TECH HIVE ADVISORY

IKIGAI

A GUIDE TO ENCRYPTION

Supported By: Internet Society

About Tech Hive™

Tech Hive Advisory Limited ("Tech Hive") is a technology policy advisory and research firm that works with private and public organisations on issues involving technology, business, and law. As an innovation partner, we help our clients get ready for and adjust to how new technologies change and affect long-standing practices.

Our experience and capability extend across Research and Policy Advisory, Privacy and Data Protection, Data Ethics, Cybersecurity, Regulatory Intelligence, Start-Up Advisory, and Digital Health. We make sure that our advice helps our clients by knowing their business and the markets in which they work. We do this by keeping track of policy and legislative changes and gathering accurate intelligence on them.

Contact: contact@techhiveadvisory.org.ng

About Ikigai Innovation Initiative™

The Ikigai Innovation Initiative, or "Ikigai," is a non-profit organisation that was set up to be Africa's one-stop shop for technology policy. We promulgate diverse research on technology policy and legal frameworks across Africa. We also talk to the right people about how the law, business, and technology interact and push for better policies for the ecosystem as a whole.

As a research centre focused on emerging technologies, policy, and research, we often collaborate with leading research institutes, academia, organisations, civil society, and individuals on policy affecting technology. We also publish whitepapers, reports, policy briefs, infographics, how-to guides, academic journals, and other publications, and we contribute to them.

Contact: policy@ikigaination.org

Authors

Adedolapo Evelyn Adegoroye

Oyindamola Banjoko

Victoria Adaramola

Editors

Olorunjoba Oguntunde

Ridwan Oloyede

Disclaimer - Usage of the Toolkit

This toolkit is both general and educational. It is not meant to be a source of legal or technical advice, and you should not use it as such. The toolkit's information and materials may not apply in all (or any) situations. So, you should not act on them without getting specific legal or technical advice based on your situation.

The tools suggested in this toolkit are merely suggestions on how to improve your privacy and security posture as a business.

The absence of any trademark or service mark from this list does not waive Tech Hive and Ikigai's intellectual property rights in that name, mark, or logo.

Introduction

From the beginning of time, people have always attempted to send private and hidden messages using symbols, signals, images, and numbers. Technology has made this process much more complex, but the intent remains similar. With the increased adoption of technology and the proliferation of internet-enabled devices, it has become necessary to defend human rights in the digital age. Governance is going digital, and more businesses and services have become technology enabled. Failure to ensure appropriate security can lead to a high cost in the digital age.

Encryption technology has served as a bastion of the preservation of confidentiality of the information and the preservation of human rights. Encryption has become necessary and important today because it protects confidential data by converting it into ciphertext, a form that is unreadable without the associated encryption key.[1] Essentially, the information will be accessible by an unauthorised, i.e. the party without the associated encryption key. Encryption makes it nearly impossible for cybercriminals or other unauthorised parties to steal and misuse the data since only those with an encryption key can decipher the data and reveal the true information. Encryption keeps data out of cybercriminals' reach, maintains privacy, and maintains the confidentiality of such information, just as it secures our homes, restricts access to critical infrastructure, and protects a company's valuable and tangible y properties. However, well-intentioned, the proposals to restrict this vital type of security could jeopardise the safety it offers.[2]

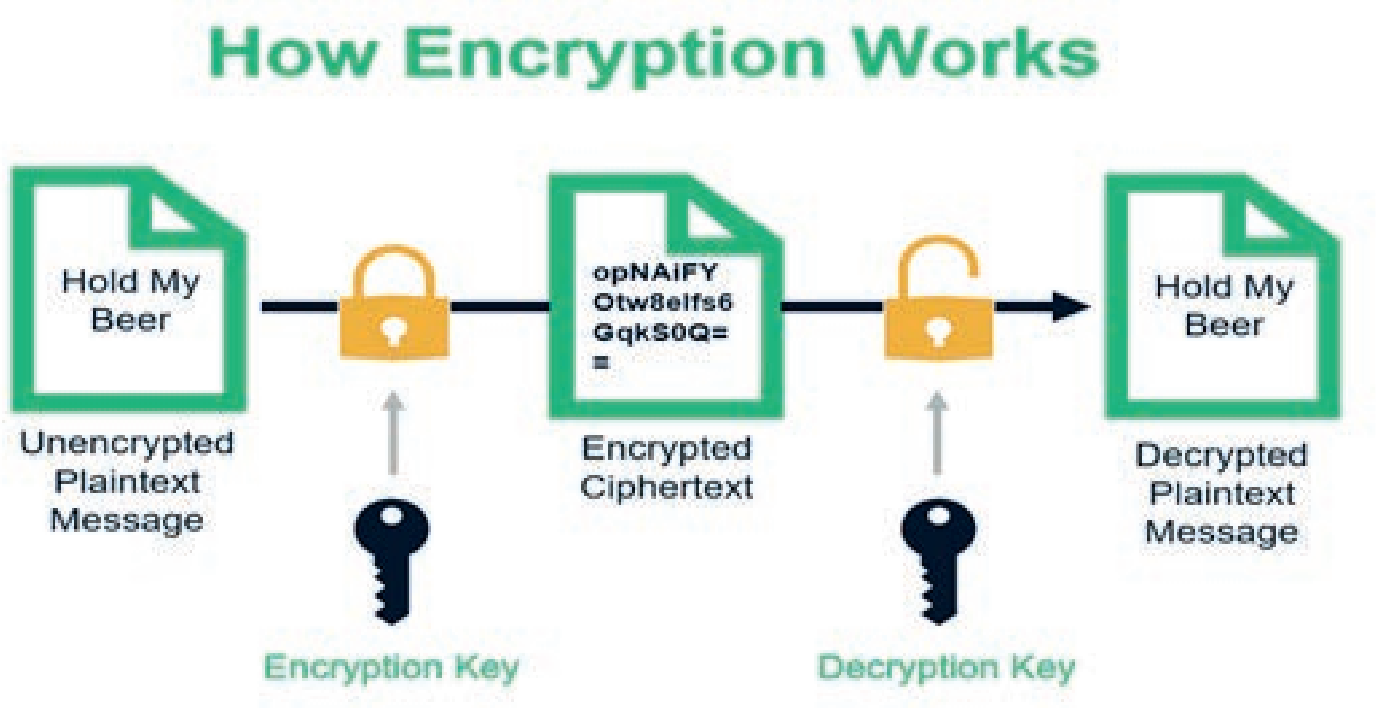

Figure A[3]

Understanding the role of encryption?

Encryption takes legible data and converts it into random and unreadable text. While encrypted data appears to be random, encryption follows a logical, predictable pattern that anyone with the encryption key can decrypt and return to plaintext. True secure encryption employs sufficiently complex keys that an unauthorised third party (someone who does not have the key or access to the key) is unlikely to decrypt or gain access to the ciphertext.[4]

Encryption is what protects us when we visit a website and have to pay for goods and services online; it protects our communication, guarantees the integrity of electronic signatures, and protects against any form of intrusion (inclusive of governmental incursion), among other things. For example, end-to-end encryption in communication tools guarantees non-interference and interception of the communication.

Use Cases of Encryption

We come across end-to-end encryption in our day-to-day use of the digital space, either through communication, banking, or the use of websites generally. Some of the use cases of end-to-end encryption include:

1. To protect sensitive information like consumer credit card data, an electronic point-of-sale (POS) system provider would incorporate end-to-end encryption in its package.

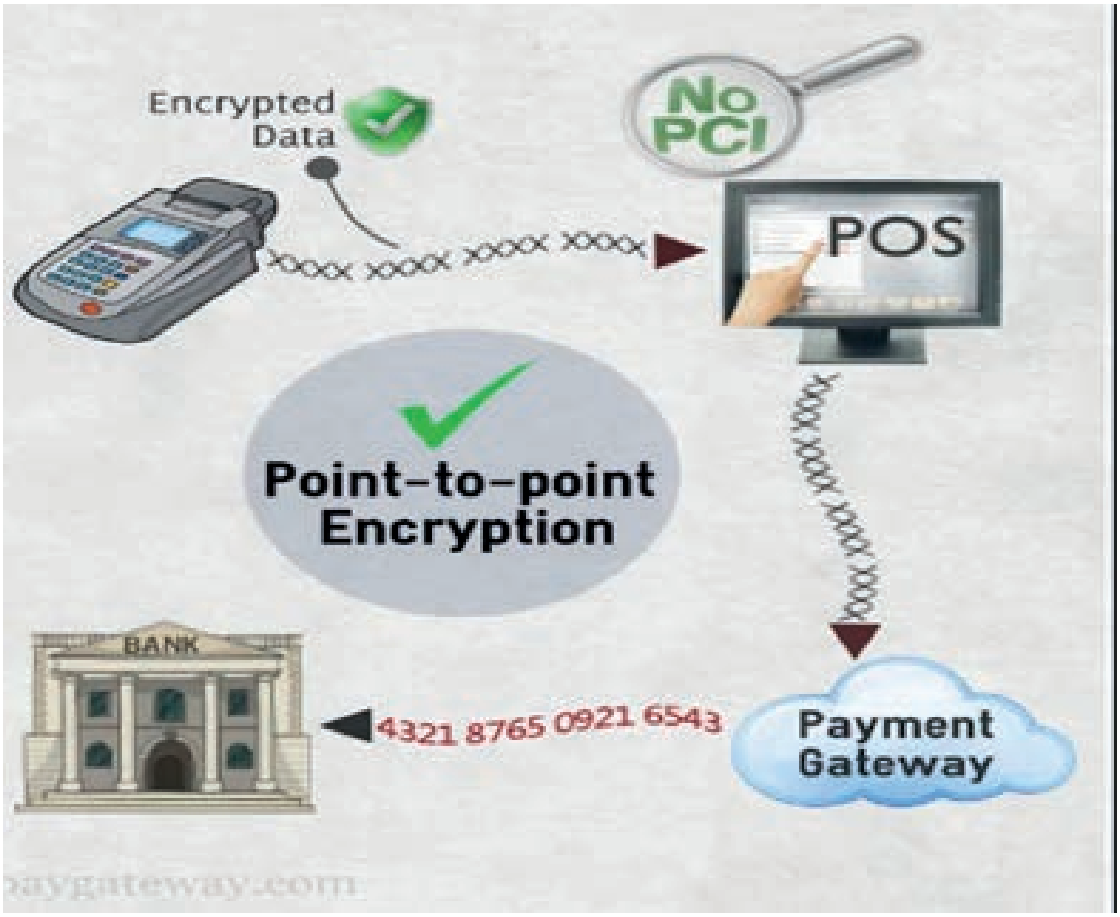

Figure B[5]

2. End-to-end encryption is used by retailers to comply with the Payment Card Industry Data Security Standard (PCI DSS), which prohibits the storage of card numbers, magnetic stripe data, and security codes on client devices.

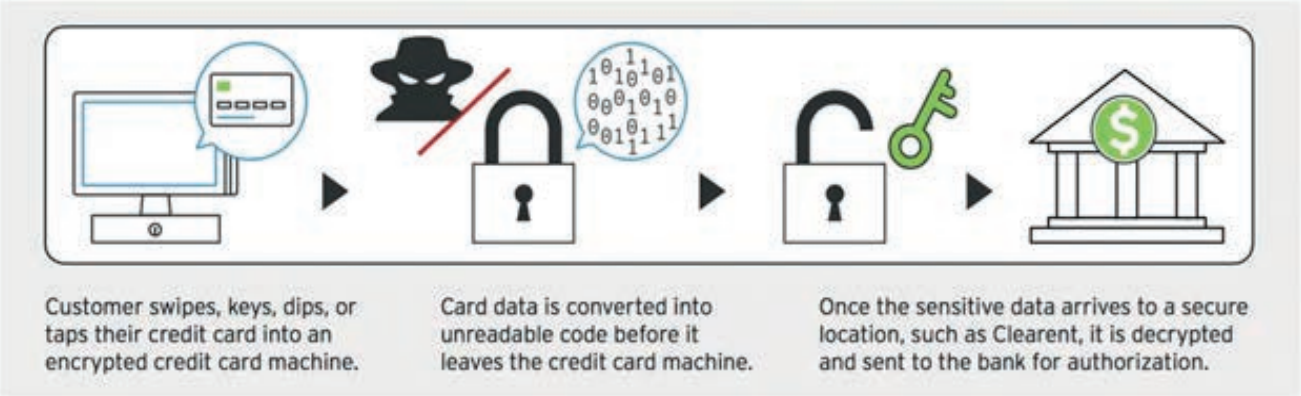

Figure C[6]

3. WhatsApp, the messaging app, incorporated end-to-end encryption since April 2016. Regardless of the content shared, all users have enjoyed security on the platform. Apple's iMessage protects users with end-to-end encryption by default on iOS and macOS. However, if you have iCloud backup turned on, which is a standard option for most users, this will produce a copy of the data that becomes accessible to Apple, effectively breaking iMessage's purported security feature (end-to-end encryption). Telegram and Signal are other messaging apps incorporating end-to-end encryption features on their platforms.[7]

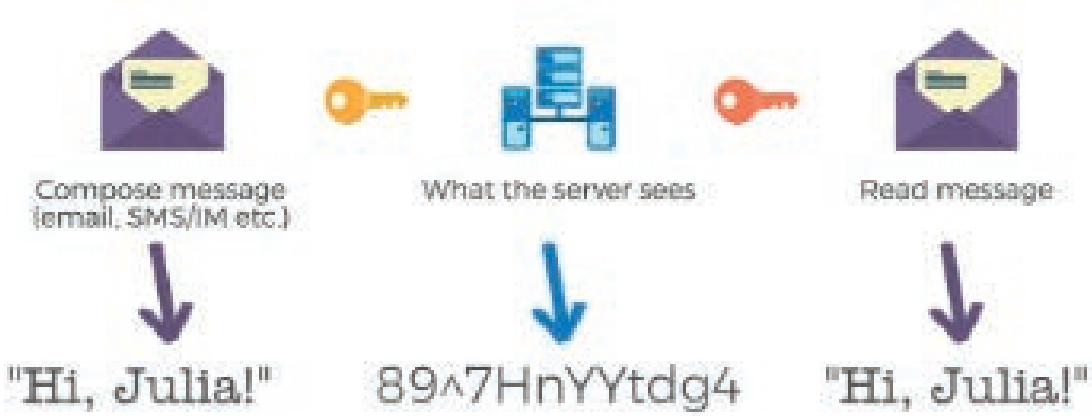

Figure D[8]

4. Encryption is available in password managers such as 1Password, BitWarden, LastPass, and Dashlane. A third party will not have access to your password vault because of the availability of the encryption feature.[9]

5. Encryption features are built into your browser and kick in when you engage in online behaviour that necessitates data security during data transmission. The Uniform Resource Locator (URL) in your browser's address bar begins with https:// rather than http://, the 's' evidences the availability of security for anything done on such website, be it payment or communication. [10]

Figure E[11]

6. When you use your credit card to make an online purchase, the credit card number is sent to the retailer via your computer. the relevant data is immediately encrypted by an automated algorithm. The retailer will then receive the encrypted data, which can only be accessed with the corresponding key. , this security has been made possible by encryption.[12]

7. Cryptocurrencies stay secure by relying on modern encryption methods and secure the nature of transactions on a blockchain.[13] Cryptocurrency holders use private keys to verify that they are owners of their cryptocurrency in order to access their cryptocurrency assets. Using encryption, the publicly accessible information on the blockchain is encrypted, preventing anyone without the secret key from accessing the information.[14]

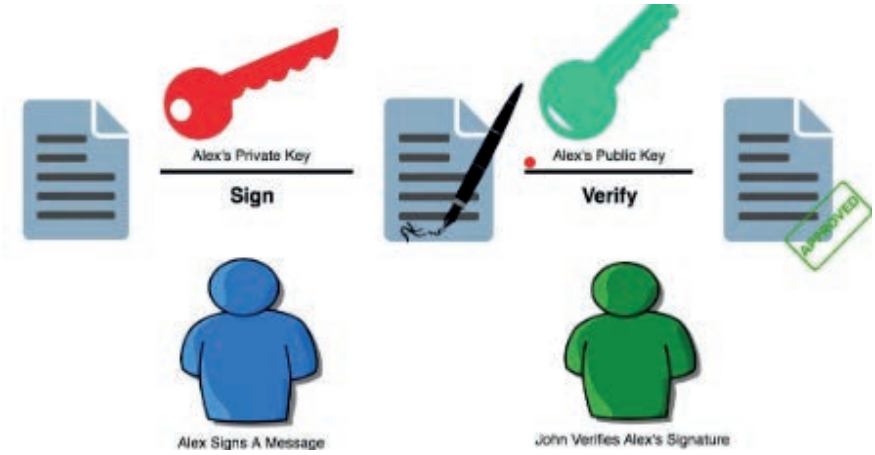

Figure F[15]

8. When it comes to storage, encryption is used to convert data to secret codes that hide the true meaning of data. Storage Encryption occurs at the firmware level of disks that are equipped with special firmware and hardware to provide additional security, also known as self-encrypting disks (SEDs). SEDs can operate either in unprotected mode like regular disks or in a protected mode requiring authentication after the power-on process.[16]

9. For data transfer, online banking employs industry-standard protocols that rely on encryption. While engaging in any online banking transaction, encryption ensures the safety of the data exchanged between your browser and the bank. Authentication ensures that you are interacting with the correct server. This protects you or your bank from being impersonated by another computer. Encryption scrambles sent data to prevent sensitive data from being intercepted and to ensure that only the server to which the data is being sent can read it.

Data integrity ensures that the data you sent to the bank was not tampered with during the transfer. After sending the message, the system will notice if data is added or deleted. The connection is dropped if there has been any manipulation.[17]

War against encryption

Despite the benefits of encryption, various governments worldwide have deliberately attempted to weaken or break encryption. These laws require telecommunications, internet, and financial service providers to weaken, break, or create a backdoor for encryption, allowing law enforcement access to encrypted data. In Australia, for example, law enforcement can compel businesses to hand over data and decrypt encrypted data.[18]

Some of the popular ways in which governments continue to interfere is through the requirement placed on telecommunication service providers to install decrypting capability on their installations or the authorisation given to law enforcement to access encrypted data without court supervision or sufficient human rights safeguards. In Nigeria, for example, law enforcement can request encrypted communication without the involvement of a court.[19] In addition, several regulations have been enacted in India over the years to allow the government access to encrypted data. The Indian government has used various social issues, such as mob action and the spread of child pornography, to justify the need for personal data decryption. For example, between 2017 and 2018, there were reports of mob actions sparked by misinformation disseminated via WhatsApp[20]. In response to these vices, moves were made to regulate data encryption. In 2018, the Indian Ministry of Electronics and Information Technology introduced a draft of new intermediary rules for social media platforms.[21] The regulation sought to hold social media platforms accountable for combating fake news. In 2021, this law was revised to include a requirement for social media intermediaries and significant social media platforms to identify the first originator of a message. Significant social media intermediaries must proactively identify and notify any party attempting to access content depicting rape and child sexual abuse.[22] This changes the end-to-end encryption that should come with these platforms, because the intermediaries must decrypt the message flow to know the contents covered in compliance with the regulation.[23]

These concerns have been documented in a recent UN report on privacy in the digital age. According to the United Nations, encryption is becoming increasingly restricted.[24] The report also highlighted the role of encryption in preserving the right to privacy and other human rights.

While we acknowledge the role of law enforcement in investigating crimes, preventing crimes and terrorism, and other national security concerns, encryption should not be breached where evidence can be sourced through other technical means, where human rights safeguards are absent, or where oversight functions and transparency are missing.

A call to defend the preservation of encryption

The Nigerian Cybercrimes Act 2015 and the Lawful Interception of Communication Regulation 2019 permit the decryption of encrypted communication without a court order.[25] Similarly, some policy measures introduced by the Nigerian government challenge the aim of anonymity online. For example, the government recently mandated SIM registration and linked national identity registration to SIM registration.[26] The Nigerian government is investing in technologies aimed at weakening encrypted communication. In July, the Nigerian Senate approved USD 11,674,287 to procure surveillance tools to monitor WhatsApp communication.[27] End-to-end encrypted communication protection is critical for preserving freedom of expression and the right to privacy.

Targeting encryption is incompatible with the integrity of communications, according to the International Principles on the Application of Human Rights to Communications Surveillance (also known as the "Necessary and Proportionate Principles") and the United Nations Draught Instrument on Government-led Surveillance and Privacy.[28] A similar warning was restated in Principle 40 (3) of the African Declaration of Principles on Freedom of Expression and Access to Information.[29]

When it comes to banking, shopping, and communicating, digital security is becoming increasingly vital. Encryption is at the heart of that security. As our lives become increasingly digital, everyone should be doing more, not less, to ensure data security. Encryption is at the heart of both modern-day economic and human rights enforcement and is a never-ending effort tied to all stakeholders, from software companies that create products to consumers that rely on these products to governments that rely on them for storage. Encryption is vital to the preservation and continuous trust across various digital services.

Encryption in Digital Communication

Technology has tremendously impacted how people communicate and interact with one another. The internet has provided us with numerous platforms and methods for interacting with friends, family, colleagues, and even strangers. However, this is a two-edged sword because it allows platform owners, operators, and third parties to eavesdrop on conversations. When you send data over the Internet, it is divided into discrete "packets" that flow from computer to computer, guided across the network to their intended destination.[30] This means that computers throughout the network may gain access to shared communication between parties A and B, making encryption essential for the entire telecommunications industry and process. End-to-end encryption safeguards data and information as it moves from one device to another. The sending and receiving devices can see the original contents, but no one else should have the keys to decrypt the communication.[31]

Encryption closes the backdoor for unauthorised third parties, platform owners, and even the government to intercept communications. As encryption is critical to the security of conversations, legislation and regulation should not jeopardise that security due to the potential harm to people's rights, particularly their right to free expression and privacy. Some social media platforms have adopted end-to-end encryption as a default setting to protect their users. For example, WhatsApp displays the caption below to inform users that messages exchanged on the platform are end-to-end encrypted.

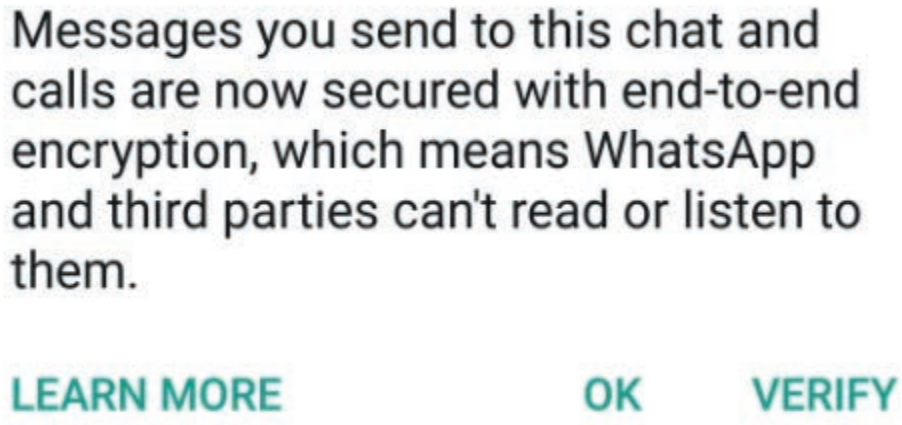

Figure G

Some other platforms require users to go a step further and configure their security settings to enable encryption rather than leaving it as the default setting. For example, on Facebook Messenger, users can enable a secret conversation feature to ensure that certain communications are encrypted.

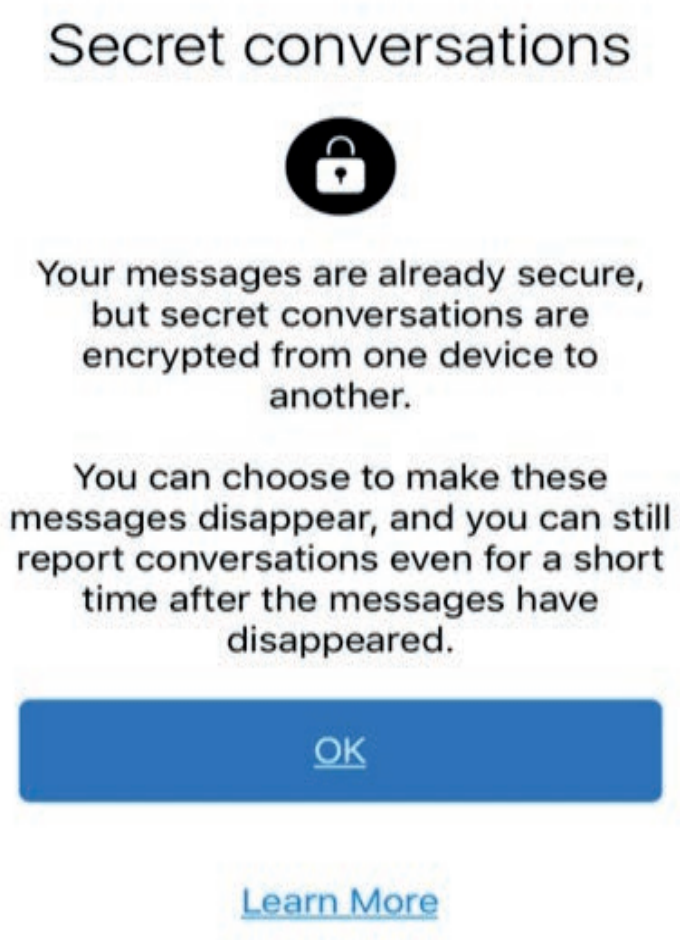

Figure H

Some social media platforms have been reported to use no encryption at all. The illustration below shows a representation of platforms and their use of end-to-end encryption.

Figure I[32]

Encryption, Anonymity and Human Rights

Human rights are standards that recognise and protect the dignity of all human beings.[33] The right to privacy is provided for under Chapter 4 of the 1999 Constitution of Nigeria as part of the fundamental human rights. Section 37 of the Constitution provides that "the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected."[34]

Article 12 of the United Nations Declaration for Human Rights also provides for the right to privacy, stating that "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Article 40 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa[35] provides that: "*States shall not adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows, and data localisation requirements, unless such measures are justifiable and compatible with international human rights law and standards*."

These provisions reinforce the fact that privacy is a fundamental human right and should be respected by the States and institutions. Hence, it is expected that there is no interference from third parties, whether state or private entities, with the right to privacy, irrespective of the platforms used.

The right to privacy includes the right of an individual to be left alone, to be free from unwarranted publicity, and to live without unwarranted interference by the public in matters with which the public is not necessarily concerned.[36] Encryption ensures that the right to privacy is maintained in the sense that parties are able to restrict their communications among themselves. It also confers the responsibility on platforms to safeguard communications from unauthorisedparties that users would not want to be privy to. Also, parties are able to control who has access to their information with encryption.

Encryption also safeguards users' communication from government surveillance. There are certain informationthat should be kept away from the government and the public. While the government seeks to actively have access to these information, such access may cause total interference in the lives of the affected person and can potentially make individuals targets of inhuman treatment. In effect, this may impact the right to dignity of the human person where such interference occurs. Encryption offersthe possibilities of eliminating communication surveillance and intrusion by unauthorised parties.

Encryption is also inextricably connected to the concept of anonymity. With the enormous opportunities created by the internet, there is the pressing need to also ensure that people are not just able to express themselves but also to do so without any fear, concern, or retribution.[37] Online users may use pseudonyms (or fake e-mail or social media accounts) to conceal their identities, images, voices, locations, and other details, but the privacy these pseudonyms offer is only temporary and can be unmaskedby governments or other parties with the requisite skill set and ability. Furthermore, in the absence of tools that combine encryption and anonymisation, the digital traces that users leave behind make their identities easiy discoverable.[38]

Therefore, it cannot be said that there is a right to privacy where people are unable to express themselves freely without fear of being prosecuted for their expressions and communications, due to a lack of anonymity because their private expressions and information are being watched. Where this is the case, the rights of people to freedom of expression become more and more eroded. To ensure anonymity, strong technical and legal processes must be adopted to make it difficult to unmask or discover the identities of the parties involved in a correspondence. Where there are no strong measures in place and people's identities can be uncovered easily via different means such as hacking, government orders to service providers, or through an existing database, then anonymity, as well as the right to privacy and freedom of expression cannot be said to be protected. When it comes to understanding of the true degree of anonymity in any given circumstance or country, the following points are notable:[39]

- Can people access services without registering or without registering with their legal identity?
- Do service providers require an online account to be linked to a government-issued identity document or to other systems that are linked to legal identity?
- Do service providers retain data, such as logs, that could be used to identify their users in the future?
- Do users have access to technical means to conceal their identity, such as privacy-enhancing technologies that make it hard to identify users?
- Do users have confidence that their identity will not be associated with their activities against their will?
- In order to strip an individual of the anonymity they choose, what effort must be taken by other parties?
- Can third parties determine an individual's identity without recourse to the courts, or must legal processes be pursued?

However, with encryption, anonymity is possible because it precludes all unauthorised parties from accessing people's private correspondence because the transmission and delivery of communication are protected.

Why is End-To-End Encryption Important?

1. Privacy Concerns: As the internet becomes more integrated into our daily lives, privacy concerns increase.

2. Hacking Issues: Hacking concerns can be minimised using encryption.

3. Regulations: The requirement to comply with legislation typically drives the adoption of encryption. Some organisations are expected to prevent unwanted third parties from accessing sensitive data.

4. Confidentiality: guarantee the confidentiality of digital data stored on computers and transmitted via the internet or any other computer network

5. Authentication: Confirms a message's origin

6. Integrity: Verifies that a message's contents haven't changed after it was sent

7. Nonrepudiation: senders are unable to deny sending the encrypted message

What Are the Benefits of Encryption?

1. Encryption improves the security of digital services.

2. Encrypted data is protected between the receiver and sender. This has data protection, data security and credibility benefits.

3. Encryption allows you to securely share files and data

Figure J[40]

4. Encryption protects your privacy. "I don't have any data worth stealing," is the most typical justification against implementing proper cybersecurity policies. This assertion is false, as cybercriminals frequently target individuals in order to steal personal information/data.[41]

5. Encryption can prevent identity theft and blackmail.

The most recent trend is to steal all of your data and then blackmail you into paying a ransom. If you don't pay, your information will be released online, used for identity theft, or sold to the highest bidder. [42]

6. Encryption also enables free expression in certain professions to protect client privileges and intellectual freedom. For example, journalists and their sources can speak without fear, retaliation, or pushback from the government.

Conclusion

Government and law enforcement agencies addressing the challenges of urban and citizen security with strict counter regulations that seek to weaken encryption is in more than one way, creating greater problems than the problem they intended to solve. Backdoors to encryption cannot be kept a secret from people with the knowledge to identify and take advantage of the vulnerabilities, whether they are state or non-state, lawful or illegal. It is a seemingly universal position among technologists that there is no special access that can be made available only to government authorities, even ones that, in principle, have the public interest in mind.[43] What this implies is that a backdoor for the government is a backdoor for all other actors, the good, the bad, the ugly and even the indifferent. In these times where people have become more reliant on digital communications for everything, including even work, there has never been a better time to advocate for stronger encryption measures to protect people's privacy and security.

References

1 Chen, Stephen. “What Is Data Encryption and Why Is It Important?” TitanFile, 13 June 2022, https://www.titanfile.com/blog/what-is-data-encryption-and-why-is-it-important/.

2 ‘Encryption: Why It Matters’ <http://encryption.bsa.org> accessed 4 October 2021

3 Mehta, Medha. “What Is Asymmetric Encryption & How Does It Work?” InfoSec Insights, 3 Nov. 2020, https://sectigostore.com/blog/what-is-asymmetric-encryption-how-does-it-work/.

4 ‘What Is Encryption and How Does It Work?’ (SearchSecurity) <https://searchsecurity.techtarget.com/definition/encryption> accessed 4 October 2021

5 “Advantages of Point-to-Point Encryption (P2PE) | UniPay Gateway.” UniPayGateway, https://unipaygateway.com/unipay-gateway/point-to-point-encryption-diagram/. Accessed 10 Oct. 2022.

6 “Tokenization Vs Encryption.” Clearent, https://clearent.com/insight/tokenization-vs-encryption/. accessed 10 Oct. 2022.

7 ‘What Is End-to-End Encryption and Why Is Everyone Fighting over It?’ (IT PRO) <https://www.itpro.co.uk/security/encryption/359943/what-is-end-to-end-encryption-and-why-is-everyone-fighting-over-it> accessed 6 December 2021

8 “End-to-End Encryption.” Shoestring Collective Tech Resources, https://techresources.shoestringcollective.com/knowledge-base/end-to-end-encryption/. accessed 10 Oct. 2022.

9 Hoffman C, ‘What Is End-to-End Encryption, and Why Does It Matter?’ (How-To Geek) <https://www.howtogeek.com/711656/what-is-end-to-end-encryption-and-why-does-it-matter/> accessed 7 December 2021

10 What Is End-to-End Encryption?’ (Lifewire) <https://www.lifewire.com/what-is-end-to-end-encryption-4028873> accessed 7 December 2021

11 “Fastmail | Secure Websites on FastMail.” Fastmail Blog, 6 Sept. 2018, https://fastmail.blog/privacy-security/secure-website-support/ accessed 29 Sept. 2022.

12 Ibid

13 “What Is Encryption in Blockchain and Crypto?” Gemini, https://www.gemini.com/cryptopedia/what-is-encryption-blockchain-symmetric-asymmetric. accessed 29 Sept. 2022.

14 “Encrypting On-Chain Data.” Blockchain Patterns, https://research.csiro.au/blockchainpatterns/general-patterns/data-management-patterns/encrypting-on-chain-data/. Accessed 29 Sept. 2022.

15 Massessi, D. Blockchain Public / Private Key Cryptography In A Nutshell <https://medium.com/coinmonks/blockchain-public-private-key-cryptography-in-a-nutshell-b7776e475e7c> accessed 5 October 2021

16 Alexb. How Storage Encryption Works. https://library.netapp.com/ecmdocs/ECMP1368859/html/GUID-1336E9A5-2ADC-4EB4-95D9-5328DB9A4E56.html. accessed 30 Sept. 2022.

17 Anin-Boateng B, ‘What Is Encryption: This Is How Apps Keep Your Data Safe’ <https://www.newcmi.com/blog/it-providers-it-experts-it-commpanies-what-is-encryption> accessed 7 December 2021

18 Sam Bocetta, 'Australia's New Anti-Encryption Law Is Unprecedented and Undermines Global Privacy | Sam Bocetta' (14 February 2019) <https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/> accessed 29 September 2022.

19 Tony Roberts and others, 'Surveillance Law in Africa: A Review of Six Countries' <https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y>.

20 Jha AB Prateek, 'Understanding the Encryption Debate in India' (Carnegie India) <https://carnegieindia.org/2021/09/13/understanding-encryption-debate-in-india-pub-85261> accessed 19 October 2022

21 Jha AB Prateek, 'Understanding the Encryption Debate in India' (Carnegie India) <https://carnegieindia.org/2021/09/13/understanding-encryption-debate-in-india-pub-85261> accessed 30 September 2022

22 Ibid

23 Ibid

24 'Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns' (OHCHR2022) <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report> accessed 29 September 2022.

25 Tony Roberts and others, 'Surveillance Law in Africa: A Review of Six Countries' <https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y>.accessed 19 October 2022

26 Ndubuisi Francis, 'FG Directs SIM Card Be Linked to National Identity Number – THISDAYLIVE' (Thisdaylive.com2022) <https://www.thisdaylive.com/index.php/2020/12/16/fg-directs-sim-card-be-linked-to-national-identity-number/> accessed 19 October 2022.

27 QueenEsther Iroanusi, 'Nigerian Govt Moves to Control Media, Allocates N4.8bn to Monitor WhatsApp, Phone Calls' (Premium Times Nigeria12 July 2021) <https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html> accessed 19 October 2022.

28 'Necessary & Proportionate' (Necessary & Proportionate2013) <https://necessaryandproportionate.org/13-principles/> accessed 19 October 2022.

29 'African Commission on Human and Peoples' Rights Legal instruments' (Achpr.org2019) <https://www.achpr.org/legalinstruments/detail?id=69> accessed 19 October 2022.

30 "Types of Encrypted Communication." Small Business - Chron.Com, https://.chron.com/types-encrypted-communication-52746.html. accessed 30 Sept. 2022.

31 'End-to-End Encryption: Important Pros and Cons' (CIO Insight, 2 June 2021) <https://www.cioinsight.com/security/end-to-end-encryption/ > accessed 5 October 2021

32 Elsayed-Ali, Sherif. "Ranking Messaging Apps on Encryption and Human Rights." Medium, 25 Oct. 2016, https://medium.com/@sherifea/ranking-messaging-apps-on-encryption-and-human-rights-9abdfe90a6c4. accessed 3 October 2022.

33 'What Are Human Rights?' <https://www.unicef.org/child-rights-convention/what-are-human-rights> accessed 30 September 2022

34 Section 37 of the 1999 Constitution of the Federal Republic of NIgeria.

35 Declaration of Principles on Freedom of Expression and Access to Information in Afric<https://www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf>

36 'The Legal Right to Privacy | Stimmel Law' <https://www.stimmel-law.com/en/articles/legal-right-privacy> accessed 3 October 2022.

37 Article 19 of the Universal Declaration of Human Rights

38 UN Human Rights Report: The Role of Encryption and Anonymity in Protecting Privacy and Freedom of Expression | Public Intelligence. 31 May 2015, https://publicintelligence.net/un-encryption-privacy-anonymity/.

39 "Anonymity and Encryption." Docslib, https://docslib.org/doc/11440497/anonymity-and-encryption. Accessed 4 Oct. 2022.

40 'End-to-End Encryption Meaning, Example & Security □' <https://www.wallarm.com/what/what-is-end-to-end-encryption> accessed 4 October 2022.

41 'Advantages of Using Encryption Technology for Data Protection' <https://ghostvolt.com/articles/benifitsofencryption.html> accessed 5 October 2021

42 Ibid

43 UN Human Rights Report: The Role of Encryption and Anonymity in Protecting Privacy and Freedom of Expression | Public Intelligence. 31 May 2015, https://publicintelligence.net/un-encryption-privacy-anonymity/.


TECH HIVE
ADVISORY


IKIGAI


Internet
Society