

Committee: General Assembly 3

Issue: The Question of Encryption and Digital Privacy

Student Officer: Hend Wahdan (General Assembly 3 president)
Ayten Labib (General Assembly 3 Chair)

I. Introduction

To **encrypt** means to hide the meaning of information by changing its form.¹ Encryption has been made use of over the course of history. Julius Caesar communicated with his generals through means of **cryptography**, and the Nazis made use of such messages in the war as well. While encryption can be deciphered by a third party, **end-to-end encryption** is encoded exclusively for the access of the sender and receiver.² End-to-end encryption, also referred to as E2EE, is a secure communication method which is achieved when “the cryptographic keys used to encrypt and decrypt the messages are stored exclusively on the endpoints.” This is done through **public keys**, which are large numbers used to encrypt data.³

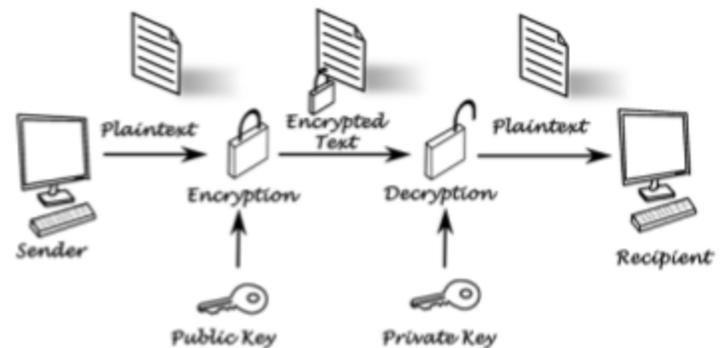


Figure 1 Public Key Encryption

“Plenty of companies brag that their communications app is encrypted...In many cases, the company itself holds the cryptographic key data that lets it decrypt your messages—and so, therefore, does any hacker who compromises the company or government official standing over its shoulder.”⁵

On digital media, online activity and personal information is often used and released without the permission of the user. **Digital privacy**, with relevance to this media, refers to the

¹ "Encrypt." Merriam-Webster.com. Merriam-Webster, n.d. Web. 22 Aug. 2017. <<https://www.merriam-webster.com/dictionary/encrypt>>.

² Titcomb, James. "What Is Encryption, How Does It Work and What Apps Use It?" *Technology*. The Telegraph, 29 Mar. 2017. Web. 22 Aug. 2017. <<http://www.telegraph.co.uk/technology/0/encryption-should-using/>>.

³ Rouse, Margaret, and Madelyn Bacon. "What Is End-to-end Encryption (E2EE)? - Definition from WhatIs.com." *SearchSecurity*. TechTarget, July 2015. Web. 22 Aug. 2017. <<http://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE>>.

⁴ Clark, Bryan. *How Does Encryption Work, and Is It Really Safe?* Digital image. *MakeUseOf*. N.p., 09 Mar. 2015. Web. 22 Aug. 2017. <<http://www.makeuseof.com/tag/encryption-care/>>.

⁵ Greenberg, Andy. "Hacker Lexicon: What Is End-to-End Encryption?" *Wired*. Conde Nast, 02 June 2017. Web. 22 Aug. 2017. <<https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/>>.

user's right to privacy.⁶ It is a right recognised by the United Nations Human Rights Office of the High Commissioner (OHCHR) and in the United Nations Declaration of Human Rights (UDHR). The topic of encryption, specifically E2EE, is a matter of digital privacy, which in itself is often dealt with as a privilege rather than a right. While some countries and organisations advocate for the protection of digital privacy and means of E2EE, others violate such rights for means of spying and surveillance.

II. Involved Countries and Organizations

Privacy International

Privacy International is a charity that exposes companies that enable government surveillance. Although the organisation is based in London, it “[advocates] for strong national, regional, and international laws that protect privacy.”⁷ Privacy International conducts research for the purpose of policy change, and informs the public of technologies and laws that compromise privacy. The organisation believes that it is a human right to know that private data is secure and under (one's own) control. “ Privacy is essential to human dignity and autonomy in all societies... We believe that technological developments should strengthen, rather than undermine, the right to a private life.”⁸

Privacy International is responsible for numerous projects. These include establishing a global privacy movement and looking into how data is exploited and advocating for more advanced legal and technological guidelines in accordance to such. They also challenge the capabilities of state surveillance through the reformation of surveillance laws, and restraint of government surveillance. Privacy International has been working globally and uploading reports on their progress and achievements.⁹

Access Now

Access Now works to protect and expand digital right of users internationally and tackle issues of privacy, digital security, human rights, and net discrimination. They work towards open and safe communications through means of “combining innovative policy, global advocacy, and direct technical support.”¹⁰ The organisation develops practices and policies that respect rights for long-term advancement in digital rights and online security, such as that implemented to reform the surveillance legislation in the United States. Through research and abidance of rights, Access Now works towards creating policy guidance for governments as

⁶ "What Is Digital Privacy." *IGI Global*. IGI Global, n.d. Web. 22 Aug. 2017.
<<https://www.igi-global.com/dictionary/digital-privacy/46799>>.

⁷ "Privacy International." *Privacy International*. Privacy International, n.d. Web. 22 Aug. 2017.
<<https://www.privacyinternational.org/>>.

⁸ Ibid

⁹ "Privacy International." *What We Do*. Privacy International, n.d. Web. 22 Aug. 2017.
<<https://www.privacyinternational.org/projects>>.

¹⁰ "Our Mission." *About Us*. Access Now, n.d. Web. 22 Aug. 2017. <<https://www.accessnow.org/about-us/>>.

well as corporations, and the public by commenting, adapting, and reforming policies of countries around the world such as Tunisia, Hungary, and Austria. Additionally, the organisation's team act as political advocates and provide a Digital Security Helpline for solutions regarding technological issues, and advice "to inform and support activists, journalists, human rights defenders, and civil society actors...at risk in circumstances where communications are not open, free, or safe."¹¹

United Kingdom

According to Australian attorney-general, George Brandis, Government Communications Headquarters (GCHQ), a British intelligence agency, can decipher messages that are end-to-end encrypted.¹² It has been revealed that the British government wants to allow intelligence agencies to have access to private messages by forcing backdoors to be built into the products of technology companies. This would violate the public's right to privacy as it would create a third party and break the end-to-end encryption. In accordance with the Investigatory Powers Act, the leaked draft government document includes "extreme new surveillance proposals."¹³ If made law, encryption would be banned. The draft is also evident of a great lack of government transparency.¹⁴

The UK government has "called for International co-operation to regulate the Internet so that it cannot be used as a 'safe space' for extremists to communicate and spread propaganda online."¹⁵ British officials blame popular internet companies for terrorist attacks since they believe that hate is spread online by extremists with the provision of "safe spaces." Theresa May, UK Prime Minister, said

"we need to work with allied, democratic governments to reach international agreements that regulate cyberspace to prevent the spread of extremism and terrorist planning. And we need to do everything we can at home to reduce the risks of extremism online...We need to deprive the extremists of their safe spaces online"¹⁶

¹¹ Ibid

¹² Sharwood, APAC Editor 14 Jul 2017 at 01:49 Tweet_btn(), Simon. "UK Spookhaus GCHQ Can Crack End-to-end Encryption, Claims Australian A-G." *The Register*. Situation, 14 July 2017. Web. 22 Aug. 2017. <https://www.theregister.co.uk/2017/07/14/uk_spookhas_gchq_can_crack_endtoend_encryption_says_australian_ag/>.

¹³ Sulleyman, Aatif. "UK Government Is Secretly Planning to Break Encryption and Spy on People's Phones, Reveals Leaked Document." *The Independent*. Independent Digital News and Media, 05 May 2017. Web. 22 Aug. 2017. <<http://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-security-services-phones-spy-break-encryption-gchq-mi5-technical-advisory-board-bskyb-bt-cable-a7719341.html>>.

¹⁴ Ibid

¹⁵ Lomas, Natasha. "We Want to Limit Use of E2e Encryption, Confirms UK minister." *TechCrunch*. TechCrunch, 05 June 2017. Web. 22 Aug. 2017. <<https://techcrunch.com/2017/06/05/we-want-to-limit-use-of-e2e-encryption-confirms-uk-minister/>>.

¹⁶ Ibid

Malaysia

The Malaysian government uses a program called FinSpy to spy on its citizens. The program is capable of stealing passwords, accessing accounts, screenshotting screens, recording conversations and keystrokes, as well as controlling cameras and microphones.¹⁷ Additionally, the government passed an amendment on the Security Offences (Special Measures) Act (SOSMA), “which authorizes phone-tapping and communications powers to the government,” mainly to prevent terrorism.¹⁸ Any sort of “invasion of privacy” principle has been rejected by the Malaysian court alongside that of other countries that abide by the English Common Law.¹⁹ It is easy to sell personal data to a third party in Malaysia due to “a public lack of awareness on giving and sharing personal data, especially when registering and signing on to services...[the] government and authority can easily monitor citizen movements due to the lack of data protection between government agencies.”²⁰ It is clear that the Malaysian government is infringing on its people’s privacy, while the majority of them are seemingly unaware. This concerns the United Nations as such a denial of digital freedom is a matter of human rights.

III. Focused Overview of the Issue

1) What is end-to-end encryption?

Encryption, derived from the Greek word *kryptos*, meaning hidden, has been around since 1900 BC, during the time of the ancient Egyptians²¹. Encryption or end-to-end encryption (E2EE) has become especially popular and an important part of daily life since 2014 when WhatsApp became end-to-end encrypted in November of that year²². End-to-end encryption as described by the Telegraph is “a way of transmitting a message so that it can only be read by the intended recipient, and not intercepted by accessing the servers or the networks via which the message is sent.”²³ These messages cannot be opened by anyone other than the sender and the receiver of the message. This is due to the messages appearing as long strings of numbers that can only be read by the sender or the receiver. End-to-end encryption is often compared to a lock

¹⁷ Kelly, Meghan. "These 5 Countries Were Ranked Best for Privacy (infographic)." *VentureBeat*. BackgroundChecks, 13 Oct. 2013. Web. 22 Aug. 2017.

<<https://venturebeat.com/2013/10/13/countries-privacy/>>.

¹⁸ "Digital Rights in Malaysia." *Digital Rights in Malaysia — English*. Sinar Project, 04 Nov. 2015. Web. 22 Aug. 2017. <<https://sinarproject.org/en/updates/digital-rights-in-malaysia>>.

¹⁹ "Privacy Rights, Data Protection, Security in Malaysia." *KASS*. KASS International, n.d. Web. 22 Aug. 2017. <<http://www.kass.com.my/data-protection/>>.

²⁰Ibid 18

²¹ "History of Encryption." *SANS Institute InfoSec Reading Room*. N.p., 2001. Web. 22 Aug. 2017. <<https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730>>.

²² Murgia, Madhumita. "WhatsApp Adds End-to-end Encryption: What Is It and What Does It Mean for You?" *The Telegraph*. Telegraph Media Group, 05 Apr. 2016. Web. 22 Aug. 2017. <<http://www.telegraph.co.uk/technology/2016/04/05/whatsapp-encryption-what-is-it-and-what-does-it-mean-for-you/>>.

²³ Murgia, Madhumita. "WhatsApp Adds End-to-end Encryption: What Is It and What Does It Mean for You?" *The Telegraph*. Telegraph Media Group, 05 Apr. 2016. Web. 22 Aug. 2017. <<http://www.telegraph.co.uk/technology/2016/04/05/whatsapp-encryption-what-is-it-and-what-does-it-mean-for-you/>>.

and key. Encryption is the lock, meaning that nobody except for those who have the key can open up the lock. The sender and the receiver of the message are the only people who have access to the messages that were and will be sent²⁴. They have the key to these messages. Pictures, voice notes, videos, documents, and calls are all end-to-end encrypted. There are a plethora of apps that include end-to-end encryption. Messaging apps such as WhatsApp, iMessage, Pryvate and signal operate using end-to-end encryption by default²⁵. These apps have become very popular due to their use of encryption.

2) Encryption and digital privacy

Moving on, digital privacy and end-to-end encryption are very closely connected to one another. To explain, digital privacy can be defined as “the right to privacy of users of digital media.”²⁶ It is not difficult to find personal information on the internet, and digital privacy states that a person has the right to keep their confidential information private. Digital privacy has become a very controversial topic recently and this is due to the differing viewpoints about whether privacy on the internet is a right or a privilege²⁷. With that being said, encryption clearly ties into digital privacy because people are looking for different ways and methods of keeping their personal information safe on the internet. Since people are looking for security on a daily level, apps like Whatsapp has proven worthy for long term usage. With the wide array of social media platforms that can easily be accessed, apps that use encryption offer safe alternatives for people where any person can store their private information and not be concerned about their information being spread or hacked into, as seen in various cases. Breaking encryption would limit the places where people can feel protected and safe on the internet.

3) Present Day Issues

It is indisputable that there are many issues surrounding encryption and impede on privacy in today’s world. Since encryption cannot be hacked into, there have been many terrorist attacks that have been planned through apps such as WhatsApp, Telegram and signal. There have been attacks in England, Barcelona, Paris, the US and Brussels. For example, in 2014, Apple implemented a new encryption system that was almost impossible to unlock²⁸. The encryption couldn't even be unlocked for higher authorities. This would clearly lead to some issues and in December 2015, the San Bernardino shooting occurred. Considered to be an act of terrorism, the shootings left 14 dead and 22 wounded and occurred during a party. The female attacker had

²⁴“WhatsApp Security.” *WhatsApp*. N.p., n.d. Web. 22 Aug. 2017. <<https://www.whatsapp.com/security/>>.

²⁵Titcomb, James. “What Is Encryption, How Does It Work and What Apps Use It?” *The Telegraph*. Telegraph Media Group, 29 Mar. 2017. Web. 22 Aug. 2017.
<<http://www.telegraph.co.uk/technology/0/encryption-should-using/>>.

²⁶ “What Is Digital Privacy.” *IGI Global*. N.p., n.d. Web. 22 Aug. 2017.
<<http://www.igi-global.com/dictionary/digital-privacy/46799>>.

²⁷Andriole, Steve. “Is Digital Privacy A Right Or A Privilege?” *Forbes*. Forbes Magazine, 07 Apr. 2017. Web. 22 Aug. 2017. <<https://www.forbes.com/sites/steveandriole/2017/04/07/is-digital-privacy-a-right-or-a-privilege/>>.

²⁸Yadron, Danny, Spencer Ackerman, and Sam Thielman. “Inside the FBI’s Encryption Battle with Apple.” *The Guardian*. Guardian News and Media, 18 Feb. 2016. Web. 22 Aug. 2017.
<<https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple>>.

made a facebook post during the attack, pledging her allegiance to ISIS²⁹. It was believed that there would be more information hidden somewhere and many of the phone calls between the attackers and different people were being looked into. Apple and the Federal Bureau of Investigation (FBI) were about to go to court after Apple's refusal to hack into one of the attacker's iPhones, except the case was suddenly dropped since the FBI had found a way to unlock the attacker's phone without Apple's help³⁰. Despite this, the case sparked major controversies about encryption and privacy in the present day.

A more recent example of the issues that encryption presents is the terrorist attacks that took place in Westminster in March 2017. That attack had occurred on Westminster bridge, using a Hyundai SUV, by ploughing through the crowd³¹. The attacker, Khalid Masood, also carried two large knives. About 5 people were killed and 55 had been left injured. Masood was later shot to death right after fatally stabbing an unarmed police officer. This attack has to do with encryption because of the fact that Masood had sent a text of relevance to it via the encrypted WhatsApp a mere two minutes before the attack was carried out³². The police were not able to access the message for several weeks due to the encryption³³. Since a bombing in Manchester took place soon after the Westminster attack, many countries such as the United Kingdom, United States, Australia, Canada, and New Zealand have shared their concerns about encryption. The concerns being about how they would not be able to access vital information to a terrorist case due to the usage of encryption, for example. After the Manchester bombing, The Telegraph had reported UK Home Secretary Amber Rudd accusing "WhatsApp of giving terrorists 'a place to hide' and said it was 'completely unacceptable' that they could communicate in secret."³⁴ Creating backdoors for the authorities has been suggested by many,

²⁹ Botelho, Greg. "San Bernardino Attack Investigated as Act of Terrorism." *CNN*. Cable News Network, 05 Dec. 2015. Web. 06 Oct. 2017. <<http://edition.cnn.com/2015/12/04/us/san-bernardino-shooting/index.html>>.

³⁰Yadron, Danny. "FBI Confirms It Won't Tell Apple How It Hacked San Bernardino Shooter's iPhone." *The Guardian*. Guardian News and Media, 28 Apr. 2016. Web. 22 Aug. 2017. <<https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino>>.

³¹Emily Allen; Barney Henderson. "Westminster Attack: Everything We Know so Far about the Events in London." *The Telegraph*. Telegraph Media Group, 22 Mar. 2017. Web. 22 Aug. 2017. <<http://www.telegraph.co.uk/news/2017/03/22/westminster-terror-attack-everything-know-far/>>.

³²Farmer, James Titcomb; Ben. "EU Deals Theresa May Encryption Setback as MEPs Propose Ban on Government Backdoors." *The Telegraph*. Telegraph Media Group, 16 June 2017. Web. 22 Aug. 2017. <<http://www.telegraph.co.uk/technology/2017/06/16/eu-deals-theresa-may-encryption-setback-meps-propose-ban-government/>>.

³³Farmer, James Titcomb; Ben. "EU Deals Theresa May Encryption Setback as MEPs Propose Ban on Government Backdoors." *The Telegraph*. Telegraph Media Group, 16 June 2017. Web. 22 Aug. 2017. <<http://www.telegraph.co.uk/technology/2017/06/16/eu-deals-theresa-may-encryption-setback-meps-propose-ban-government/>>.

³⁴Farmer, James Titcomb; Ben. "EU Deals Theresa May Encryption Setback as MEPs Propose Ban on Government Backdoors." *The Telegraph*. Telegraph Media Group, 16 June 2017. Web. 22 Aug. 2017. <<http://www.telegraph.co.uk/technology/2017/06/16/eu-deals-theresa-may-encryption-setback-meps-propose-ban-government/>>.

including the Federal Bureau of Investigation (FBI) and Amber Rudd herself, in order to prevent these attacks³⁵.

Due to this, people have become more and more concerned about their privacy. Apps are either encrypted or they are not. It is viewed that creating backdoors defeats the purpose of having encryption and if backdoors are created, criminals could take advantage of the weakened system and retrieve personal information on other users with ease³⁶. Rudd asserts that authorities “also need to have a system whereby when the police have an investigation, where the security services have put forward a warrant signed off by the home secretary, we can get that information when a terrorist is involved.”³⁷ Thus, the question of encryption and digital privacy is one that requires much thought and planning.

III. Key Vocabulary

Encryption: A way of transmitting a message so only the sender and receiver can access what was sent³⁸. If anyone other than these two key holders attempt to access the messages, a long string of numbers shall replace what was sent, making it almost impossible to get to the information being searched for.

Digital Privacy: “The right to privacy of users of digital media.”³⁹

Cryptography: “the enciphering and deciphering of messages in secret code or cipher.”⁴⁰ Encryption is a type of cryptography.⁴¹

³⁵“Center for Democracy & Technology.” *Issue Brief: A “Backdoor” to Encryption for Government Surveillance* | Center for Democracy & Technology. N.p., n.d. Web. 06 Oct. 2017.

<<https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/>>.

³⁶Haynes, Jonathan. “Backdoor Access to WhatsApp? Rudd’s Call Suggests a Hazy Grasp of Encryption.” *The Guardian*. Guardian News and Media, 27 Mar. 2017. Web. 22 Aug. 2017.

<<https://www.theguardian.com/technology/2017/mar/27/amber-rudd-call-backdoor-access-hazy-grasp-encryption>>.

³⁷Haynes, Jonathan. “Backdoor Access to WhatsApp? Rudd’s Call Suggests a Hazy Grasp of Encryption.” *The Guardian*. Guardian News and Media, 27 Mar. 2017. Web. 22 Aug. 2017.

<<https://www.theguardian.com/technology/2017/mar/27/amber-rudd-call-backdoor-access-hazy-grasp-encryption>>.

³⁸Murgia, Madhumita. “WhatsApp Adds End-to-end Encryption: What Is It and What Does It Mean for You?” *The Telegraph*. Telegraph Media Group, 05 Apr. 2016. Web. 22 Aug. 2017.

<<http://www.telegraph.co.uk/technology/2016/04/05/whatsapp-encryption-what-is-it-and-what-does-it-mean-for-you/>>.

³⁹“What Is Digital Privacy.” *IGI Global*. N.p., n.d. Web. 22 Aug. 2017.

<<http://www.igi-global.com/dictionary/digital-privacy/46799>>.

⁴⁰“Cryptography.” Merriam-Webster.com. Merriam-Webster, n.d. Web. 22 Aug. 2017.

<<https://www.merriam-webster.com/dictionary/cryptography>>.

⁴¹Forlanda, J. “What Is the Difference between Encryption and Cryptography?” *Bright Hub*. N.p., 26 May 2015.

Web. 22 Aug. 2017. <<http://www.brighthub.com/computing/enterprise-security/articles/65254.aspx>>.

Public Key: used to encrypt data using large numbers. Public key encryption is used for E2EE.⁴²

Internet Service Provider (ISP): “a company that provides its customers with access to the Internet and that may also provide other Internet-related services (such as e-mail accounts).”⁴³ ISPs are important in net neutrality and digital privacy.

Net Neutrality: (also referred to as open internet, or internet freedom) maintains the ability to be anywhere online at any time.⁴⁴ These rules are relevant to the discussion of digital privacy since it sets the premise of digital rights. “The essence of net neutrality is that ISPs cannot discriminate access or service based on preferences tied to payments.”⁴⁵

IV. Important Events & Chronology

| Date | Event |
|----------------|--|
| Late 1960s | Modern computer cryptography began being developed by Government Communications Headquarters (GCHQ) ⁴⁶ , the British intelligence organisation. It continues to be used today for means of securing transactions and messages that take place online. ⁴⁷ |
| December, 2013 | The United Nations expressed concern regarding negative impact on human rights as a result of surveillance and communication interception by adopting the General Assembly’s Resolution 68/167. ⁴⁸ |

⁴²Rouse, Margaret. "Public Key." *SearchSecurity*. TechTarget, Oct. 2006. Web. 22 Aug. 2017. <<http://searchsecurity.techtarget.com/definition/public-key>>.

⁴³ "Internet Service Provider." Merriam-Webster.com. Merriam-Webster, n.d. Web. 22 Aug. 2017. <<https://www.merriam-webster.com/dictionary/Internet%20service%20provider>>.

⁴⁴ United States of America. Federal Communications Commission. *The Open Internet*. Federal Communications Commission, n.d. Web. 22 Aug. 2017. <<https://www.fcc.gov/consumers/guides/open-internet>>.

⁴⁵ Andriole, Steve. "Net Neutrality And The Unfortunate Politics Of Digital." *Tech*. Forbes, 21 May 2017. Web. 22 Aug. 2017. <<https://www.forbes.com/sites/steveandriole/2017/03/21/net-neutrality-the-unfortunate-politics-of-digital/#ab057dd1b4eb>>.

⁴⁶ United Kingdom. Government Communications Headquarters. *Government Communications Headquarters*. Crown, n.d. Web. 22 Aug. 2017. <United Kingdom. Government Communications Headquarters. Government Communications Headquarters - GOV.UK. N.p., n.d. Web. 22 Aug. 2017. <<https://www.gov.uk/government/organisations/government-communications-headquarters>>.

⁴⁷ Titcomb, James. "What Is Encryption, How Does It Work and What Apps Use It?" *Technology*. The Telegraph, 29 Mar. 2017. Web. 22 Aug. 2017. <<http://www.telegraph.co.uk/technology/0/encryption-should-using/>>.

⁴⁸ "The Right to Privacy in the Digital Age." *Digital Age*. OHCHR, 13 Nov. 2014. Web. 22 Aug. 2017. <<http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>>.

| | |
|----------------|---|
| November, 2014 | WhatsApp became end-to-end encrypted, making WhatsApp one of the most secure networks and sparking major controversy about privacy and how much access should be given to authorities. ⁴⁹ |
| March 28, 2017 | US congress passed bill to repeal privacy regulations that protected users by requiring their consent to share personal data. Internet providers are now free to sell such data to advertisers. ⁵⁰ |

V. Past Resolutions and Treaties

Universal Declaration of Human Rights⁵¹

Announced on December 10, 1948⁵², the Universal Declaration of Human Rights (UDHR) is one of the biggest milestones in the history of human rights. It consists of the basic and essential standards for people in all countries. The declaration was drafted by many countries from all over the globe and included representatives from Australia, China, France, Chile, Lebanon, and the United States⁵³. Article 12 of the declaration states 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.”⁵⁴

Breaking or creating backdoors for encryption has been viewed as an attack on people’s privacy and this article, although not legally binding, recognizes privacy as a right. David Kaye, the Special Rapporteur on freedom of opinion and expression, has voiced that “Laws, practices and policies that ban, restrict, or otherwise undermine encryption and anonymity – all in the name of public order or counter-terrorism – do significant, and I would say disproportionate, damage to

⁴⁹ Murgia, Madhumita. "WhatsApp Adds End-to-end Encryption: What Is It and What Does It Mean for You?" *The Telegraph*. Telegraph Media Group, 05 Apr. 2016. Web. 22 Aug. 2017.
<<http://www.telegraph.co.uk/technology/2016/04/05/whatsapp-encryption-what-is-it-and-what-does-it-mean-for-you/>>.

⁵⁰ Hatmaker, Taylor. "Congress Just Voted to Let Internet Providers Sell Your Browsing history." *TechCrunch*. TechCrunch, 28 Mar. 2017. Web. 22 Aug. 2017.
<<https://techcrunch.com/2017/03/28/house-vote-sj-34-isp-regulations-fcc/>>.

⁵¹ "Universal Declaration of Human Rights." *United Nations*. United Nations, n.d. Web. 22 Aug. 2017.
<<http://www.un.org/en/universal-declaration-human-rights/>>.

⁵² "Universal Declaration of Human Rights." *United Nations*. United Nations, n.d. Web. 22 Aug. 2017.
<<http://www.un.org/en/universal-declaration-human-rights/>>.

⁵³ "Human Rights." *United Nations*. United Nations, n.d. Web. 22 Aug. 2017.
<<http://research.un.org/en/undhr/draftingcommittee>>.

⁵⁴ "Universal Declaration of Human Rights." *United Nations*. United Nations, n.d. Web. 22 Aug. 2017.
<<http://www.un.org/en/universal-declaration-human-rights/>>.

the rights at the heart of my mandate.”⁵⁵ Plainly, the declaration has relevance to the topic at hand and must be considered when creating and drafting resolutions for this issue in the future.

[General Assembly resolution A/HRC/33/L.6](#)⁵⁶

The General Assembly has passed a plethora of resolutions on many different topics throughout the years. One of the resolutions that have relevance to the case being discussed is resolution A/HRC/33/L.6, the safety of journalists⁵⁷. This resolution has been drafted by many states including Austria, Belgium, France, Germany, Switzerland, and the United States⁵⁸. This resolution goes on to recognize that encryption and anonymity are a large part of today’s world, especially for journalists, who depend on the existence and usage of encryption and anonymity. The resolution discusses how encryption help journalists exercise their freedom of privacy and to express themselves freely. This can be seen in clause 13 of the resolution:

“13. Emphasizes that, in the digital age, encryption and anonymity tools have become vital for many journalists to exercise freely 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, with any restrictions thereon complying with States’ obligations under international human rights law;”⁵⁹

Although this resolution targets journalists, there are many jobs that can relate and depend on the usage of encryption. The Special Rapporteur on freedom of opinion and expression, David Kaye, has pointed out “that encryption and anonymity tools have become vital for journalists, activists, artists, academics and others to exercise their professions and their

⁵⁵ "Human Rights, Encryption and Anonymity in a Digital Age." *OHCHR*. N.p., n.d. Web. 22 Aug. 2017. <<http://www.ohchr.org/en/NewsEvents/Pages/NewsSearch.aspx>>.

⁵⁶ *The Safety of Journalists* (2016): 1-6. *United Nations*. United Nations, 26 Sept. 2016. Web. 22 Aug. 2017. <https://cpj.org/Safety_of_Journalists%20resolution.pdf>.

⁵⁷ *The Safety of Journalists* (2016): 1-6. *United Nations*. United Nations, 26 Sept. 2016. Web. 22 Aug. 2017. <https://cpj.org/Safety_of_Journalists%20resolution.pdf>.

⁵⁸ *The Safety of Journalists* (2016): 1-6. *United Nations*. United Nations, 26 Sept. 2016. Web. 22 Aug. 2017. <https://cpj.org/Safety_of_Journalists%20resolution.pdf>.

⁵⁹ *The Safety of Journalists* (2016): 1-6. *United Nations*. United Nations, 26 Sept. 2016. Web. 22 Aug. 2017. <https://cpj.org/Safety_of_Journalists%20resolution.pdf>.

human rights freely.”⁶⁰ Even lawyers depend on encryption in order to prevent losing client confidentiality⁶¹.

VI. Failed Solution Attempts

The issues relating to encryption and digital privacy are relatively new, yet some of the proposed solutions have not succeeded in solving the matter at hand. For example, creating backdoors for encrypted apps has obviously been met with both negative criticism and with supportive remarks. This is due to the fact that people view encryption as being two sided, an app is either encrypted or it isn't. Many people support the creation of keys for encryption, while others do not. Creating keys for the authorities such as the FBI leaves people with feelings of loss of privacy. Not only that, but it increases the chances of criminals to access private information due to the existence of these keys and backdoors. Another solution attempt was to break encryption completely yet that was seen as being a “grave security risk” by cryptologists⁶² since the once private information locked safely in apps such as WhatsApp will now become accessible to the public, especially criminals. These apps are successful for their use of encryption, so by getting rid of encryption and privacy, these apps become redundant since no personal information can be safely stored there without there being a possibility of the information being accessed. Clearly, the issues surrounding this topic are ones that aren't solved simply.

VII. Possible Solutions

- Creating heavily guarded backdoors for encrypted apps.
- The creation of a protocol for authority such as the FBI following a terrorist attack in order to obtain any encrypted information.
- Government transparency for the public's security and knowledge of what their personal information and online history is being used for.
- Establishing digital security hubs for the provision of digital security training, as well as advice or support on technical issues .
- Raising awareness on digital rights and security so that the people can be reassured of what is expected of the applications, websites, and servers they use and the rights they are entitled to.

⁶⁰ "Human Rights, Encryption and Anonymity in a Digital Age." *OHCHR*. N.p., n.d. Web. 22 Aug. 2017. <<http://www.ohchr.org/en/NewsEvents/Pages/NewsSearch.aspx>>.

⁶¹ McIntyre, Niamh. "Government Vows Cyber Encryption Crackdown after Manchester Suicide Bombing." *The Independent*. Independent Digital News and Media, 26 May 2017. Web. 22 Aug. 2017. <<http://www.independent.co.uk/news/uk/home-news/government-cyber-encryption-crackdown-manchester-suicide-bombing-attack-facebook-social-media-a7756666.html>>.

⁶² Kerry, Cameron F. "The Backdoor Threat to Encryption." *Brookings*. Brookings, 29 July 2016. Web. 06 Oct. 2017. <<https://www.brookings.edu/blog/techtank/2015/10/12/the-backdoor-threat-to-encryption/>>.

VIII. Useful Links

What is End-To-End Encryption?

Explains what encryption is, the difference between symmetric and asymmetric encryption, in addition to E2EE and how to use it.

Unuth, Nadeem. "What Is End-to-End Encryption?" *Lifewire*. N.p., 31 May 2017. Web. 22 Aug. 2017. <<https://www.lifewire.com/what-is-end-to-end-encryption-4028873>>.

WhatsApp and End-to-End Encryption: Here's Everything You Need to Know

An article about E2EE regarding whatsapp specifically, why it has it, what the protocol is, the topic of backdoor entry (even for governments), dealing with law enforcements, and such.

Dhapola, Shruti. "WhatsApp and End-to-end Encryption: Here's Everything You Need to Know." *Indian Express*. WordPress, 22 Aug. 2017. Web. 22 Aug. 2017. <<http://indianexpress.com/article/technology/social/whatsapp-and-its-end-to-end-encryption-everything-you-ever-wanted-to-know-4807191/>>.

Is Digital Privacy A Right Or A Privilege?

A brief account on current day digital privacy being dealt with as a privilege.

Andriole, Steve. "Is Digital Privacy A Right Or A Privilege?" *Tech. Forbes*, 7 Apr. 2017. Web. 22 Aug. 2017. <<https://www.forbes.com/sites/steveandriole/2017/04/07/is-digital-privacy-a-right-or-a-privilege/#30c5da8b48cf>>.

Congress Just Voted to Let Internet Providers Sell Your Browsing History

Discusses the bill passed by the US congress mentioned in section "IV. Important Events and Chronology" of the chair report.

Hatmaker, Taylor. "Congress Just Voted to Let Internet Providers Sell Your Browsing history." *TechCrunch*. TechCrunch, 28 Mar. 2017. Web. 22 Aug. 2017. <<https://techcrunch.com/2017/03/28/house-vote-sj-34-isp-regulations-fcc/>>.

These 5 Countries Were Ranked Best for Privacy (Infographic)

Gives insight on digital privacy of numerous countries such as Malaysia, Syria, Nigeria, Iran, Bahrain, China, and the United States.

Kelly, Meghan. "These 5 Countries Were Ranked Best for Privacy (infographic)." *VentureBeat*. BackgroundChecks, 13 Oct. 2013. Web. 22 Aug. 2017. <<https://venturebeat.com/2013/10/13/countries-privacy/>>.

Report on Encryption, Anonymity, and the Human Rights Framework

Includes government policies and positions of countries such as Cuba, Germany, Greece, Guatemala, Lebanon, Qatar, Sweden, Turkey, and the US.

"Report on Encryption, Anonymity, and the Human Rights Framework." *United Nations Human Rights Office of the High Commissioner*. OHCHR, n.d. Web. 22 Aug. 2017. <<http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx>>.

IX. Works Cited

Andriole, Steve. "Is Digital Privacy A Right Or A Privilege?" *Forbes*. Forbes Magazine, 07 Apr. 2017.

Web. 22 Aug. 2017.

<<https://www.forbes.com/sites/steveandriole/2017/04/07/is-digital-privacy-a-right-or-a-privilege/>>.

Andriole, Steve. "Net Neutrality And The Unfortunate Politics Of Digital." *Tech*. Forbes, 21 May 2017.

Web. 22 Aug. 2017.

<<https://www.forbes.com/sites/steveandriole/2017/03/21/net-neutrality-the-unfortunate-politics-of-digital/#ab057dd1b4eb>>.

Botelho, Greg. "San Bernardino Attack Investigated as Act of Terrorism." *CNN*. Cable News Network, 05

Dec. 2015. Web. 06 Oct. 2017.

<<http://edition.cnn.com/2015/12/04/us/san-bernardino-shooting/index.html>>.

Clark, Bryan. *How Does Encryption Work, and Is It Really Safe?* Digital image. *MakeUseOf*. N.p., 09 Mar. 2015. Web. 22 Aug. 2017. <<http://www.makeuseof.com/tag/encryption-care/>>.

"Center for Democracy & Technology." *Issue Brief: A "Backdoor" to Encryption for Government Surveillance* | *Center for Democracy & Technology*. N.p., n.d. Web. 06 Oct. 2017. <<https://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/>>.

"Cryptography." Merriam-Webster.com. Merriam-Webster, n.d. Web. 22 Aug. 2017. <<https://www.merriam-webster.com/dictionary/cryptography>>.

"Digital Privacy to Come Under Supreme Court's Scrutiny." *The New York Times*. The New York Times, 10 July 2017. Web. 22 Aug. 2017. <<https://www.nytimes.com/2017/07/10/business/dealbook/digital-privacy-supreme-court.html>>.

"Digital Rights in Malaysia." *Digital Rights in Malaysia — English*. Sinar Project, 04 Nov. 2015. Web. 22 Aug. 2017. <<https://sinarproject.org/en/updates/digital-rights-in-malaysia>>.

Emily Allen; Barney Henderson. "Westminster Attack: Everything We Know so Far about the Events in London." *The Telegraph*. Telegraph Media Group, 22 Mar. 2017. Web. 22 Aug. 2017. <<http://www.telegraph.co.uk/news/2017/03/22/westminster-terror-attack-everything-know-far/>>.

"Encrypt." Merriam-Webster.com. Merriam-Webster, n.d. Web. 22 Aug. 2017. <<https://www.merriam-webster.com/dictionary/encrypt>>.

Farmer, James Titcomb; Ben. "EU Deals Theresa May Encryption Setback as MEPs Propose Ban on Government Backdoors." *The Telegraph*. Telegraph Media Group, 16 June 2017. Web. 22 Aug. 2017. <<http://>

www.telegraph.co.uk/technology/2017/06/16/eu-deals-theresa-may-encryption-setback-meps-propos-e-ban-government/>.

Forlanda, J. "What Is the Difference between Encryption and Cryptography?" *Bright Hub*. N.p., 26 May 2015. Web. 22 Aug. 2017.

<<http://www.brighthub.com/computing/enterprise-security/articles/65254.aspx>>.

Gore, Will. "Amber Rudd's Call to End WhatsApp Encryption Is Incredibly Naïve." *The Independent*. Independent Digital News and Media, 27 Mar. 2017. Web. 22 Aug. 2017.

<<http://www.independent.co.uk/voices/whatsapp-amber-rudd-khalid-masood-terrorism-niave-a7652806.html>>.

Greenberg, Andy. "Hacker Lexicon: What Is End-to-End Encryption?" *Wired*. Conde Nast, 02 June 2017.

Web. 22 Aug. 2017. <<https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/>>.

Haynes, Jonathan. "Backdoor Access to WhatsApp? Rudd's Call Suggests a Hazy Grasp of Encryption." *The Guardian*. Guardian News and Media, 27 Mar. 2017. Web. 22 Aug. 2017.

<<https://www.theguardian.com/technology/2017/mar/27/amber-rudd-call-backdoor-access-hazy-grasp-encryption>>.

"History of Encryption." *SANS Institute InfoSec Reading Room*. N.p., 2001. Web. 22 Aug. 2017.

<<https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730>>.

"Human Rights, Encryption and Anonymity in a Digital Age." *OHCHR*. N.p., n.d. Web. 22 Aug. 2017.

<<http://www.ohchr.org/en/NewsEvents/Pages/NewsSearch.aspx>>.

"Human Rights." *United Nations*. United Nations, n.d. Web. 22 Aug. 2017.

<<http://research.un.org/en/undhr/draftingcommittee>>.

"Internet Service Provider." Merriam-Webster.com. Merriam-Webster, n.d. Web. 22 Aug. 2017.

<<https://www.merriam-webster.com/dictionary/Internet%20service%20provider>>.

Kerry, Cameron F. "The Backdoor Threat to Encryption." *Brookings*. Brookings, 29 July 2016. Web. 06 Oct. 2017.

<<https://www.brookings.edu/blog/techtank/2015/10/12/the-backdoor-threat-to-encryption/>>.

Lomas, Natasha. "We Want to Limit Use of E2e Encryption, Confirms UK minister." *TechCrunch*. TechCrunch, 05 June 2017. Web. 22 Aug. 2017.

<<https://techcrunch.com/2017/06/05/we-want-to-limit-use-of-e2e-encryption-confirms-uk-minister/>>

McIntyre, Niamh. "Government Vows Cyber Encryption Crackdown after Manchester Suicide Bombing." *The Independent*. Independent Digital News and Media, 26 May 2017. Web. 22 Aug. 2017. <[http://](http://www.independent.co.uk/news/uk/home-news/government-cyber-encryption-crackdown-manchester-suicide-bombing-attack-facebook-social-media-a7756666.html)

www.independent.co.uk/news/uk/home-news/government-cyber-encryption-crackdown-manchester-suicide-bombing-attack-facebook-social-media-a7756666.html>.

Murgia, Madhumita. "WhatsApp Adds End-to-end Encryption: What Is It and What Does It Mean for You?" *The Telegraph*. Telegraph Media Group, 05 Apr. 2016. Web. 22 Aug. 2017.

<<http://www.telegraph.co.uk/technology/2016/04/05/whatsapp-encryption-what-is-it-and-what-does-it-mean-for-you/>>.

"Our Mission." *About Us*. Access Now, n.d. Web. 22 Aug. 2017.

<<https://www.accessnow.org/about-us/>>.

"Privacy International." *Privacy International*. Privacy International, n.d. Web. 22 Aug. 2017.

<<https://www.privacyinternational.org/>>.

"Privacy International." *What We Do*. Privacy International, n.d. Web. 22 Aug. 2017.

<<https://www.privacyinternational.org/projects>>.

"Privacy Rights, Data Protection, Security in Malaysia." *KASS*. KASS International, n.d. Web. 22 Aug. 2017. <<http://www.kass.com.my/data-protection/>>.

Rouse, Margaret, and Madelyn Bacon. "What Is End-to-end Encryption (E2EE)? - Definition from WhatIs.com." *SearchSecurity*. TechTarget, July 2015. Web. 22 Aug. 2017. <<http://searchsecurity.techtarget.com/definition/end-to-end-encryption-E2EE>>.

Rouse, Margaret. "Public Key." *SearchSecurity*. TechTarget, Oct. 2006. Web. 22 Aug. 2017. <<http://searchsecurity.techtarget.com/definition/public-key>>.

Sharwood, APAC Editor 14 Jul 2017 at 01:49 Tweet_btn(), Simon. "UK Spookhaus GCHQ Can Crack End-to-end Encryption, Claims Australian A-G." *The Register*. Situation, 14 July 2017. Web. 22 Aug. 2017. <https://www.theregister.co.uk/2017/07/14/uk_spookhas_gchq_can_crack_endtoend_encryption_says_australian_ag/>.

Sulleyman, Aatif. "UK Government Is Secretly Planning to Break Encryption and Spy on People's Phones, Reveals Leaked Document." *The Independent*. Independent Digital News and Media, 05 May 2017. Web. 22 Aug. 2017. <<http://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-security-services-phones-spy-break-encryption-gchq-mi5-technical-advisory-board-bskyb-bt-cable-a7719341.html>>.

"The Right to Privacy in the Digital Age." *Digital Age*. OHCHR, 13 Nov. 2014. Web. 22 Aug. 2017. <<http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>>.

The Safety of Journalists (2016): 1-6. *United Nations*. United Nations, 26 Sept. 2016. Web. 22 Aug. 2017. <https://cpj.org/Safety_of_Journalists%20resolution.pdf>.

Titcomb, James. "What Is Encryption, How Does It Work and What Apps Use It?" *Technology*. The Telegraph, 29 Mar. 2017. Web. 22 Aug. 2017.

<<http://www.telegraph.co.uk/technology/0/encryption-should-using/>>.

United Kingdom. Government Communications Headquarters. *Government Communications Headquarters*. Crown, n.d. Web. 22 Aug. 2017. <United Kingdom. Government Communications Headquarters. Government Communications Headquarters - GOV.UK. N.p., n.d. Web. 22 Aug. 2017. <<https://www.gov.uk/government/organisations/government-communications-headquarters/>>.

United States of America. Federal Communications Commission. *The Open Internet*. Federal Communications Commission, n.d. Web. 22 Aug. 2017.

<<https://www.fcc.gov/consumers/guides/open-internet/>>.

"Universal Declaration of Human Rights." *United Nations*. United Nations, n.d. Web. 22 Aug. 2017.

<<http://www.un.org/en/universal-declaration-human-rights/>>.

"What Is Digital Privacy." *IGI Global*. IGI Global, n.d. Web. 22 Aug. 2017.

<<https://www.igi-global.com/dictionary/digital-privacy/46799/>>.

"WhatsApp Security." *WhatsApp*. N.p., n.d. Web. 22 Aug. 2017. <<https://www.whatsapp.com/security/>>.

Yadron, Danny. "FBI Confirms It Won't Tell Apple How It Hacked San Bernardino Shooter's iPhone."

The Guardian. Guardian News and Media, 28 Apr. 2016. Web. 22 Aug. 2017.

<<https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino>>.

Yadron, Danny, Spencer Ackerman, and Sam Thielman. "Inside the FBI's Encryption Battle with Apple."

The Guardian. Guardian News and Media, 18 Feb. 2016. Web. 22 Aug. 2017.

<<https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple>>.