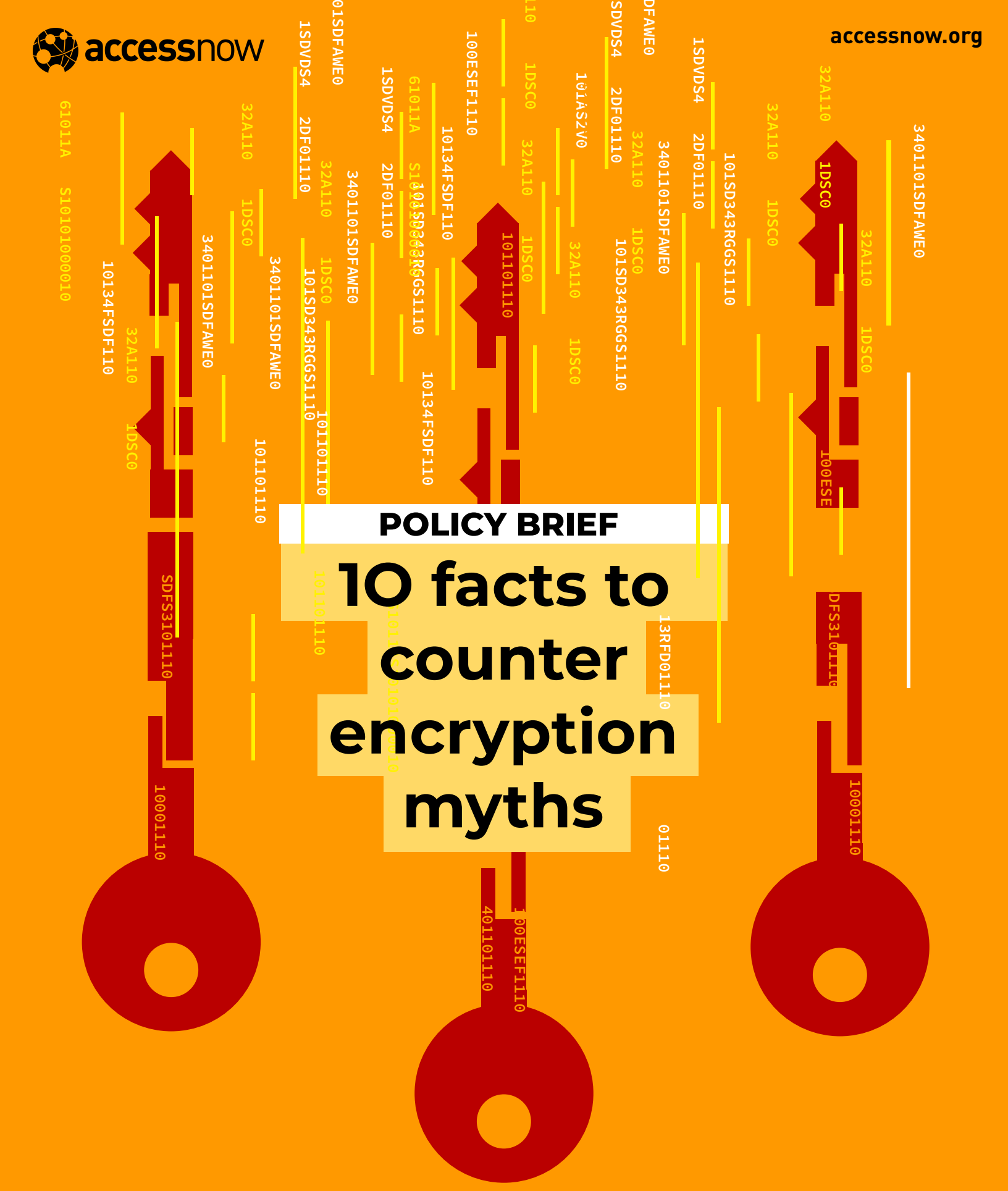
accessnow

accessnow.org

POLICY BRIEF

10 facts to counter encryption myths



Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

POLICY BRIEF

10 facts to counter encryption myths

accessnow

August 2021

This brief is an Access Now publication. It is written by Namrata Maheshwari. We would like to thank the Access Now team members who provided support, including Raman Jit Singh Chima, Javier Pallero, Estelle Massé, Natalia Krapiva, Eric Null, Gustaf Björksten, and Peter Micek. We would also like to thank those participants of the private meeting on encryption and human rights held during RightsCon 2021 who provided feedback on an outline of this publication.

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as Rightscon, we fight for human rights in the digital age.

For more information, contact: Namrata Maheshwari at namrata@accessnow.org

accessnow

Table of contents

I. Introduction

During the 2020 outbreak of the COVID-19 pandemic, we saw an unprecedented rise in online activity. We also witnessed a consequent spike in cybersecurity challenges. In the same year, however, government and law enforcement agencies in many countries issued deeply problematic domestic and international statements essentially demanding that encryption – a critical tool for cybersecurity and privacy – be weakened (see Section IV). Now, in the wake of the Pegasus Project revelations that demonstrate just how vulnerable our private communications are to hacking and exposure, underscoring the need for strong encryption, we are seeing new calls by authorities to undermine encrypted systems, and the implementation of technological measures to circumvent end-to-end encryption. This further jeopardizes our online privacy and security.

Encryption is a process in cryptography of encoding information such that only authorized persons (typically the sender and the recipient/s) can decode or decrypt the information with a "key." Encryption therefore ensures that communications between two or more parties are protected from unauthorized access by third parties. In case of end-to-end encryption, even the provider of an encrypted service is unable to access the information exchanged. Encryption can secure both data in transit (data moving through the internet or a private network) and data at rest (data stored on a device or in "the cloud").

The benefits of robust encryption are clear. Examples in daily life include enabling secure electronic banking and financial transactions, confidential private communications, and the secure exchange of sensitive information, such as healthcare data. Strong encryption serves the interests of every stakeholder in a democratic society. It protects individuals and communities by bolstering the right to privacy, freedom of speech, and freedom of association, by enabling private communications and secure storage of data. Encryption is beneficial to companies because it secures trade secrets, inspires consumers' trust, limits data breaches, and fuels innovation such as blockchain technology and virtual private

networks. And finally, law enforcement agencies and the government need encryption to protect national security, classified information, and citizens' data.

The purpose of this paper is to respond to some of the primary justifications or myths that governments rely on in their demands for targeted or exceptional access, or backdoors, to encrypted systems, to expose the inherent inconsistencies and inaccuracies. Even if a proposal to backdoor encryption purports to achieve a legitimate objective, weakening encryption for everyone is not likely to be a necessary or proportionate approach and will be detrimental to human rights, national security, democracy, and the economy.

II. 10 facts to counter encryption myths

Fact #1 Strong encryption is essential for internet security

Myth: Backdoors for targeted or exceptional access by law enforcement will not undermine internet security

Encryption is an entirely mathematical process. Content is either encrypted and secure or it is not – one cannot meaningfully claim that content is *mostly* encrypted, i.e., encrypted but with the possibility of a certain third party gaining access should they wish to. Such exceptional access essentially breaks encryption. There is no technological way of allowing access by the government without also enabling access by other unauthorized actors. A government demand for exceptional access to an encrypted system but *in a way that preserves security* is a concept rightly described as being at war with mathematics.

A backdoor to encrypted content is a security flaw that makes the entire system and the underlying data vulnerable. Targeted or exceptional access, as law enforcement agencies demand, would necessitate the creation of a backdoor in some form. Once such a weakness is created, it can be exploited by a host of malicious actors. There is simply no such thing as a backdoor that only the "good guys" have the keys to. As computer scientists and security experts have explained, implementing exceptional access mechanisms means mandating insecurity. Therefore the assertion that a backdoor can be implemented securely is paradoxical. Bolting the front door is of little avail if the backdoor is unlocked – and a single backdoor indiscriminately puts the security of all users of an encrypted system at risk.

Fact #2 Giving law enforcement exceptional access threatens human rights and democracy

Myth: Law enforcement backdoors will not impact our rights or democracy

Privacy is essential to being human. It allows individuals and communities to forge interpersonal relationships, seek medical or legal advice without fear of exposure, and express their views freely – even when they are unpopular or controversial. We need privacy simply to think freely. The knowledge of possible surveillance has a stifling effect on human behavior. As the European Court of Human Rights has observed, the mere existence of a law authorizing secret monitoring of communications is at odds with the freedom of expression and the right to privacy. This is of particular consequence for journalists, doctors, lawyers, and people targeted for discrimination or abuse, who rely on private communications to stay safe. In some circumstances, undermining encryption and stripping privacy puts lives at risk.

By enabling private and uninhibited communication free from surveillance, encryption protects human rights and freedoms pertaining to privacy, free expression, and free assembly and association. These rights are fundamental to the functioning of a healthy democracy. Encryption is therefore at the center of human rights in the digital age and an attack on encryption is also an attack on human rights and democracy.

Fact #3 Strong encryption strengthens both privacy and security

Myth: To achieve security, we must sacrifice privacy

Proponents of encryption backdoors inaccurately portray privacy and security as part of a zero-sum game where one's gains necessarily equal the other's losses and vice versa. This "privacy versus security" framing is premised on a false binary. Privacy and security are mutually reinforcing principles.

Strong encryption strengthens both privacy and security. When personal communication and information is protected and financial transactions are secured, the result is a reduction in data breaches. The benefits of encryption in providing a robust defense against cyberattacks accrue not just to individuals but also to government and law enforcement agencies that would otherwise have to deal with the aftermath of these attacks. Encryption is also integral to the strong cybersecurity infrastructure that governments and law enforcement agencies need to protect national security. Deliberately weakening encrypted systems would therefore make soft targets of individuals, governments, and businesses, and give malicious actors the capacity to use vulnerabilities in these systems as weapons. A more appropriate framing of the debate would therefore be "security versus security," as encryption not only protects privacy, it protects security. A "security" policy that targets encryption can easily become an "insecurity" policy, creating more dangers than it seeks to prevent.

Fact #4 Law enforcement has entered the golden age of surveillance — without breaking encryption

Myth: Law enforcement is facing a "going dark" problem which makes it necessary to break encryption

Intelligence and law enforcement agencies complain that encryption prevents interception - a phenomenon known as "going dark." The implication is that technological changes have diminished their surveillance capabilities. However, the "going dark" metaphor deserves to be questioned.

It ignores the fact that technological changes have made available much more data about individuals than ever before. What we see today is not an era of "going dark" but rather a "golden age of surveillance," in which details about our intimate lives, including location information, information about our contacts, and many other details previously unrecorded can easily be compiled into "digital dossiers." The unprecedented surge of online activity during the COVID-19 pandemic has only added to our digital footprints. In addition, a report by the Berkman Klein Center for Internet & Society at Harvard University concluded that encryption is not as pervasive as governments suggest, nor is it likely to become so. Meanwhile, the growth of "Internet of Things" will likely introduce new vectors for surveillance through our devices, increasing the number of security weaknesses to exploit.

None of this is new. The Snowden revelations in 2013 made it plain just how much user data governments can acquire through overreaching surveillance programs. Digital technology is not plunging our data into the dark; to the contrary, it is making it more vulnerable to exposure. Indeed, even with encryption and other tools to protect data, limiting the reach of surveillance will entail organizations and companies following strict data minimization principles and governments implementing meaningful surveillance reforms that safeguard rights and freedoms.

Fact #5 Weakening encryption will not stop criminals and terrorists from using strong encryption

Myth: Weakening encryption is an effective measure to counter terrorism and criminal activity

If tech companies are required to introduce backdoors in their software and applications, the only certain outcome will be that the general public is deprived of their ability to choose a platform where fundamental rights are protected and data is not at risk. Criminals, including terrorists, will simply shift to encrypted platforms available in foreign jurisdictions or on the black market, or they may even create their own. These platforms are more likely to be beyond the reach of law and law enforcement, making it even harder to prevent and investigate crime. At present, even though encrypted platforms protect the content of users' communications, in most jurisdictions, law enforcement has the power to access metadata and other information that significantly aids investigations. Given the sensitivity of metadata itself, it is imperative that such access is permissible only when strictly aligned with the principles of necessity and proportionality. The use of metadata for mass surveillance, and mandates requiring retention of metadata, are presumptively contrary to human rights.

Increased surveillance capabilities often lead to invasive surveillance without sufficient evidence of its effectiveness. The very creation of the ability to access encrypted information could lead to non-targeted surveillance in violation of the principles of data minimization, and of necessity and proportionality. In an investigation of the efficacy of surveillance for preventing terrorism, a study in the U.S. suggests that the link between increased surveillance capabilities and prevention of attacks is tenuous. In 2004, the FBI analyzed a surveillance program involving bulk phone and email collection activities to discern how many had made a "significant contribution to identifying terrorists, deporting a terrorism suspect, or developing a confidential informant about terrorists." Between 2001 and 2004, a mere 1.2% of the tips fit the bill. Between 2004 and 2006, none of the tips had proved useful. Therefore, weakening encryption to amplify surveillance capacity would not only undermine internet security and harm the public at large, but would not necessarily provide any meaningful, sustained, and enhanced ability to prevent terrorism. Weakening everyone's security for the mere possibility of identifying a few bad actors online is an entirely disproportionate approach, jeopardizing the privacy and security of all users of a platform without evidence to show it will achieve its aim of stopping attacks.

Fact #6 Strong encryption contributes to children's safety online

Myth: Encryption makes the internet unsafe for children

Some proponents of breaking encryption see it as a solution to the problem of Child Sexual Abuse Material (CSAM) online. However, like other criminals, perpetrators will turn to alternative encrypted platforms offered in other jurisdictions or in the black market, or create their own encrypted platforms, to hide their activities. That means that the problem will persist – it will simply move out of law enforcement's reach, precluding lawful access even to metadata that can be instrumental in investigations.

It must be emphasized that retention of metadata ought not to be mandated. Access to any data by law enforcement, including metadata, must be permissible only within a legal framework that prioritizes human rights and complies with stringent standards of necessity and proportionality.

More importantly, children need privacy and strong encryption to staysafe online. They need encrypted platforms where the identity of individuals they are interacting with can be authenticated and where their personal information is not at risk of exposure to third parties. The United Nations Convention on the Rights of the Child recognizes that, among other things, children have the rights to privacy, freedom of expression, access to information, and freedom of association. UNICEF has emphasized the importance of protecting these rights for children online. Further, a survey by UNESCO indicated that privacy is important to over 90% of youth respondents who believe they can stay safe online by acquiring the necessary information and technological competencies. Encryption is one of the best tools we have to stay safe and secure online. Owing to the pandemic and remote learning, more children are online. Consequently, governments should encourage use of strong encryption to keep children safe, not deliberately introduce security vulnerabilities into the technology they use.

Fact #7 Mandating "traceability" will risk privacy and chill free expression

Myth: Traceability must be implemented to prevent the spread of disinformation

Governments have proposed combating the spread of disinformation via online messaging platforms by mandating "traceability." Such a mandate would require intermediaries to trace the origin of content circulating on their platforms. Traceability challenges the security offered by end-to-end encryption and is problematic for a number of reasons that we outline below. It is not only an impediment to fundamental rights, it has limited utility in practice.

Implementing traceability would require end-to-end encrypted platforms to develop a new capability to discern who sent which message to whom, when, and in some cases, from where. They do not currently have this ability in order to protect privacy and security. Traceability would compel end-to-end encrypted platforms to be fundamentally redesigned, to enable access and storage of information about users and their communications in a way that is currently not possible. Technologists have explained that traceability and end-to-end encryption cannot coexist. No matter how traceability is implemented, it will adversely impact privacy and security, which constitute the core promise of end-to-end encryption.

In putting anonymity and the right to privacy at risk, traceability would inevitably have a chilling effect on free speech. Individuals will not communicate freely owing to the possibility of having to face consequences if the message is widely circulated. This constitutes a threat to the very foundations of a democracy. The mere virality of a message ought not to become a cause for culpability or suspicion. Additionally, the practical effectiveness of traceability is dubious. The originator of a message on a particular platform may not be the creator of the content. Further, the prevalence of misinformation on social media platforms indicates that traceability may not be a useful deterrent.

Finally, the argument that traceability only entails the collection of metadata, not content, and therefore does not violate privacy or free expression, is misleading. The stated purpose of traceability is to find out *who* sent a particular message because law enforcement already

knows *what* was in the message and has deemed it to be problematic. It is the metadata in such cases, i.e. who sent the message to whom and when, that protects the privacy and freedom of expression of individuals. As we state above, the collection of metadata must strictly comply with human rights, and the principles of necessary and proportionate. The implementation of traceability runs afoul of these principles. It will necessarily entail massive collection and retention of metadata, which will imperil the privacy and security of billions of users, for the mere possibility of identifying certain bad actors.

Fact #8 Strong encryption is crucial for cybersecurity and protects national security

Myth: Exceptional access to encrypted content is necessary to protect national security

Strong encryption is vital for a resilient cybersecurity infrastructure that safeguards national security. This includes ensuring that default end-to-end encryption protects the sensitive communications carried out routinely by government and intelligence officers. Furthermore, when commonly used systems and platforms are kept secure using encryption, it also secures the nation. If only certain individuals or organizations deploy encryption, or they use it for only certain purposes, it automatically signals the value of the data and exacerbates the risk of an attack.

The increase in cybersecurity incidents and targeted breaches is an argument for, not against, strong encryption. These attacks, involving a range of agencies, officials, and individuals with sensitive data, including federal agencies in the U.S., the President and Prime Minister of India, and activists, journalists, and business persons, put national security at risk. Without strong encryption, we would see more unauthorized access and exposure of classified information and citizens' personal information in government datasets, a boon to cybercriminals or state-sponsored adversaries. We would also see more successful attacks on essential infrastructure such as healthcare systems, elections, and public transport, as encrypted systems help keep their operations secure.

Fact #9 Strong encryption maintains trust in the digital ecosystem and supports economic growth

Myth: Deliberately undermining encryption will have no effect on the economy

Encryption is critical to maintaining the confidentiality and authenticity of data in the digital ecosystem. For instance, banks rely extensively on encryption to facilitate transactions, ensure protection of account information and other customer data, and protect trade secrets. Encryption also ensures customers trust banking institutions. This foundation of trust and security fuels innovation and incentivizes the development of resilient technological infrastructure, propelling industry competition and contributing to a country's economic growth. Thus, encryption is a cornerstone of the modern digital economy.

Deliberately undermining encryption would impose steep costs on companies that rely on it, and adversely impact the economy. The compliance burden imposed by laws to weaken encryption has compelled tech companies to retreat from the market in some countries. This kind of retreat not only hurts competition and innovation, it also impacts employment. In a country that undermines encryption, the market will suffer the loss of companies that offer or depend on security products and services, and companies will be disincentivized from innovating and developing such products.

Further, strong encryption can prevent or mitigate the impact of cybersecurity incidents that would otherwise do more damage and cost more money. Cybersecurity incidents are pervasive, and 80% of European companies have experienced at least one such incident. In India, nearly 1.16 million cyber attacks were reported in 2020. The average cost of a single data breach is approximately $3.86 million. Encryption reduces the risk of these breaches and controls costs, to the benefit of commercial interests and the economy as a whole.

Fact #10 Law enforcement and intelligence agencies don't have to break encryption to investigate crime

Myth: Authorities have no alternative but to break encryption

Creating encryption backdoors can enable authorities to access data they seek in certain circumstances, but that does not establish that mandating deliberate security weaknesses is necessary, proportionate, or even appropriate to achieve law enforcement or intelligence objectives in modern, rights-respecting democracies. As we have discussed, intelligence and law enforcement agencies already benefit from the vast increase in data about individuals that is available in the digital age. There are many alternatives to weakening encryption for investigating crimes.

One example of data that is often available to authorities is the metadata of communications. It can be instrumental for investigations, provided it is accessed in compliance with the international principles on the application of human rights to communications surveillance, including the principles of necessity and proportionality. These strict standards for lawful access to data are necessary because even data that is not the content of communications reveals an intimate portrait of one's activities. Law enforcement can also obtain direct testimonies from parties to the communication and in some cases can access content through data back-ups.

Furthermore, even if the content of electronic communications may be useful in some cases, it is rarely the only evidence. In a vast majority of cases, law enforcement agencies still rely primarily on traditional evidence such as witnesses, informants, physical evidence, and business records from banks and cell companies. It is worth noting that there are often situations in which a certain amount of evidence becomes inaccessible to law enforcement for a variety of reasons. For instance, a user permanently deletes a communication or the footage from a security camera is damaged.

The bottom line: It is impossible to get 100% of all potentially available evidence 100% of the time. Attempting to do so will be practically impossible and may violate people's rights. Creating encryption backdoors and weakening security for everyone in an attempt to get all possible evidence in specific cases does not align with human rights and freedoms, and in practice, will never be a substitute for good investigative work.

III. Conclusion: We need more internet security, not less; encryption must be strengthened, not weakened

There is no question that we must address the issues of child safety, disinformation, national security, and criminal activity in the digital age. However, even if the stated end goal for mandating encryption backdoors is legitimate, the means must be necessary and proportionate. Deliberately introducing security weaknesses in encrypted systems fails this test. Weakening encryption will create more dangers than it will prevent. Further, there is no evidence base for claiming that breaking encryption will achieve the desired outcomes. At best, exceptional access to encrypted content will only serve as a short-term or partial solution for law enforcement.

As we have explained in this brief, encryption is a vital tool for the protection of human rights, democracy, cybersecurity, and the economy. The right to privacy and the right to freedom of expression are basic human rights, and in today's digital world, we cannot meaningfully separate these rights from the need for secure online communication channels that are free from undue surveillance. Encryption is a crucial building block for a secure technological infrastructure, and governments should promote its use, not repeatedly seek to undermine it.

IV. Appendix

a. Major statements on encryption by governments and authorities

INTERNATIONAL STATEMENTS

July 26, 2021	Opinion by Catherine De Bolle, the executive director of Europol; and Cyrus R. Vance, Jr., the district attorney of New York County, New York	“Encryption unregulated is justice denied” Source: Politico
June 10, 2021	Joint Statement on the Visit to the United Kingdom of U.S. President Biden at the invitation of U.K. Prime Minister Johnson	"We look forward to bringing into force a robust bilateral data access agreement, to be based on a mutual recognition that both countries have an appropriately high level of data protection, that allows law enforcement investigations on both sides of the Atlantic to obtain the evidence needed to bring offenders to justice, whilst maintaining rigorous privacy standards. We will work together to maintain tightly-controlled lawful access to communications content that is vital to the investigation and prosecution of serious crimes including terrorism and child abuse. And we will work in partnership with technology companies to do this, protecting the safety of our citizens." Source: U.S.-U.K.Joint Statement
2020	Munich Security Report	“Frequently outpacing jihadist extremists in the use and reach of social media posts, right-wing extremists strongly rely on internet platforms to communicate and disseminate their ideas. With the increased takedowns of extremist content by platforms like Twitter, Facebook, and YouTube, right-wing extremists have shifted more and more to encrypted apps like Telegram and Discord as well as unregulated platforms such as 8chan or Gab. These ‘far corners of the internet’ also decisively contribute to self-radicalization processes.” Source: Munich Security Report 2020

Oct 11, 2020	Five Eyes, India, and Japan	International Statement: End-To-End Encryption and Public Safety Demands backdoors for law enforcement to access encrypted content in the interest of public safety.
Sept 2020	European Commission	Report titled "Technical solutions to detect child sexual abuse in end-to-end encrypted communications" Analyzed different methods to identify Child Sexual Abuse Material (CSAM) in private electronic communications that use end-to-end encryption.
Sept 2020	European Commission	An internal note indicated that the European Commission is contemplating ways to enable law enforcement access to end-to-end encrypted communications, within an appropriate legal framework, to address CSAM and organized crime. Source: Now, E.U. Is Deliberating On Law Enforcement Access To End-To-End Encrypted Communications [Note: The European Commission later issued a clarification to MediaNama stating that backdoors should not be introduced and encryption should not be weakened.]
July 2020	Indian Minister of Information Technology Ravi Shankar Prasad at the Meeting of G20 Digital Economy Ministers	"It is time to acknowledge that digital platforms anywhere in the world have to be responsive and accountable towards the sovereign concerns of countries including defense, privacy, and security of citizens." Source: Press Release by the Indian Ministry of Electronics and Information Technology
Oct 4, 2019	U.K. Home Secretary Priti Patel, U.S. Attorney General Barr, Secretary of Homeland Security (Acting) McAleenan, and Australian Minister for Home Affairs Dutton - to Mark Zuckerberg	Open Letter re: Facebook's "Privacy first" proposals Requested that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services to protect users and children.
Jul 2019	Five Eyes	Joint Meeting of FCM and Quintet of Attorneys-General Stated that "[t]ech companies should include mechanisms in the design of their encrypted products and services whereby

		governments, acting with appropriate legal authority, can obtain access to data in a readable and usable format."
July 2017	G20	"Another set of issues, Merkel reported, are messenger services. The published statement sounds clandestine, saying: 'In line with the expectations of our peoples we also encourage collaboration with industry to provide lawful and non-arbitrary access to available information where access is necessary for the protection of national security against terrorist threats.' But it is clear that the target is encryption. They have to be able to understand, where there is reasonable suspicion, the content of terrorist communication, Merkel explained." Source: G20 Reaches Agreement Against Terrorism, Appears To Target Encryption

DOMESTIC STATEMENTS

Dec 3, 2020	Australia Home Affairs Minister Peter Dutton	"Encryption is good in that sense where it protects us from criminals, but encryption is bad where it protects criminals from the police." Source: AFP's new approach to flush pedophiles from 'sewer of the internet'
Dec 2020	Children's Commissioner for England, Anne Longfield	Report on how end-to-end encryption threatens children's safety online Recommends four tests that tech companies must meet before rolling out end-to-end encryption.
Nov 2020	National Crime Agency, U.K.	If content on Facebook is end-to-end encrypted, there is a real risk that justice would not be served to victims of child abuse. Source: Facebook's encryption plans could help child abusers escape justice, NCA warns
Nov 13, 2020	E.U. Home Affairs Ministers	Joint statement by the E.U. home affairs ministers on the recent terrorist attacks in Europe Argued that competent authorities' access to digital information – whether it is traffic data or in some cases content data – is "essential for preventing and eliminating terrorist action." It called upon the Council to consider the matter of data encryption to ensure lawful collection of evidence while maintaining the trustworthiness of encrypted technology. [Note: This statement does not explicitly condemn or seek to undermine encryption. But the latter may be a possible consequence.]

Oct 20, 2020	Australian Department of Home Affairs Secretary Mike Pezzullo	"We are particularly concerned about Facebook's plans to go to end-to-end encryption of their entire platform to create, in effect, the world's biggest dark web." Source: Facebook Set to Create 'Biggest Dark Web' With End-To-End Encryption, Says Australian Minister
Oct 23, 2020	Australian Home Affairs Minister Peter Dutton	Social media giants, including Facebook, are blocking global law enforcement attempts to combat sexual exploitation of children. Dutton said that Facebook, in particular, is taking deliberate decisions with end-to-end encryption to starve referrals of matters that otherwise in previous years would have been made to law enforcement. Source: Facebook putting children at risk: Dutton
Feb 3, 2020	India	Report of the Adhoc Committee of the Rajya Sabha to Study the Alarming Issue of Pornography on Social Media and its Effect on Children and Society as a Whole Recommended that the law should be amended to permit breaking of end-to-end encryption to trace distributors of Child Sexual Abuse Material (CSAM).
June 3, 2020	Former U.S. Attorney General William P. Barr	Statement from Attorney General William P. Barr on Introduction of Lawful Access Bill in Senate Argued that warrant-proof encryption allows child predators, terrorists, drug traffickers, and even hackers to operate with impunity.
Jan 2020	Former U.S. Attorney General William P. Barr	On law enforcement's struggles with encryption: "We don't want to get into a world where we have to spend months and even years exhausting efforts when lives are in the balance…We should be able to get in once we have a warrant that establishes that criminal activity is probably under way." Source: Barr's Encryption Push Is Decades in the Making, but Troubles Some at FBI
Oct 2019	Indian Minister of Information Technology Ravi Shankar Prasad	The origin of messages on WhatsApp should be accessible. The right to privacy is not for those who misuse communication platforms. Source: Right to privacy not for those who abuse internet platform: Ravi Shankar Prasad

b. Summary of encryption facts vs. myths

Fact #1: Strong encryption is essential for internet security
Myth: Backdoors for targeted or exceptional access by law enforcement will not not undermine internet security

- ➔ Encryption is a mathematical process that cannot be selectively applied. Any demand for a backdoor that only works for the government is essentially at war with mathematics.
- ➔ A backdoor to encrypted content is a security flaw that makes the entire system and the underlying data vulnerable. Even if it is created only for government access, it will inevitably be exploited by a host of other malicious actors.

Fact #2: Giving law enforcement exceptional access threatens human rights and democracy
Myth: Law enforcement backdoors will not impact our rights or democracy

- ➔ Encryption is critical to democratic governance and the protection of the right to privacy and the right to freedom of expression in the digital age. Weakening encryption through exceptional access mechanisms jeopardizes these basic human rights and democracy as a whole.
- ➔ Encryption is particularly necessary for certain individuals and groups, including journalists, lawyers, doctors, and vulnerable communities whose work and lives depend on the availability of communication channels free from the possibility of surveillance.

Fact #3: Strong encryption strengthens privacy *and* security
Myth: To achieve security, we must sacrifice privacy

- ➔ The framing of the debate on encryption policy as “privacy versus security” is inaccurate and premised on a false binary. The two are mutually reinforcing principles.
- ➔ A more appropriate framing would be “security versus security,” as encryption not only protects privacy, it also protects security. This reframing would help ensure a purported “security” policy does not become an “insecurity” policy, creating more dangers than it seeks to prevent.

Fact #4: Law enforcement has entered the golden age of surveillance — without breaking encryption
Myth: Law enforcement is facing a “going dark” problem which makes it necessary to break encryption

- ➔ The “going dark” metaphor is inaccurate. It implies that technological changes have diminished surveillance capabilities, when they have vastly expanded.
- ➔ A more accurate metaphor is “a golden age of surveillance,” as far more data about individuals is available today than ever before, including our location information, information about our contacts, and many other previously unrecorded details that can be compiled to create “digital dossiers” that paint an intimate portrait of our daily lives.

Fact #5: Weakening encryption will not stop criminals and terrorists from using strong encryption

Myth: Weakening encryption is an effective measure to counter terrorism and criminal activity

- ➔ The effect of weakening encryption is that the general public is deprived of a platform where data and fundamental rights are protected. Criminals will simply shift to encrypted platforms available in foreign jurisdictions or on the black market, or they may even create their own.
- ➔ Increased surveillance capabilities often lead to invasive surveillance without sufficient evidence of its effectiveness. One study in the U.S.suggests that the link between increased surveillance capabilities and prevention of terrorism is tenuous. Regardless of efficacy for fighting terrorism, it is not necessary or proportionate to jeopardize the privacy and security of all users of a platform or system in the hope of identifying the fraction that engages in criminal conduct.

Fact #6: Strong encryption contributes to children’s safety online

Myth: Encryption makes the internet unsafe for children

- ➔ Like other criminals, perpetrators of crimes against children will turn to alternative encrypted platforms offered in foreign jurisdictions, or create their own platforms, to hide their activities. That means that the criminal activity will persist – it will simply move out of law enforcement’s reach, precluding lawful access even to metadata that can be instrumental in investigations.
- ➔ Children need encrypted platforms where the identity of individuals they are interacting with can be authenticated, and where their personal information is not at risk of exposure to third parties. With more children online due to the global pandemic, governments should encourage use of strong encryption to keep children safe, not deliberately introduce security vulnerabilities into the technology they use.

Fact #7: Mandating “traceability” will risk privacy chill free expression

Myth: Traceability must be implemented to prevent the spread of disinformation

- ➔ Traceability puts anonymity and the right to privacy at risk and has a chilling effect on free speech. It is therefore incompatible with both human rights and democracy.

- ➔ Traceability has limited utility in practice and will not serve as an effective tool to combat disinformation.

Fact #8: Strong encryption is crucial for cybersecurity and protects national security

Myth: Exceptional access to encrypted content is necessary to protect national security

- ➔ Strong encryption is vital for a resilient cybersecurity infrastructure that safeguards national security. Undermining encryption imperils national security.
- ➔ The increase in cybersecurity incidents and targeted breaches is an argument for, not against, strong encryption. Without strong encryption, we would see more unauthorized access and exposure of classified information, a boon to cybercriminals or state-sponsored adversaries. We would also see more successful attacks on essential infrastructure such as healthcare systems, elections, and public transport, as encrypted systems help keep their operations secure.

Fact #9: Strong encryption maintains trust in the digital ecosystem and supports economic growth

Myth: Deliberately undermining encryption will have no effect on the economy

- ➔ Encryption is a cornerstone of the modern digital economy, maintaining the confidentiality of customers' data and the authenticity of financial transactions. Trust in encrypted systems spurs investment, innovation, and economic growth.
- ➔ Encryption can also prevent or mitigate the impact of cybersecurity incidents that would otherwise do more damage and cost more money. It both reduces the risk of data breaches and controls the costs of such breaches, aiding commercial interests and supporting the economy as a whole.

Fact #10: Law enforcement and intelligence agencies don't have to break encryption to investigate crime

Myth: Authorities have no alternative but to break encryption

- ➔ Intelligence and law enforcement agencies already benefit greatly from the vast increase in data about individuals that is available in the digital age. There is no evidence to show that undermining encryption is a necessary, proportionate, or effective means to achieve government objectives in modern, rights-respecting democracies.
- ➔ In most cases, authorities still rely primarily on traditional evidence such as witnesses, informants, physical evidence, and business records from banks and cell companies. Undermining encryption and weakening security for everyone in an attempt to get all possible evidence in specific cases does not align with human rights and freedoms, and in practice, will never be a substitute for good investigative work.