How reliable is encryption for our security and privacy?

Introduction:

According to digital guardian, encryption disorganizes the data, so only people who have access to the “decrypt key” can read it. Presently, encryption is one of the most in demand and successful data security methods by organizations and governments (nate lord, 2020). However currently, a conflict between law enforcement and privacy is being fought over encryption (kenneth roth,2017) in this report we will discuss the use of encryption in authoritarian regimes as well democratic countries. I'll be discussing in depth issues and will evaluate and discuss perspectives from the USA, Xinjiang province in China and my personal perspective.

Mass surveillance overcomes the use of encryption:

Surveillance is the custom of spying a whole or a significant part of a population (Benson Egwuonwu, 2016). This is largely practiced by the government and companies. Already worldwide 4.66 billion or 59.5% of the population actively use the internet in 2021 (joseph johnson, 2021) and Globally, more than 80 countries implement some form of digital surveillance (SC Greitens, 2020). Oppositions and protests at any scale is inevitable as many people believe this is illegal spying. In recent times many governments have attempted to limit access to strong encryption or restrict anonymity online (HumanRightsWatch, 2015). Governments achieved this by gaining backdoors access into end -to-end encryption. (tony cole, 2020) This completely violates a person's privacy and can prove violent for journalists and human right defenders who rely on strong encryption for their security and privacy. According to Pew Research center, after edward snowden leaked files on mass surveillance by NSA (united states national security agency) many debates have been ignited worldwide.

causes:

According to global database,Terrorism is a common cause as it is highly likely in the middle east for eg. syria ,iraq, south asia for eg. pakistan, india and africa for eg. nigeria as 95% of deaths caused by terrorism are specifically in these parts of the world rather than in australia where according to global terrorism index 2020, ‘terrosim’ is low (score of 2.1 out of 10) however australia has high cybercrime with 57% of australian internet users experienced cyber crime (statista,2019) which aggravates governments to practice mass surveillance. In the USA after the 9/11 terrorist attack, the patriot act was passed which allowed the US to monitor phone calls and emails and track internet activity of americans (dale minishima, 2019) by accessing encryption. According to the center for strategic and international studies, Authoritarian regimes such as China and Russia use mass surveillance to further develop intelligence aims and control the population whereas advanced democracies like new zealand practice surveillance on the grounds of preventing cybercrime and catching suspected criminals. To control the population nationally the chinese government enforced one child per family policy (Kenneth pletcher).families were monitored through mass surveillance to ensure implementation of this

policy. Due to the rise of covid-19 cases in Pakistan at a rapid pace, the government is listening to private phone conversations to monitor possible symptoms and tracking potential virus carriers. (kaukab shairani, 2020) and according to a report from CNBC, China, israel and south korea are also implementing the same methods to fight covid-19.

Perspectives:
Since Mass surveillance is a global issue, some support it and others oppose it. The United Nations argue that governments and other actors hack computers, mobile phones, networks to shadow journalists, UN investigators, politicians and human rights defenders.

In my perspective, encryption is their digital bodyguard. Without encryption, mass surveillance does not allow them to dig deep into cases or files, for instance lawyers who need to find proof to protect their clients and advocates who are against a future "surveillance state" According to the century foundation, mass surveillance has an impact on everyone but its hand is the heaviest in communities already disadvantaged by their race, ethnicity, religion, poverty and immigration status. To back up this claim,

China forbids technology that blocks access by ministry public security (Bruce Sussman, 2019) meaning no access to encryption, private servers or VPN. Consequently, In the Xinjiang province of China, more than one million Uyghur muslims and other turkic ethnic minorities are compelled into labour concentrations also known as "reeducation camps" as a result of being surveillanced through intrusive digital means (2). Maya Wang, a chinese researcher for human rights watch says xinjiang is a more invasive and extreme example of china's large scale surveillance .this is because china is the most surveillanced country in the world (avery coop, 2021) however as per Human rights watch, chinese authorities argue that their "sophisticated" systems are targeting terrorists "with precision" to keep Xinjiang safe .

Consequences:
Talking from an unbiased perspective, the UK prevented 13 terror attacks over 5 years due to surveillance (BBC ,2017). Countries like japan, india, uk, australia and canada, USA (etc) are supporting access to backdoors (Russell Brandom, 2020)

There is an ongoing rivalry between 6 governments and global tech companies over encryption as these companies oppose laws restricting encryption (Aaron Holmes, 2020) due to mass surveillance on their customers. This isn't healthy since tech companies have large consumers globally (Deborah Brown, 2020) and technology is the key driver of economic growth (harvard.edu). Hence, a lot is at risk.

However governments did not consider the fact that cybercriminals and malicious actors also have backdoor access (Tony Cole, 2020) ultimately giving them power to invade people's privacy and potential safety, this is because once the vulnerability of crimes may be hacked and would in turn create much more crimes (kenneth roth, 2017).

According to the UN a possibility of extrajudicial killings are linked to mass surveillance. This is more likely to happen in south asia and the middle east as many cases have been reported there. for instance, murder alllegation of journalist Saleem Shahzad by pakistans intelligence agency ISI (amir mir , 2016)

Course of action:

A solution implemented nationally is ideal. Countries like Ireland where a data protection commission actively is investigating 18 tech companies in the US (Paul Bischoff,2019). According to a study by comparitech Ireland it has the highest privacy and surveillance protection. France also scores second to Ireland as it has the Commission Nationale de l'Informatique et des Libertés (CNIL). Meaning these data protection councils/committees limit mass surveillance effectively and efficiently. These data protection committees can also be made in muslim countries such as iran , egypt etc as there is much cooperation by citizens due to their religious beliefs connected to privacy. Journalists and human rights defenders will also have a safe environment .

Encryption and the insider threat:

Insider data breaches pose a threat to businesses , institutions and the government. According to a 2020 global report the cost of insider threats increased by 31% meaning $11.45 million globally, yet the enterprise use of encryption has seen its largest increase in the past decade. Therefore, encryption is useless against the insider threat as suggested by articles such as guardtime, McKinsey and company (etc) Regardless of spreading awareness of insider attack risks and improving cybersecurity tools the percentage of insider attacks keep rising (Ekran ,2020).

According to BBC, Edward Snowden, a former CIA contractor and present whistleblower leaked insider global mass surveillance files from NSA.. he didn't need to break the encryption, he only compromised the credentials of the administrators granted access to the encrypted data (mike gault, 2021). The source is reliable as the author is the CEO of the website this was published on and has a PHd in electrical and electronics engineering. This leak sparked global debates and many countries like brazil, india and germany made it hard for us firms to do business there (Elizabeth Dwoskin, 2014). Hence , due to this insider breach USA was impacted politically and economically and the government's privacy was violated. Even local companies can be affected such as Sage, in the UK known for accounting and HR software, compromised 280 of its business customers through an insider-data breach (ObserveIT, 2018).

Causes and consequences:

According to a study by Carnegie Mellon university computer emergency response team, after studying 700 well documented insider attacks it has concluded that reasons for insider threat are theft for financial gain , IT sabotage meaning an act of revenge against the organization by foreign and personal methods. Human error and carelessness is also a common reason for insider threats as said by the ponemon institute. For instance despite using email encryption for

malicious hackers, employees can send data to the wrong person intentionally or unintentionally.

According to Cisco,a multinational organization, one third of businesses lost 20% of their revenue due to data breaches, for instance the american superconductor suffered $800 million in revenue due to intellectual property theft meaning an insider stole the company's invention or idea.

According to a study by a multinational company, deloitte, due to insider breaches customer acquisition has decreased by 50%. Thus, due to a tarnished reputation, companies lose a large amount of customers and therefore revenue. This same study uncovered a large company could experience an effect of $250 million over a five year period by the devaluation of its trade name alone. Consequently, people in these companies will lose their jobs or earn less salaries in many countries worldwide. In Fact many countries are the root cause behind insider threats such as north korea and sony production (voa news 2020) controversy and an incident in which former twitter employees were caught spying for saudia arabia (Nick Statt, 2020)

Course of action:

Insider breach mitigation technology is inconsistently utilized according to an egress in depth study. We have tried using encryption of all forms as a mitigation technique but it only works on external attackers and is useless when it comes to insider attacks (cloud mask). By spreading awareness in the importance and the uniqueness of insider attacks starting from a local level this global issue may be solved. These awareness sessions will ultimately teach employees to be proactive and know the risk and impact of carelessness as 60% of insider attacks are due to carelessness (dice, 2020). These employees should also be tested by company high officials and founders. So , incase of any real-life leak of confidential data employees are trained to respond quickly without tension and confusion. In addition to these sessions companies should also install an insider threat detection system which is effective because it has an overall of 5 stars (capterra) this will be used for malicious insiders and moles- foreign or domestic. If prevention of insider attacks through this solution is successful locally for instance in karachi or new delhi. This is likely to become a national and then potential global solution especially nowadays in the midst of the covid 19 pandemic insider threats are rising (jane grafton, 2020) hence a global solution is in demand.

Conclusion:

In the end, my view on encryption has changed. Through this report I learnt how progressive we are in the realm of technology (max roser,2013) this source is authentic as it is cited by 64 people. From biometric and facial recognition systems to supercomputers which can break encryption (Michael winter, 2013). As I've read through many articles and studies that with the rise of digital technology conflict increases (Philip Reiner, 2019) such as the Sci-fi movie "mortal engines". On a serious note, I learnt how powerful encryption is and how it protects us from cyber criminals (Riana Pfefferkon, 2019). After analysing the perspectives from Xinjiang, China,

it occurred to me, the extent countries reach to oppress their citizens by driving them into prison camps and barely no one is talking about them. My research on the situation of Uyghur muslims motivates me to raise my voice for the voiceless through social media. from the perspectives of the journalists and human right defenders I learnt their most dominant qualities "courage and initiative". incase of a potential democratic riot, they would be first in line to sacrifice themselves in the name of freedom and equality

References:

Lord, Nate. (2020) "what is data encryption? definition, best practices and more" Digital guardian , 1st december. Online . https://digitalguardian.com/blog/what-data-encryption accessed: 30/4/2021

Roth, Kenneth (2017) "the battle over encryption and what it means for our privacy" human rights watch, 28 June. online. https://www.hrw.org/news/2017/06/28/battle-over-encryption-and-what-it-means-our-privacy accessed: 22/4/2021

Egwuonwu, Benson (2016) "What Is Mass Surveillance And What Does It Have To Do With Human Rights?" eachother.org.uk, 11 april. Online. https://eachother.org.uk/explainer-mass-surveillance-human-rights/ accessed: 29/4/2021

Johnson, Joseph (2021) "global number of internet users 2005-2019" statista, 27 Jan. online.

https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ accessed: 27/4/2021

Greitens, S.C. (2020). "China's Surveillance State at Home & Abroad: Challenges for U.S. Policy, Working Paper for the Penn Project on the Future of U.S.-China Relations", October 2020. Online https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/b/732/files/2020/10/Sheena-Greitens_Chinas-Surveillance-State-at-Home-Abroad_Final.pdf accessed: 17/3/2021

No author (2015) "UN: Online Anonymity, Encryption Protect Rights"
Human rights watch, 17 June, Online.
https://www.hrw.org/news/2015/06/17/un-online-anonymity-encryption-protect-rights accessed: 20/4/2021

Cole, Tony (2020) "The Dangers of Government-Mandated Encryption Backdoors" security boulevard, 9 october. Online.
https://securityboulevard.com/2020/10/the-dangers-of-government-mandated-encryption-backdoors/ accessed: 21/4/2021

No author (2020) "Percentage of internet users in selected countries who have ever experienced any cyber crime as of December 2019" statista, march .online.
https://www.statista

.com/statistics/194133/cybercrime-rate-in-selected-countries/ accessed: 23/4/2021

Mineshima, Dale (2019) "THE FIRST AMENDMENT ENCYCLOPEDIA" mtsu.edu, July. online. https://www.mtsu.edu/first-amendment/article/1096/usa-patriot-act-of-2001 accessed: 18/4/2021

Pletcher , Kenneth. No date "one child policy" Britannica. Online. https://www.britannica.com/topic/one-child-policy accessed: 25/4/2021

Shairani, Kaukab (2020) " ""Will Pakistan's Mass Surveillance Strategy Outlive the Pandemic?" the diplomat. 5 June. online. https://thediplomat.com/2020/06/will-pakistans-mass-surveillance-strategy-outlive-the-pandemic/ accessed: 20/4/2021

Sussman, Bruce (2019) "Chilling Assessment of China's New Cybersecurity Law: 'There Is NO Place to Hide'" Secure world expo. 15 october. Online. https://www.secureworldexpo.com/industry-news/what-does-new-china-cybersecurity-law-do accessed: 1/4/2021

Coop, Avery (2021) "Mapped: The Top Surveillance Cities Worldwide". Visual capitalist. 1st January. Online

https://www.visualcapitalist.com/mapped-the-top-surveillance-cities-worldwide/ accessed: 26/4/2021

No author (2017) "Security services prevented 13 UK terror attacks since 2013" BBC .6 March, online. https://www.bbc.com/news/uk-39176110 accessed: 25/4/2021

Brandom, Russell (2020) "US joins six countries in new call for backdoor encryption access" the verge. 12 october. Online https://www.theverge.com/2020/10/12/21513212/backdoor-encryption-access-us-canada-australia-new-zealand-uk-india-japan accessed: 22/4/2021

Holmes, Aaron (2020) "The US and 6 other countries are pressuring tech companies to weaken encryption and make it easier for police to snoop on apps like iMessage or WhatsApp" business insider .21 october. Online. https://www.businessinsider.com/us-doj-barr-five-eyes-weaker-encryption-backdoors-2020-10 accessed: 27/3/2021

brown , Deborah (2020) "BIG TECH'S HEAVY HAND AROUND THE GLOBE"
FPIF (forieign policies in focus). 2 september. Online

https://fpif.org/big-techs-heavy-hand-around-the-globe/ accessed: 21/4/2021

Mir, Amir (2016) "5 years later: Saleem Shahzad's unsolved murder further weakens press freedom in Pakistan" asia times. 29 May. online https://asiatimes.com/2016/05/5-years-later-saleem-shahzads-unsolved-murder-further-weakens-press-freedom-in-pakistan accessed: 25/4/2021

Bischoff, paul (2019) "Data privacy laws & government surveillance by country: Which countries best protect their citizens? Comparitech. 15 october. Online https://www.comparitech.com/blog/vpn-privacy/surveillance-states/ accessed: 30/3/2021

No author (2020) ""Insider Threat Statistics for 2020: Facts and Figures" ekran. 28 december. Online. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures accessed: 22/4/2021

Gault, Mike " Six Reasons why Encryption isn't working" guardtime. Online https://guardtime.com/blog/6-reasons-why-encryption-isnt-workin accessed: 24/4/2021

Dwoskin, Elizabeth (2014) "new report:Snowden revelations hurt US companies" the wall street journal. 30 July. online

https://www.wsj.com/articles/BL-DGB-36772

No author (2018) "5 Examples of Insider Threat-Caused Breaches That Illustrate the Scope of the Problem" ObserveIT. 22 march. Online https://www.observeit.com/blog/5-examples-of-insider-threat-caused-breaches/

No author (2021) "Three North Koreans Indicted in Sony Hack" VOA news . 17 february . online https://www.voanews.com/economy-business/three-north-koreans-indicted-sony-hack accessed: 25/4/2021

Statt , Nick (2020) "US seeks to drop charges against former Twitter employees accused of spying for Saudi Arabia" the verge. 28 july. Online https://www.theverge.com/2020/7/28/21345794/twitter-employees-saudi-arabia-spies-charges-dropped-case-dismissed accessed: 25/4/2021

No author "how data protection can fail against insiders" cloud mask. No date. Online https://www.cloudmask.com/blog/data-protection-under-breach/data-protection-fail-against-insiders accessed: 27/4/2021

No author (2020) "Insider Threats: How Co-Workers Became a Bigger Security Headache" dice. 27 february. Online

https://insights.dice.com/2020/02/27/insider-threats-co-workers-bigger-security-headache/ accessed: 25/4/2021

Grafton , Jane (2020) "insider threats are on the rise" security boulevard. 30 june. Online https://securityboulevard.com/2020/06/insider-threats-are-on-the-rise/ accessed: 26/4/2021

Roser, max and ritchie, hannah "technological progress" our world in data. No date . online https://ourworldindata.org/technological-progress accessed: 30/4/2021

winter , michael (2013) "NSA uses supercomputers to crack Web encryption, files show" usa today. 5 september. Online https://www.usatoday.com/story/news/nation/2013/09/05/nsa-snowden-encryption-cracked/2772721/ accessed: 25/4/2021

reiner , philip (2019) "Technology, change, and the inevitability of conflict" digital frontiers. 22 october. Online https://www.orfonline.org/expert-speak/technology-change-and-the-inevitability-of-conflict-56889/

Pfefferkorn, Reina (2020) "THE EARN IT ACT: HOW TO BAN END-TO-END ENCRYPTION WITHOUT ACTUALLY BANNING IT" stanford law school. 30 january. Online. accessed: 25/4/2021

http://cyberlaw.stanford.edu/blog/2020/01/earn-it-act-how-ban-end-end-encryption-without-actually-banning-it