Personal Information

I am Jay Hunter, student number S3855709, I am 22-years old working as a Pharmacy Assistant in Brisbane. In my free time I enjoy reading articles on medical technology and computer engineering, reading books on history and philosophy, and playing guitar. Next year, I will be studying Computer Engineering at the University of Queensland majoring in Image and Pattern Recognition and High-Performance Computing. Currently I have no professional experience in IT, only enthusiast projects and research.

Team Profile

Jay’s three tests were *Myers-Briggs*, *Learning Type*, and a *Career Aptitude* test which categorised him as ENFP, a Visual Learner, and the following careers: Remote Sensing Technician, Timing Device Assembler and Adjuster, Computer-Controlled Machine Tool Operator. Using this information, Jay can communicate effectively with the group and work on any task given without dissent. Being a visual learner, he may be able to provide useful graphics or styling ideas for the group.

IT Technologies: Cyber Security

What does it do?

One of the main focuses of Cyber Security is Encryption. This is the process of taking ‘plain text’ a file anyone can easily access and open and converting it to ‘cipher text’ through an Encryption Algorithm (Norton, 2020). ‘Cipher text’ cannot be easily accessed or opened due to the file being ‘scrambled’ by the encryption algorithm, only users with a ‘key’ can ‘unscramble’ or ‘decrypt’ the file and access its contents (Mercer-Myers, 2018). There are two main categories or encryption device encryption and end-to-end Encryption.

End-to-end encryption is used to secure connect two devices. This could be messages, credit card payments, or visiting a website. There are two main types of handling end-to-end encryption: symmetric and asymmetric encryption. Symmetric encryption uses one key for both encrypting and decrypting data. This allows for multiple people to easily access the data that’s encrypted. This method the data is only as safe as the most careless person with a key (Norton, 2020).

Asymmetric encrypted uses two keys. One is a public key which is shared and can encrypt data, and the other is a private key which decrypts data. End-to-end encryption often utilises asymmetric encryption (Mercer-Myers, 2018). This is often seen in the use of HTTPS as explained by CloudFlare, “A client will obtain a website's public key from that website's TLS certificate (or SSL certificate) and use that to initiate secure communication,” by initiating the connection with the public key, the user accessing the website is able to encrypt their traffic and only they can decrypt the information they receive (CloudFare, 2020) (Electronic Frontier Foundation, 2020). Mobile apps such as WhatsApp, Signal, and mobile banking apps also use asymmetric encryption for secure connection (WhatsApp, 2020) (Signal, 2020) (Weil, 2018). In 2017, International Business Machines (IBM) unveiled a line of mainframe computers which focused on encryption. These mainframes ‘IBM Z’ were targeted towards banking and insurance companies encrypting incoming and outgoing connections and the servers themselves through both peer-to-peer and device encryption (Greenwald, 2017). [Elaborate on why this is important]

Device encryption is where the entire device or its storage is encrypted, often through symmetric encryption. This protects the owners’ files if their phone or laptop is stolen, it can also protect businesses and government agencies from local hackers trying to access sensitive information. SSD manufacture’s such as Intel and Samsung include built-in encryption to their storage (Intel, 2020) (Samsung, 2020). Apple has gained a reputation for their iPhones innovation in biometric keys (using finger-prints or face scans as keys) and their devices impenetrability as shown in their 2016 legal dispute with the FBI (The Wallstreet Journal Editorial Board, 2020) (Yadron, et al., 2016) (Wallstreet Journal Editorial Board, 2016) (Mossberg, 2013) (Mickle & McMillan, 2017). The importance of device encryption is emphasised by Bruce Schneier, board member of the EFF, in his blog, “we only use encryption when we're working with important data, then encryption signals that data's importance” (Schneier, 2019).

In 2018, Steve Rosenbush wrote ‘Why Encryption of Corporate Data Remains a Powerful but Underutilized Tool,’ in *The Wallstreet Journal*, two years later following the Covid-19 Pandemic *Zoom* has been banned by *Tesla*, *Google*, and New York City Schools because of the lack of P2P Encryption and security concerns with China (Rosenbush, 2018) (Langley, 2020) (Wood, 2020) (Whittaker, 2020). Despite Zoom’s CEO Eric Yuan publicly apologising for misleading marketing of end-to-end encryption and having the company focus on creating end-to-end encryption, their public image has been tarnished (Tilley & McMillan, 2020) (Lee & Grauer, 2020) (Whittaker, 2020) (Whittaker, 2020). This is furthered by instances of ‘zoombombing’ where pranksters interrupt many types of group calls including Alcoholics Anonymous, classes, and, children’s birthday parties (Bindley, 2020) (Nguyen, 2020) (Hern, 2020). The backlash that Zoom has faced shows that businesses are understanding the importance of Cyber Security, namely encryption, for the protection of sensitive data and communication (Whittaker, 2020). What standards should these businesses follow?

Government agencies such as the American Department of Commerce’s *National Institute of Standards and Technology* (NIST) work with other government agencies and the private sector to develop standards for encryption (Chen, 2019). In 1977, the U.S. government created the Data Encryption Standard (DES). In 1985, Triple-DES became an academic community standard to replace DES, as it became clear that DES could be ‘brute forced.’ Brute forcing is when a machine or program can decrypt the encryption. NIST decided to back Belgian algorithm, Rijindael, which became the Advanced Encryption Standard (AES) in 1997 (Schneier, 2004). This continues to be the standard to this day. As technology improves rapidly it will become obsolete, and government departments and private companies understand this. Similar to the Space Race, the U.S. and China are racing to the create better technology then the other, with cyber security in the centre of this (Fitch & Woo, 2020) (Strong, 2018) (Mims, 2019) (Castellanos, 2017).

The next critical step for encryption is developing a ‘quantum proof’ encryption algorithm. IBM, Cisco, and Google alongside dozens of companies currently working on this technology (Mann, 2013) (Hackett, 2019) (Porter, 2019) (Metz, 2019) (Vincent, 2019) (Hartnett, 2019) (Bryson, 2019) (Castellanos, 2018). When talking to the Wallstreet Journal, for NSA Director Michael Hayden stated, “I don't know whether quantum computing will inherently favor the offense or inherently favor the defense, when it comes to encryption, security, espionage and so on, but I do know it's going to affect something.” This was in discussion of current encryption methods and future issues cyber security faces (Strong, 2018). Whether quantum cryptography is developed in three or ten years is uncertain. What is, however, the standards that come from this technology will change and develop over time. *Data Encryption Standard* became *Advanced Encryption Standard* and today there are a plethora of encryption standards. *Quantum Encryption Standard* will be that next step. But as technology evolves, so does legislation.

What is the likely impact?

Beginning in 1946, the UKUSA agreement began an intelligence co-operation with the United Kingdom and the United States. Nine years later, in 1955, the agreement was updated to include Canada, Australia, and New Zealand (Farrell, 2013) (National Security Agency, 2020). Colloquially, this alliance is known as the ‘Five Eyes.’ Together, they develop new intelligence methods and data retention legislation. It has later been uncovered that this extends to a further nine countries in an alliance known as SIGINT Seniors Europe (SSEUR) or the ‘Fourteen Eyes.’ This extension shares intel only (Taylor, 2020) (Kelion, 2014) (Gallagher, 2018) (Koch, 2018). As part of the core ‘Five Eyes’ both the Australian and American governments and security officials have pushed both to ban individuals and force companies to introduce ‘backdoors’ into their security systems. Groups like the Electronic Frontiers Foundation (EFF) and companies such as Apple and Google have pushed back on this (Ruiz, 2018) (Mullin, 2020) (Karp, 2018) (Whittaker, 2018). Apple, as previously mentioned, had fought against the FBI in 2016 and creating a backdoor for their line of iPhones (Wallstreet Journal Editorial Board, 2016). Both American government officials and law enforcement had framed the issues to be against terrorism, Apple knew that the matter would leave precedent and be abused for minor crimes too. The repercussions of doing so would give both Russia and China power over the company to give them backdoors or they would find the any that were created.

Foreign agencies being able to hack and track unwitting citizens is not the goal of this legislation; it is for domestic agencies to. But given that ability, cyber-attacks and crimes would become far easier for bad actors actively looking for vulnerabilities.

<https://www.forbes.com/sites/jasonbrett/2020/04/10/how-working-remote-and-protecting-encryption-is-natural-for-this-blockchain-company/#219dafdc3771>

<https://www.eff.org/deeplinks/2020/03/earn-it-bill-governments-not-so-secret-plan-scan-every-message-online>

<https://www.bbc.com/news/world-australia-46463029>

<https://www.wired.com/story/australia-encryption-law-global-impact/>

How will this affect you? (300 words)

# Bibliography

Bindley, K., 2020. *Zoombombing Harms the Alcoholics Anonymous Community.* [Online]   
Available at: https://www.wsj.com/articles/zoombombing-harms-the-alcoholics-anonymous-community-11586091602

Brett, J., 2020. *How Working Remote And Protecting Encryption Is Natural For This Blockchain Company.* [Online]   
Available at: https://www.forbes.com/sites/jasonbrett/2020/04/10/how-working-remote-and-protecting-encryption-is-natural-for-this-blockchain-company/#219dafdc3771

Bryson, S., 2019. *Is quantum computing technology around the corner?.* [Online]   
Available at: https://www.cisco.com/c/en/us/solutions/enterprise-networks/quantum-computing-technology.html

Castellanos, S., 2017. *Crypto Researchers Brace For Quantum Computing’s Threat To Security.* [Online]   
Available at: https://blogs.wsj.com/cio/2017/08/07/crypto-researchers-brace-for-quantum-computings-threat-to-security/

Castellanos, S., 2018. *Cisco, Researchers Develop New Security Techniques to Thwart Quantum Attacks.* [Online]   
Available at: https://blogs.wsj.com/cio/2018/04/11/cisco-researchers-develop-new-security-techniques-to-thwart-quantum-attacks/

Chen, L., 2019. *Cryptographic Standards and Guidelines.* [Online]   
Available at: https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development

CloudFare, 2020. *What Is Asymmetric Encryption?.* [Online]   
Available at: https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/

Electronic Frontier Foundation, 2020. *Encrypting the Web.* [Online]   
Available at: https://www.eff.org/encrypt-the-web

Farrell, P., 2013. *History of 5-Eyes – explainer.* [Online]   
Available at: https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer

Fitch, A. & Woo, S., 2020. *The U.S. vs. China: Who Is Winning the Key Technology Battles?.* [Online]   
Available at: https://www.wsj.com/articles/the-u-s-vs-china-who-is-winning-the-key-technology-battles-11586548597?mod=djemCIO

Gallagher, R., 2018. *The Powerful Global Spy Alliance You Never Knew Existed.* [Online]   
Available at: https://theintercept.com/2018/03/01/nsa-global-surveillance-sigint-seniors/

Greenwald, T., 2017. *IBM’s Latest Line of Mainframe Computers Focuses on Encryption.* [Online]   
Available at: https://www.wsj.com/articles/ibms-latest-line-of-mainframe-computers-focuses-on-encryption-1500264061

Hackett, R., 2019. *Google Claims ‘Quantum Supremacy,’ Marking a Major Milestone in Computing.* [Online]   
Available at: https://fortune.com/2019/09/20/google-claims-quantum-supremacy/

Hartnett, K., 2019. *Google and IBM Clash Over Milestone Quantum Computing Experiment.* [Online]   
Available at: https://www.quantamagazine.org/google-and-ibm-clash-over-quantum-supremacy-claim-20191023/

Hern, A., 2020. *Trolls exploit Zoom privacy settings as app gains popularity.* [Online]   
Available at: https://www.theguardian.com/technology/2020/mar/27/trolls-zoom-privacy-settings-covid-19-lockdown

Intel, 2020. *Intel® Optane™ SSD 905P Series.* [Online]   
Available at: https://www.intel.com/content/www/us/en/products/memory-storage/solid-state-drives/consumer-ssds/optane-ssd-9-series/optane-ssd-905p-series/905p-380gb-m-2-110mm-20nm.html

Karp, P., 2018. *Australia's war on encryption: the sweeping new powers rushed into law.* [Online]   
Available at: https://www.theguardian.com/technology/2018/dec/08/australias-war-on-encryption-the-sweeping-new-powers-rushed-into-law

Kelion, L., 2014. *NSA-GCHQ Snowden leaks: A glossary of the key terms.* [Online]   
Available at: https://www.bbc.com/news/technology-25085592

Koch, R., 2018. *What countries are in the 5 Eyes, 9 Eyes, and 14 Eyes agreements?.* [Online]   
Available at: https://protonvpn.com/blog/5-eyes-global-surveillance/

Langley, H., 2020. *Google has banned the Zoom app from all employee computers over 'security vulnerabilities'.* [Online]   
Available at: https://www.businessinsider.com.au/google-bans-zoom-from-employee-computers-due-to-security-concerns-2020-4?r=US&IR=T

Lee, M. & Grauer, Y., 2020. *Zoom Meetings Aren’t End-to-End Encrypted, Despite Misleading Marketing.* [Online]   
Available at: https://theintercept.com/2020/03/31/zoom-meeting-encryption/

Mann, A., 2013. *Laws of Physics Say Quantum Cryptography Is Unhackable. It's Not.* [Online]   
Available at: https://www.wired.com/2013/06/quantum-cryptography-hack/

Mercer-Myers, C., 2018. *What is encryption?.* [Online]   
Available at: https://www.techworld.com/security/what-is-encryption-3659671/

Metz, C., 2019. *Google Claims a Quantum Breakthrough That Could Change Computing.* [Online]   
Available at: https://www.nytimes.com/2019/10/23/technology/quantum-computing-google.html

Mickle, T. & McMillan, R., 2017. *Can Apple Unlock Promise of Facial Recognition?.* [Online]   
Available at: https://www.wsj.com/articles/can-apple-unlock-promise-of-facial-recognition-1505320165

Mims, C., 2019. *The Day When Computers Can Break All Encryption Is Coming.* [Online]   
Available at: https://www.wsj.com/articles/the-race-to-save-encryption-11559646737

Mossberg, W. S., 2013. *A New Touch for iPhone.* [Online]   
Available at: https://www.wsj.com/articles/a-new-touch-for-iphone-1379466195

Mullin, J., 2020. *The Graham-Blumenthal Bill: A New Path for DOJ to Finally Break Encryption.* [Online]   
Available at: https://www.eff.org/deeplinks/2020/03/graham-blumenthal-bill-new-path-doj-finally-break-encryption

National Security Agency, 2020. *UKUSA Agreement Release.* [Online]   
Available at: https://www.nsa.gov/news-features/declassified-documents/ukusa/

Nguyen, N., 2020. *Don’t Get Bombed: How to Host Zoom Meetings, Hangouts, Houseparty and More.* [Online]   
Available at: https://www.wsj.com/articles/dont-get-bombed-how-to-host-zoom-meetings-hangouts-houseparty-and-more-11585819821?mod=cxrecs\_join

Norton, 2020. *What is encryption and how does it protect your data?.* [Online]   
Available at: https://us.norton.com/internetsecurity-privacy-what-is-encryption.html

Porter, J., 2019. *Google may have just ushered in an era of ‘quantum supremacy’.* [Online]   
Available at: https://www.theverge.com/2019/9/23/20879485/google-quantum-supremacy-qubits-nasa

Rosenbush, S., 2018. *Why Encryption of Corporate Data Remains a Powerful but Underutilized Tool.* [Online]   
Available at: https://blogs.wsj.com/cio/2018/05/30/the-morning-download-why-encryption-of-corporate-data-remains-a-powerful-but-underutilized-tool/

Ruiz, D., 2018. *There is No Middle Ground on Encryption.* [Online]   
Available at: https://www.eff.org/deeplinks/2018/05/there-no-middle-ground-encryption

Samsung, 2020. *SSD 970 PRO.* [Online]   
Available at: https://www.samsung.com/semiconductor/minisite/ssd/product/consumer/970pro/

Schneier, B., 2004. *The Legacy of DES.* [Online]   
Available at: https://www.schneier.com/blog/archives/2004/10/the\_legacy\_of\_d.html

Schneier, B., 2019. *Why We Encrypt.* [Online]   
Available at: https://www.schneier.com/blog/archives/2015/06/why\_we\_encrypt.html

Signal, 2020. *Technical Information.* [Online]   
Available at: https://www.signal.org/docs/

Strong, J., 2018. *Quantum Computing Will Reshape Digital Battlefield, Says Former NSA Director Hayden.* [Online]   
Available at: https://blogs.wsj.com/cio/2018/06/27/quantum-computing-will-reshape-digital-battlefield-says-former-nsa-director-hayden/

Taylor, S., 2020. *Five Eyes, Nine Eyes, 14 Eyes – Explained.* [Online]   
Available at: https://restoreprivacy.com/5-eyes-9-eyes-14-eyes/

The Wallstreet Journal Editorial Board, 2020. *The Case of Bill Barr vs. Apple.* [Online]   
Available at: https://www.wsj.com/articles/the-case-of-bill-barr-vs-apple-11579047641

Tilley, A. & McMillan, R., 2020. *Zoom CEO: ‘I Really Messed Up’ on Security as Coronavirus Drove Video Tool’s Appeal.* [Online]   
Available at: https://www.wsj.com/articles/zoom-ceo-i-really-messed-up-on-security-as-coronavirus-drove-video-tools-appeal-11586031129

Vincent, J., 2019. *IBM’s new quantum computer is a symbol, not a breakthrough.* [Online]   
Available at: https://www.theverge.com/2019/1/8/18171732/ibm-quantum-computer-20-qubit-q-system-one-ces-2019

Wallstreet Journal Editorial Board, 2016. *Apple Is Right on Encryption.* [Online]   
Available at: https://www.wsj.com/articles/apple-is-right-on-encryption-1456877827

Weil, D., 2018. *How Secure Is Mobile Banking?.* [Online]   
Available at: https://www.wsj.com/articles/how-secure-is-mobile-banking-1521424920

WhatsApp, 2020. *WhatsApp Security.* [Online]   
Available at: https://www.whatsapp.com/security/

Whittaker, Z., 2018. *Australia passes ‘dangerous’ anti-encryption law after bipartisan compromise.* [Online]   
Available at: https://techcrunch.com/2018/12/05/australia-rushes-its-dangerous-anti-encryption-bill-into-parliament/?guccounter=1

Whittaker, Z., 2020. *Ex-NSA hacker drops new zero-day doom for Zoom.* [Online]   
Available at: https://techcrunch.com/2020/04/01/zoom-doom/

Whittaker, Z., 2020. *Maybe we shouldn’t use Zoom after all.* [Online]   
Available at: https://techcrunch.com/2020/03/31/zoom-at-your-own-risk/

Whittaker, Z., 2020. *New York City bans Zoom in schools, citing security concerns.* [Online]   
Available at: https://techcrunch.com/2020/04/05/zoom-new-york-city-schools/

Wood, C., 2020. *Elon Musk's SpaceX bans Zoom over security and privacy concerns.* [Online]   
Available at: https://www.businessinsider.com.au/elon-musk-bans-zoom-security-concerns-2020-4?r=US&IR=T

Yadron, D., Ackerman, S. & Thielman, S., 2016. *Inside the FBI's encryption battle with Apple.* [Online]   
Available at: https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple