General instructions to be followed to pass essay

1- Spend time on rightly comprehension of the topic, you won't pass the essay unless and untill you addressed the asked part

2- Try to make your main heading in the outline from the words in the question statement

3- Try to add hook in the introduction. The length of introduction must be of 2 sides

4- your topic sentence in your argument must be aligned with the ending sentence

5- Avoid firstly, secondly, thirdly etc. in outline

6- add references in your arguments with proper source. Go for diversification of references

7- Do not add new idea or point in Conclusion

8- You won't pass the essay if make more than 4-5 grammatical mistakes

9- outlines that are not self explanatory or does not aligned to with the essay statement are liable to mark 0 and the essay would become null and void

10- always try to be relevant to the topic, if even your 1 or 2 arguments are irrelevant, the examiner would not pass your essay.

DATE: __/__/____ DAY: __/__/____

Name: Muhammad Osama Shahzad

Batch: BS

Mock Exam

Essay

Technology as a threat to Privacy

Outline

1. Introduction

1.1 Hook

1.2 Background

1.3 Thesis statement: While technology stress ease of connectivity, comfort and innovation, it poses a severe threat to individual privacy, data exploitation and is a tool that can be used by individuals, corporates or states against humanity.

Also

Where is the main header?

2. Mechanism of surveillance in everyday life

2.1 Facebook, Smartphones, Credit Cards, Bank transfers and ATM withdrawls.

How is it a threat?

2.2 Everywhere Digital footprints, tracking, hacking, firewalls and tracking patterns.

2.3 Cameras, biometrics are not always your friend

DATE: __/__/____

3 Humans are the Product in data harvesting

3.1 Corporates' role

3.1.1 Deceptive and long terms of service allows corporate to collect data freely.

3.1.2 Corporate use data Patterns for commercial benefits.

3.2 Governments' role

3.2.1 Governments use data to influence their citizen behaviour

3.2.2 Governments use data for Political Purposes.

4 Hacking and Cybersecurity challenges

4.1 Personal data being sold on black web.

4.2 Cybersecurity as a tool of War.

4.3 Data related crimes: A source of terror funding and financing.

5 Implications on Freedom of Speech and Ethical Ramification

5.1 AI based surviliance of targeted groups

5.2 Use of Generative AI to generate fake images and videos

5.3 Access of explicit sites & sites and data to underage citizen

You are talking about the negative impacts of technology. You are not presenting the arguments pertinent to threat to privacy

Work on your topic comprehension
Improve your phrasing
Words selection must be improved

Must attend the tutorial session for further suggestions and mistakes

DATE: __/__/____ DAY: __/__/____

6 Counterarguments - Technology a Friend of Everyone

6.1 Technology a Privacy enabler

6.2 Technology a source of information Chat GPT Case study

6.3 Rebuttal and inefficiency of enough cybersecurity cover for common People.

7 Conclusion

7.1 Restate Thesis

7.2 Call to Action

Essay

Imagine going through your social media and liking the Pictures of a beach in Bali. Moments later, being bombarded by ads for flights to Bali — a coincidence? Not really. According to Cambridge Analytics, Facebook harvested data of 87 million users without consent and used it to manipulate its users on a global scale. This is not a one time occurance but a new normal in this data driven world. Internet of things (IOT), smart equipments, cameras, cars and the wide array of consumer Products make our life easier but also make us vulnerable equally. Privacy, that was once a right, sometimes willingly and other times in ignorance is being traded for fancy goods that makes data harvest easier. While technology offers unprecedented innovation, it also makes us a target of Privacy breaches, data exploitation, surviliance and manipulation. Data has been weaponised and humans have limited counters to it. Only effective counters against a cyber attack is to do a counterattack with greater force. While countries might win in this war, a common man might have a lot to loose.

Not up to the mark introduction

Online Platforms always keep a track of their users' activities. They are regardless of either they country they oPrate in or they country they are based in or, conveniently, for sake of user's convenience. FATF and other such agencies requires governments to keep a track of financial transaction of every Person. The card a Person use or the transactions done by a banking aPP are a record of daily life, where we went in the morning for breakfast, which train we took, what we bought, which countries we visited — Thus, all of our financial money trail is there in a recorded form in some cloud platform to be used by governments or can be hacked (HBL 2017 data breach) and stolen. The banks and governments might have insured consumer's accounts for monetary losses but the data once gone has no substitute and can be later used agains consumers by criminals. Cameras, being used in the name of safety are also being used in surviliance. There is no law against the governments for misusing the cameras and digital firewalls that were [illegible] for the Peoples' safety to be later

Argumentation is missing

used against them. Amnesty International accuses the authoritarian regimes for using such platforms (like Pegasus) to crub voices of opposition and do Political engineering while carrying out human rights violations. The data breach of Pakistanis from NADRA is one other such example that happened in 2021 and put millions of Pakistanis at risk whose personal data, including biometrics are up for grab at darkweb. Thus, the surviliance by governments put its citizens at risk with little incentive being offered to them.

Technology companies are mostly public companies - like Facebook, Twitter and Google e.t.c - and their main objective is to increase their profits. They aren't charitable organizations out there to preach about morality, social norms or to do good but there is a vicious race among them to grab a bigger piece of pie in terms of profitability and market share. Such companies have always come under criticism for violation of individual's privacy and many times, such incidents remain unnoticed due to the government's

involvement. The whole Problem USA had with a social media Platform Tiktok was its allegedly chinese origin and USA wanted to take it over due to this so[illegible] of its [illegible] being [illegible] exploited by a [illegible] country was a security risk. In 2019, Meta (Parent company of Facebook) was fined $ 5 billion for GDPR violations and misusing its consumers and users data for its commercial benefits and this was not the first time they were accused of this Practice. Companies harvest the data of its users, sort and clean it and then analyze the data to get results that may benefit them commercially and helps them to make strategic decisions such as: when to show an ad? what kind of ads are effective for a specific area? and find out their target audience and ways to manipulate them into clicking on the ads and spending money. Thus, the Platform that is offering its services for free is not free at all and is involved in data harvesting and later using it to manipulate its users. The governments also have an unseen role in these

Your own thoughts are missing. You are just providing me the information

Practices. It will be difficult to accuse a state's involvement - directly - in data harvesting but states turn blind eyes towards the corporatocracy in their data related practices. In return, they use the same IT companies for political engineering and influencing on election. Russia, in the previous two US elections, has been accused by US politicians for using social media to try influencing US elections in favour of Trump (Republicans). Similarly, the governments in power use the data the acquire in their political campaigns, development work and to make strategic decisions such as dividing constituencies, choosing electoral candidates, announcing funds for constituencies. According to Amnesty International, governments misuse their powers to suppress voices of dissent and political rivals. The data can be used with the alliance of fifth pillar of a nation — media — for doing propaganda and misguiding people just like the USA did during cold war era by branding every voice of dissent as a communist. Thus, it can be concluded that the humans are the products and data is the commodity that is being used by both the corporate and

DATE: __/__/____ DAY: __/__/____

Politicians for their own gains.

The darkest and scariest Part of Privacy debacle is that some hacker -whose Potential target is you- knows more about your Patterns and behaviour than you, yourself. The Personal data security is a myth; If there is a lock then it also has a key. Similarly, if the data is on the cloud storage, there is a way to hack it, the only question is about the time. CIA vault 7 data breach happened in 2016, Indian Adhaar card data in 2018, Pakistan's NADRA data in 2021. These data breaches are enough to water down the claim of data security as millions of Peoples' financial data and biometrics are up for grab on the dark web for the right Price. States either deny such incidents or refuses to take any responsibility. NADRA denied a complete hack but also refused to reveal the scale of it and not a single Person was sacked for the 2021 data breach. Data security is a tool of strategic Importance and is being used by countries to target

subject or People of interest. Israel has repeatedly used it by first targeting Hizballah in Lebnon in 2024 by detonating hundreds of walkie-talkies fitted with explosives in 2024 and then Precisely targeting the top miltary and nuclear Program leadership using FPV drones and Precision strikes. All of this was Possible due to the Perfect and real-time information due to data breaches coupled with on ground human intelligence. In Operation Sindoor Pakistan also employed the attacks in Indian cyber space. The cyber attacks were directed towards indian strategic websites and infrastructure related to Power sector. Pakistan's attacks were confirmed by indian minister Manohar Lal according to whom all such attacks were successfully repelled. Risk for such attacks on an even larger scale exists in the future such conflicts as cyberspace has been identified as an avenue of war and a Place to contest and disrupt. It can Potentially but billions of users' data at risk and the damages to the common People might not be sudden but may happen during extented Periods and in such cased, even the governments

will refuse to take responsibility of such damages. Lastly, cyber space has become a thriving place for the criminals and terrorists. Criminals-terrorists nexus is unbreakable and this nexus has also been rooted in the cyber space where wide range of cyber attacks are used to steal data and money and later people are blackmailed by that information for money or the information is used to carry out direct crimes such as ~~kidnapp~~ kidnaping or theft. Data is employed by terrorists against the state for their attacks for example to calculate response time of state or to devise strategies for their henious acts. Pakistan was put into grey list by FATF to strengthen it banking system and make its structure resilient against terror financing. Crypto, another digital tool loved by terrorists and criminals for financing due to its hard to track nature and exstence of decentralized exchanges but strategies are being devised to counter this issue and make terror financing difficult and traceable. It can be concluded that hacking is tricky to deal with but can be countered by awareness and education to general public

and Promote data security practices so criminal activities and terror financing from cyberspace can be curtailed.

Artificial Intelligence is a tool without any morals or ethics. It does what its user wishes to do without contemplating on the outcomes. It is like a gun with endless bullets in wrong hands and any one with right knowledge can train his own algorithm for his specific task. Artificial Intelligence has ended or greatly limited humans' role in monitoring security cameras. It has the ability to find the person of interest from a fottage of days in a matter of seconds. It makes it a dangerous tool in hands of dictators and has been repeatedly used to target specific groups (Amnesty International) Furthermore, the use of Generative AI to Produce fake videos has endless ethical implications. It is an issue that has created a moral dilemma and a grey area. On one side, it can be used to treat untreatable wounds and diseases while other side it has been widely used in Propagandas and social engineering in recent wars (Israel-Gaza conflict). It can be used for Political

engineering by using doctored videos and images of political opponents and spreading it by fake and untraceable accounts. To curb such crimes Pakistan had FIA cyber crime wing but also raised a seperate department called NCCIA and has used cyber firewall but the out of country accounts can't still be controlled by these ~~institutes~~ institutes. Lastly, the use of explicit material sites and access of such material on open internet to the underage is a major issue. Due to this issue, Australian government has banned usage of social media for children upto 13 years of age in 2025. There are millions of accounts uploading and sharing stuff online on social media so the platforms lack the capability to monitor all of that data in real-time due to which it can be concluded that the technology unlimited access to underage has implications and it is altering the ethical roots of society. It will affect the mental health of the underaged users and their social tracks will keep chasing them in the future due to the Privacy decisions gone wrong.

On the contorary, technology has Proved to be a Privacy enabler. The VPNs, firewalls, Privacy settings, updates, antiviruses, AI recommendations for account Protection are a few examples on how technology is guarding our Privacy. The controls on who can view our Profile and Personal data makes use secure and the data breaches reduce on a Personal level collectively. Furthermore, ChatGPT is trained on the data of People but has today turned out to be the biggest helper of People. It can give opinions and information to People relatively easily and can answer basic questions like usage of a specific medicine, today's headlines, weather forcast, food recipies and can create budget, help make smarter decisions to People. So, the data harvesting is being used for the collective good and People are also benifitting from it. It's helping making better cities, reducing crimes, improving quality of lives and finding cure of diseases but despite all that, if the foundation is wrong, it won't make the building on it durable. The Privacy concerns if

DATE: __/__/____ DAY: __/__/____

weighted their implications would be far worse and personal choice and concent has its own place. If concent is not involved, it will make the whole Practice fruitless and will leave even greater holes for misuse of authority in the future.

There is a need for collective efforts by all the countries on the forum of UN to make collective cybersecurity and Privacy framework where Personal consent is respected and humans individual Privacy is Protected. AI must be used responsibly. Technology is changing our lives for the good, making our lives easier, improving comfort and quality of life but it must not become a threat to personal Privacy. The laws must be there to ensure data security and data deletion after a specific time so no data can be misused. In absence of such frameworks and willingness of major countries to support such frameworks, technology will keep being a threat to individual freedom, security and will keep being a risk for personal fundamental rights.