of legality, see, for example, UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (16 December 2020)("Noting that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant."); see also Privacy International, PI's Guide to International Law and Surveillance (December 2021), https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance

47 See, for example, Privacy International, Winning and losing and still fighting the crypto wars (2 May 2018), https://privacyinternational.org/impact/winning-and-losing-and-still-fighting-crypto-wars

48 For criticism of the EU proposal on detecting, reporting, removing, and blocking online child sexual abuse material (CSAM), see the European Data Protection Board's and European Data Protection Supervisor's joint opinion, EDPB-EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (adopted 8 July 2022), https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf ; see also Global Encryption Coalition, Joint Statement on the dangers of the EU's proposed regulation for fighting child sexual abuse online (12 May 2022), https://www.globalencryption.org/2022/05/joint-statement-on-the-dangers-of-the-eus-proposed-regulation-for-fighting-child-sexual-abuse-online/

49 For criticism of the UK's proposed Online Safety Bill and its impact on E2EE, see Global Encryption Coalition, 45 organizations and cybersecurity experts sign open letter expressing concerns with UK's Online Safety Bill (14 April 2022), https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill/ ; see also Open Rights Group, Encryption in the Online Safety Bill (20 July 2021), https://www.openrightsgroup.org/blog/encryption-in-the-online-safety-bill/

50 Szabó and Vissy v Hungary, App No 37138/14, ECtHR, § 73 (12 January 2016); see also, Liblik and Others v Estonia, App Nos 173/15 and 5 others, ECtHR, § 131 (28 May 2019) ("powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions").

51 According to a 2016 Flash Eurobarometer survey by the European Commission, an overwhelming majority of 90% of people in the European Union agree that "they should be able to encrypt their messages and calls, so they are only read by the recipient", Flash Eurobarometer 443 Report: e-Privacy, 43 (December 2016), https://europa.eu/eurobarometer/surveys/detail/2124

52 Privacy International et al., Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages (29 May 2019), https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages

53 See section IV, subsection "Client-side scanning"; see also Privacy International, Apple opens the door to mass surveillance (6 August 2021), https://privacyinternational.org/news-analysis/4604/apple-opens-door-mass-surveillance

54 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, § 20 (3 August 2018).

55 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, § 25 (4 August 2022).

56 Ibid. at § 25.

57 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, § 23 (3 August 2018).

58 UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4, § 9 (7 October 2021).

59 See, for example, Charter of Fundamental Rights of the European Union (2007/C 303/01); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 11, 1; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 37.

60 Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 89.

61 Ibid, Article 29 (Security of processing)

62 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194.

63 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981, ETS no. 108).

64 David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32 (22 May 2015), http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

65 Ibid. at § 39.

66 Ibid. at § 42.

67 For an outline of companies' responsibilities in relation to the right to privacy, see Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, § 42-49 (3 August 2018).

68 UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc

A/HRC/RES/48/4 (7 October 2021)

69 European Data Protection Supervisor, Encryption, https://edps.europa.eu/data-protection/our-work/subjects/encryption_en (last visited 25 August 2022)

70 Data Protection Commission, For Organisations: Data Protection – The Basics: Know Your Obligations: Data Security , https://www.dataprotection.ie/en/organisations/know-your-obligations/data-security-guidance (last visited 25 August 2022)

71 Information Commissioner's Office, For organisations/ Guide to Data Protection/ Guide to the General Data Protection Regulation / Security/ Encryption, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption (last visited 25 August 2022)

72 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201 , 37

73 EDPB-EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse § 97 (adopted 8 July 2022), https://edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf

74 See, for example, Susan Landau, The Five Eyes Statement on Encryption: Things Are Seldom What They Seem, Lawfare (26 September 2018); see also Riana Pfefferkorn, The EARN IT Act is Back, and It's More Dangerous Than Ever, The Center for Internet and Society at Stanford Law School (4 February 2022), https://cyberlaw.stanford.edu/blog/2022/02/earn-it-act-back-and-it%E2%80%99s-more-dangerous-ever

75 See, for example, Encryption: UK watchdog criticises government campaign, BBC News (21 January 2022), https://www.bbc.co.uk/news/technology-60072191

76 See, for example, Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN

77 For a description of the restrictive laws in Russia, China and Egypt, as well as a number of other countries, see Global Partners Digital, World map of encryption laws and policies, https://www.gp-digital.org/world-map-of-encryption/ (last visited 12 September 2022)

78 See David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32 at § 8 (22 May 2015), http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx; see also Harold Abelson et al., Keys Under Doormats: Mandating Insecurity By Requiring Govenrment Access to All Data and Communications (7 July 2015), https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf

79 For more examples of how software security flaws can be exploited across the globe, see Privacy International, Backdoors, https://privacyinternational.org/examples/backdoors (last visited 12 September 2022)

80 Piero Colaprico, "Da Telecom dossier sui Ds" Mancini parla dei politici, La Repubblica (26 January 2007), http://www.repubblica.it/2006/12/sezioni/cronaca/sismi-mancini-8/dossier-ds/dossier-ds.html

81 Vassilis Prevelakis and Diomidis Spinellis, The Athens Affair, 44 IEEE Spectrum 7, 26-33 (2 July 2007), http://ieeexplore.ieee.org/xpls/absall.jsp?arnumber=4263124

82 Zack Whittaker, Two years after WannaCry, a million computers remain at risk, TechCrunch (12 May 2019), https://techcrunch.com/2019/05/12/wannacry-two-years-on

83 EU Agency for Fundamental Rights (FRA), Fundamental Rights Report 2018, 161 (2018), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-fundamental-rights-report-2018_en.pdf

84 See, for example, Dr Ian Levy and Crispin Robinson, Thoughts on Child Safety on Commodity Platforms (21 July 2022), https://arxiv.org/pdf/2207.09506.pdf

85 See, for example, Virtue Security, Debian Predictable Random Number Generator Weakness, https://www.virtuesecurity.com/kb/debian-predictable-random-number-generator-weakness/ (last visited 25 August 2022)

86 See, for example, Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation, Before the Senate Judiciary Committee, EPIC (9 July 1997), https://archive.epic.org/crypto/legislation/freeh_797.html

87 See Section II above.

88 See, for example, Signal, The Double Rachet Algorithm (20 November 2016), https://signal.org/docs/specifications/doubleratchet/

89 Mohit Arora, How Secure is AES 128 and 256 Encryption Against Brute Force Attacks?, EE Times (7 May 2012), https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/

90 Global Partners Digital, World map of encryptions laws and policies, navigate to China on map, https://www.gp-digital.org/world-map-of-encryption/ (last accessed 13 September 2022)

91 Dr Ian Levy and Crispin Robinson, Principles for a More Informed Exceptional Access Debate, Lawfare (28 November 2018), https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

92 Privacy International at al., Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages (29 May 2019), https://privacyinternational.org/news-analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages

93 Ibid

94 Ibid

95 For a more in-depth discussion of the ghost protocol, see ibid.

96 Hash constant: Govt's solution to tracing originator of viral messages, Hindustan Times (2 March 2021), https://www.hindustantimes.com/india-news/hash-constant-govt-s-solution-to-tracing-originator-of-viral-messages-101614667706841.html

97 Ibid.

98 Namrata Maheshwari and Greg Nojem, Part 2: New Intermediary Rules in India Imperil Free Expression, Privacy and Security, CDT (4 June 2021), https://cdt.org/insights/part-2-new-intermediary-rules-in-india-imperil-free-expression-privacy-and-security/

99 Ibid.

100 See Section II above for an explanation of E2EE and the field model.

101 See, for example, Dr Ian Levy and Crispin Robinson, Thoughts on Child Safety on Commodity Platforms (21 July 2022), https://arxiv.org/pdf/2207.09506.pdf

102 Ibid.

103 See, ibid.

104 See Mallory Knobel, The Problems With the Levy/Robinson UK Paper on Protecting Children from Online Sexual Abuse (21 July 2022), https://cdt.org/insights/the-problems-with-the-levy-robinson-uk-paper-on-protecting-children-from-online-sexual-abuse/; see also Hal Abelson et al., Bugs in Our Pockets: The Risks of Client-Side Scanning (15 October 2021), https://arxiv.org/pdf/2110.07450.pdf (further highlighting that CSS is also extremely problematic in that it can expand the scope of what is scanned from content in transit to any content on the device, thus detecting material that was never meant to be shared).

105 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, § 27 (4 August 2022).

106 See, for example, an analysis pointing out the technical hurdles in the European Commission's recent proposal to detect CSAM, Susan Landau, The EU's Proposal on CSAM Is a Dangerous Misfire, Lawfare (23 June 2022), https://www.lawfareblog.com/eus-proposal-csam-dangerous-misfire

107 Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, § 27 (4 August 2022).

108 Susan Landau, The EU's Proposal on CSAM Is a Dangerous Misfire, Lawfare (23 June 2022), https://www.lawfareblog.com/eus-proposal-csam-dangerous-misfire; see also Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, § 28 (4 August 2022) ("[W]here the rule of law is weak and human rights are under threat, the impact of client-side screening could be much broader, for example it could be used to suppress political debate or to target opposition figures, journalists and human rights defenders.")

109 Ibid.

110 Ibid.

111 See, for example, BSR, Human Rights Impact Assessment: Meta's Expansion of End-to-End Encryption 22, 26 (2022), https://www.bsr.org/reports/bsr-meta-human-rights-impact-assessment-e2ee-report.pdf

112 See, for example, Big Brother Watch and Others v The United Kingdom, Apps Nos 58170/13, 62322/14 and 24960/15, Judgment, Grand Chamber, ECtHR §§ 341-343, 363 (25 May 2021); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021); UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (28 December 2020)

113 Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others (C-623/17), Grand Chamber, CJEU §§ 80-82 (6 October 2020)

114 See, for example, UK Investigatory Powers Act 2016, Part 5 & Part 6, Chapter 3

115 Privacy International, Hacking Necessary Safeguards, https://privacyinternational.org/demand/government-hacking-safeguards (last accessed 13 September 2022)

116 Ibid.

117 See Section III above.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org