ESSAY Date:

TECHNOLOGY IS A THREAT TO PRIVACY

Your language is fine
Your outline should be self explainatory to pass the essay

OUTLINE

1. Introduction
   - Thesis statement: The ~~~~ technological advancement poses a great threat to privacy, from an individual to the state level.
   - Hook: "Every swap and tap allows technology to erode ~~the~~ the personal lives privacy.
2. How technology can be a threat to privacy.
3. Areas that shows that technology is a threat to privacy.
   a. Growing cyber crime reports (Interpol report 2024)
   Use it as a reference
   b. AI and deepfakes. (Elon Musk speech)
   c. Sell of data on darkweb (India Adhaar card data leak 2021).
   d. Surveillance through electronic gadgets.

Your points must show how it is eroding points and not the case studies

Date:

e. Use of VPN and VPS.

f. Financial frauds (1.6% GDP loss to Global IT economy annually)

g. Threat to state's privacy (National Bank cyber attack ; 153 countries affected by Wannacry ransom attack)

These are just tools

h. Threat to global security (Stuxnet attack on Iran's nuclear facilities).

is prevalent.

4. How threat to privacy ~~can be mitigated~~. (weak laws, unprosecuted cases ITU report, low digital literacy).

5. How threat to privacy can be mitigated. (EU AI Act 2024, UNESCO recommendation 2021, IRRI report - Public private partnership).

6. Conclusion.

"Every swap and tap allows technology to erode the personal lives' privacy".

The growing technological advancement pose a great threat to privacy, from an individual to state level. In the contemporary times, the technological advancement has been part of daily lives and every aspect.

Date:

Thus, avoiding technology to protect the privacy is not a realistic idea to implement. Whereas, the human lives is so dependant upon the technology that it could not imagine a moment without technology. In a world, where human life is so immensely dependent on technology, the negative side of it poses threat to everyday life in terms of privacy etc. The growing number of cyber crime case throughout the world shows the rate of misconduct occur through the use of technology. The current advancement in artificial intelligence that enables users to create deepfakes easily that it erodes the privacy of other individuals. Whereas, there are number of incidents reported where the personal data is evidently to be sold on the platforms like dark webs. This selling of data did not confined to threat the individual's privacy solely, but the state's data. Another evidence shows that the phones uses its camera and microphone 24 hours. The purpose of this surviellance is unknown, but its threat to privacy is significant. Similarly, the unauthorized use of location changing softwares such as VPN and VPS have intensified the privacy

Date: _____

matters. On the other hand, the scammers get hands on the private data so easily that they commit financial frauds and gain handsome amount of money annually. At the state level, the hacking of government's sites and ransomware attacks also erode the privacy of state's data. This can also affect the state's secrecy. The intensity of such attacks can be observed through the incident when the nuclear sites of Iran got hacked. This incident not only shows the fact that nuclear secrecy of Iran was eroded, but this also pose threat to nuclear confrontation in the region. There are multiple reasons due to which the technology is a threat to privacy like, weak laws, unprosecuted cases and digital literacy. However, the pragmatic measures can help to reduce this threat. For instance, the EU has introduced AI act in 2024 which will work on firewalls and swift violators to curb the privacy threats. Whereas, the UNESCO recommendations can also help in this regard. The public-private partnership programs are also beneficial as evident in other developed countries. Thus, technology poses threat to privacy, but it can be prevented

Date: _____

through prerequisite measures.

In the twenty-first century, everyday life revolves around technology. This makes it impossible to eliminate technology from lives for the sake of privacy. Technology involves daily communication, making memories, financial transactions, online earning, banking system and state's security as well. In all the dimensions in which technology plays its part, it also poses threat to it. The threat is not just limited to leak of data and information but the actual threat begins from the misuse of the respective data. Thus, technology can be threatening to one's private data.

There are several areas that evidently shows that technology is a threat to privacy. These areas include from an individual level to the state level.

The growing cases of cyber crime shows the number of violation occured through the use of technology. The violator uses technology to scan.

Date:

blackmail by getting their private information. According to the report by Interpol in 2024, the developing countries face 10 times more cyber crime cases than developed countries due to lack of tech-security advancement. These cyber crime cases are the one that are reported to the authorities. There are numerous violation to privacy occurs which went unreported and unnoticed by the authorities. Hence, the violators through the use of technology violates the privacy of other individuals.

Bring it before concluding note

The advancement in the field of artificial intelligence that it can generate realistic images that seems ~~so~~ real and can rarely be noticed its authenticity. Once Elon Musk, the founder of world's most used AI platforms ~~says~~ said that, "AI can be so dangerous as much as it is useful". Because it can generate exact facial and voice identity by minimal data. These deepfakes are being used for blackmailing purposes as well. In this manner, through AI and deepfakes, the privacy of every user ~~and~~ is undermined.

Date: _____

The most negative aspect of technology is its websites like darkwebs. It is reported that the illegal and inhuman activities are being conducted on darkweb at an unprecedent level. These activities cannot be easily traced or prevented due to absence of centeralized authority on these sites. The data of individuals is easily available and being sold on darkweb. For instance, in 2021, India's Adhaar card data was found to be sold on the darkweb. This means, the every individual's personal data in India was present on the internet which can be easily accessible and can be used for harmful purposes. This incident reflect that the privacy is at risk through technological means.

Switch referehces with black pen

The phone's cameras and microphones are always in working. It is noticed the smartphone devices has secondary camera and microphone which is constantly working and it can be seen through the settings but turning it off is not available in the options. The question arises that why these gadget have activated camera and microphones as a surveillance device. This can also be used by

Date: _____

~~through prerequisite measures.~~

the apps on which the user voluntarily give consent in order to access the app such as, facebook, instagram, snapchat etc. These apps demands access to certain ~~feaut~~ features of the phone at the time of installing them. Their constant access to such features compromises the privacy aspects of an individual.

The unauthorized use of location changing softwares has ~~further~~ aggravated the menace. The softwares like Virtual ~~Alctuo~~ Positioning Network (VPN) and Virtual Positioning Server (VPS) allows users to change its location on the internet to any desired place around the globe. These softwares are used ~~by~~ for the online earning purpose, but it gets dangerous when the scammers use it for financial gain without being traced. Through using such softwares, the violators are difficult to be traced and caught by the cyber authorities. In this way, VPS and VPN allows users to change their ~~int~~ identity and erode others' privacy conviniently.

Use it as a reference

Date:

Through the misuse of technology and privacy, it became easy to commit financial misconducts. According to International telecommunication Union, the global economy losses around 1.6% of GDP due to financial misconducts. However, the financial misconducts can only be conducted when the violators have access to the victim's personal data such as card number, CVC or bank account number. They only require the One-time password (OTP) to access their financial belongings. This also shows that through the confidential credentials, technology can be threat to financial privacy.

Beyond the individual level, technology can also be dangerous for the state. The state's confidential data and information is also at risk to the hackers. For instance, in 2022, the National Bank of Pakistan ~~was~~ has aborted all their online operations due to a hacking attack. ~~This~~ The operations were restored after 3-days when the confidence over the platform was restored completely. However, the degree of threat can be examined when the Government bank's online platform was hacked and was unfunctional for

Date:

three consecutive days. This shows that the technology poses great threat to Government institutions beyond the individual's sphere.

These ransomware attack are prevalent and they impact the states. Similarly, another ransomware attack "wannacry" affected over 153 countries around the world. Thus, # in this way, technology impact the state's privacy.

The technology can also be a threat to global security where it undermines the security confidentiality of countries. For instance, the stuxnet attack on Iran's Natz nuclear facility. This attack apparently showed that the nukes are being monitored but this was a mere hacked information. It could also ~~be~~ hinder the control of nuclear arsenals. However, such attacks illustrated that the secrets of state such as nuclear capabilities can be at risk of confidentiality due to technology. The technology can be used to undermine the state's confidential information.

Date:

The technological advancement has opened numerous opportunities that are ~~possible~~ positive. Simultaneously, it also raise privacy concerns. However, identifying the core reasons due to which the privacy threat is prevalent, it can help to mitigate those areas.

The most prominent ~~is~~ factor that excerbate the misuse of technology is weak laws. The laws regard misconduct through the use of technology is are introduced but its interpretation and implement is yet to be strengthened. According to ITU report, over 65% of cybercrime case went unprosecuted due to weak laws. Besides that, as per the UNESCO report, only 31% of population is digital literate in developing countries. In this way, the people will easily fall into the trap of technological misconduct. Thus, the primary reasons behind the unprecendented technological threats is lack of laws and low digital literacy.

These areas can be improved by improving the technological structure. This can be possible through collective effort and infrastructural betterment. Recently, EU AI Act 2024, Paris AI Summit

Date:

Summit shows that the technological threats can be prevented by implementing laws and collective efforts. On the other hand, UNESCO recommended a framework in 2021 that suggested collective responsible action and respect of each other's sovereignty over technology. This framework also suggested to build strong firewalls to limit technological threats. The Islamabad Policy Research Institution (IPRI) suggested that through public-private partnership, this threat can be mitigated to some extent.

Concluded

Thus, it can be concluded that technology is a threat to privacy from an individual to state level. The growing technological advancement, particularly in the field of AI, poses threat to privacy in terms of individual's identity. However, these threats can be overcome by implementing timely and pragmatic actions. The collective effort is crucial in this regard for swift control. It is not a realistic idea to reverse the technological advancement, but altering it to lessen the privacy threat is a viable strategy to adopt.

Elaborate it