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

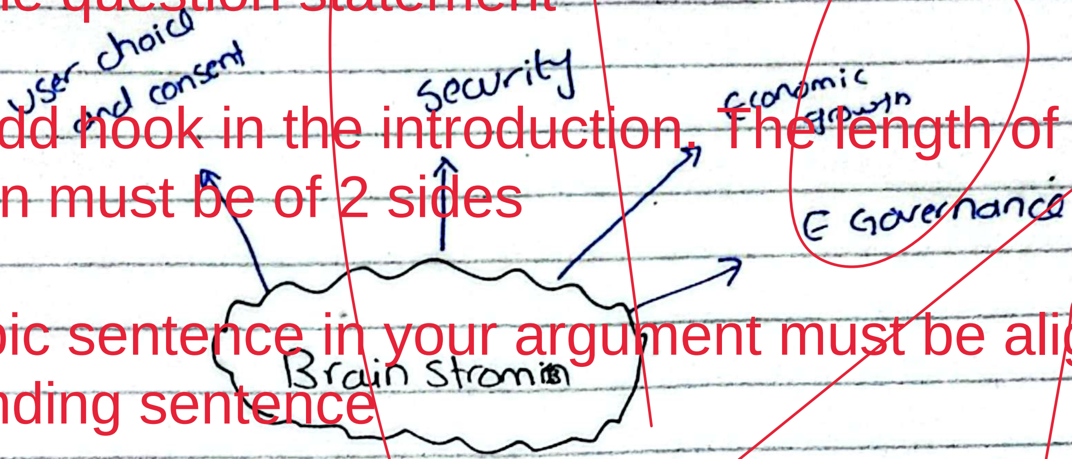
7- Do not add new idea or point in Conclusion

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.

Technology is a threat to privacy.



Outline

1- Introduction

1.1 Hook

1.2- General statement

1.3. Thesis Statement

while technology offers real benefits, but the way it collects, stores and tracks our data makes it a serious threat to personal privacy today.

2. Technology Is NOT a Threat to privacy

2.1. Enhances Security Throug surveillence and Data Monitoring.

2.1.1. CCTV, biometrics and digital tracking reduce crimes

2.1.2. Data collection improves public safety.

2.2. User consent and control over personal Data.

2.2.1 Platfoms provide privacy settings, opt-ins and permissions.

2.2.2. Individuals choose what to share.

2.3. Essential for Digital Banking and services

2.3.1. Ecommerce, banking, telemedicine rely on data sharing

2.3.2. without data access, services would collapse.

2.4. Improves Governance Transparecy

2.4.1 Digital record keeping reduces corruption

2.4.2 NADRA, e-governance systems streamline services

If this is your stance, try to provide more arguments in this header

2.5- Threat Comes from Misuses Not Technology itself

2.5.1 Tools are neutral; responsibility lies with human and institution

3 Rebuttal: Technology is a Threat to privacy

3.1- Survaillence often crosseses into overreach

3.1.1 - The same tools that "prevent crimes" create mass survaillence and profiling

3.1.2. Citizens lose anomity and autonomy when the state or corporation watch everything

3.2- User consent is Mostly an illusion.

3.2.1 Unending terms and conditions, dark patterns and default tracking make consent meaningless

3.2.2- Users have no real control once data enters corporate servers

3.3- Digital Economy Exploits data. Not just uses it.

3.3.1. Companies like Meta, Google, Instagram monetize behavior preferences and even emotions

3.3.2- Data brokers trade personal information without transparency

3.4 E-Governance Risks Massive Data leaks

3.4.1- Centralized databases (like NADRA) are prime hacking targets

3.4.2- Mismanagement leads to identity theft, unauthorized surveillance and political manipulation

3.5- Tools are not Neutral - They are designed to Extract Data.

3.5.1- Algorithms AI cookies, location tracking are build for Surveillance capitalism

3.5.2- They are designed intentionally prioritized data harvesting over User Privacy

4. Condusion:

Most of your points are the negative or positive implications of technology rather than threat to privacy.
Must work on your topic comprehension
Improve your phrasing
Word selection must be improved

Must attend the tutorial session for further suggestions and mistakes

Essay

In 2018, the fitness app Strava released a global activity map that Unintentionally revealed the movements of military personnel at sensitive bases. What was meant as a harmless feature exposed highly private information to the public. This incident shows how technology even for simple convenience can turn into a serious threat to privacy. Technology has become an ~~Ad~~ inseparable part of our daily life, making communication, shopping bankng and entertainment easier than ever. smartphones Social media and smart phones collect vast amount of personal data and information often without people fully realizing the extent. Even when privacy settings are available, consent is often superficial and data can be misused ~~the extent~~ or even sold. While these tools being efficent and convinient, they also open doors for surveillance identity theft and data exploitation. Technology gives many benefits but the way it collects, stories and tracks our data makes it a serious threat to personal privacy today

Introduction is not up to the mark at all. Must work on your introduction

Surveillance technology. Such as CCTV Cameras, biomatric systems and digital tracking tools is often praised for enhancing security and maintaining public safety. These systems allow authorities to monitor high risk areas deter criminal activities and respond quickly to incidents. for example in urban centers the presence of cameras has been shown to reduce pretty crimes and traffic violation. Recently Sindh Government has introduced E-challan system in Karachi which have make traffic control in the city easier than the manual system. and even if someone violates the traffic rules CCTV cameras catch the traffic violators through the number plate of car and motorcycle and track the number and the fine gets delivered to their houses, similary biometric identification in airports and banks ensure that only authorized individual gain access preventing fraud and identity theft. Moreover these technologies help build safer communities while improving emergency response time

Moreover. Modern digital platforms often emphasizes user consent and control over personal data claiming that individuals can choose what to share and what not to share.

Seems like you don't have the idea regarding argumentation. Because you are providing me the information only

Many websites and apps provide privacy settings allowing users to adjust who can see their information and offer opt-in mechanism for communication For example social media apps like facebook and instagram let its user to decide whether their posts and stories are private, only friends or public. Features like close-Friends built in on apps like instagram to protect and user consent privacy. Most apps upon installing. ask user consent whether to allow app to access camera, location, photos. call logs. One of the most prominent example of Individuals choose what to share is ride hailing or taxi apps like Indrive. If the rider or the user of the app wants to contact eachother without sharing their phone number. the indrive app facilitates the user and the rider with built in call where there is no need to share your personal number to call or text the rider of the app.

In addition to that data sharing has become the backbone of digital economy and modern services making technology indispensible in daily life. E-commerce Platforms for

Example, rely on customer data to provide personalized recommendations, manage inventory and process payment efficiently. similerly online banking and digital payment system needs access to sensitive financial information to authenticate users. detect fraud and enable secure transactions Hospitals also depends on patient records and real time health data to deliver accurate diagnoses and remote consultation without the smooth exchange and use of such data, these services would struggle to function. Digital banking also makes user convenience for example before 2026 the fee submission of CSS written exam was manual one had to go to a bank physically and submit it but no after 2025 it has been shifted to online banking through easypaisa Jazzcash or any mobile banking app, this shows how technology has made people life convinient without threatening their privacy.

Furthermore, Digital technologies have significantly improved governance and increased transparency in Public services. Digital record-keeping for instance, reduces opportunities for corruption by maintaing accurate, easily auditable records.

systems like NADRA in Pakiston allow for centralized management of citizen data, ensuring that services such as issuing identity cards or passports are more efficient and less prone to manipulation - E governance platforms also streamline administrative process, allowing citizens to access information, submit applications and track progress online without relying on intermediates.

Many experts argues that technology itself is not harmful it's neutral and that the risks to privacy arise primarily from human misuse. Tools such as smart phones, social media platforms and data analytics systems are designed to provide convenience efficiency and connectivity. problems occurs when individuals corporations or govt exploits these tools irresponsibly, such as collecting excessive data, ingnoring consent or using information for surveillence or manipulation. In this view it is not the technology that threatens privacy but the decisions and public awareness to prevent abuse

While Surveillance technologies are often praised for improving security, in reality they frequently cross the line into overreach, posing a serias thread to privacy. Tools such as CCTV cameras, facial recognition and digital tracking, which are intended to prevent crime, can easily be used to monitor citizens excessively and profile them without their consent. for instance E-challan System in Karachi which proved to be a good initiative to curb traffic violaters but at the same time it exposes the vehicle's owner identity without consent. the violator along with their car number plate circulates all over the social media and any one on social media can trace down the owner and his identity without consent and its alarming violating privacy of people. and it leads ~~to~~ citizens to ~~loose~~ lose anomity and autonomy when the state and corporations watches everything. Thus while surveillance aims to protect. It frequently undermines individual autonomy showing that technology designed for safety can simultaneously become a powerful thread to personal privacy

Sentence structure mistake

Although Platfurms advertise user consent and control over personal data ; in reality, this consent is often ineffectue. firstly lengthy and unending terms and conditions make it difficult for users to fully understand what they are agreeing to. In addition, apps commonly use dark patterns - designed techniques that subtly push users to share more informatiron than intended. furthurmore default settings typically favor data collection requiring users to opt out rather than opt in which many overlook As a result once data enters corporate servers Individuals loso meaningful control over how it is stored. shared or utilized. Even with privacy settings available, true autonomy is rarely guaranteed. consequently users often unknowingly expose sensitive information showing that consent mechanisms alone cannot safeguard privacy. This demonstrates that despite appearing to offer control, technology can still poss significant thread to personal data.

Argumentation is completely missing

furthermore debunking the essentional for Digital Banking and services, it is true although the digital economy relies on data and services like e-commerce, banking and telemediaince. In practice much of this data is exploited rather than simply used. for instance companies such as Meta Google. and TikTok monetize user behavior, preferences and even emotional responses to target audience and advertisments. Moreover data brokers frequently buy and sell personal information without transparency, leaving users unaware of who holds their data and how it is being utilized. in addition. algorithms designed to enhance user experience often prioritize engagement over privacy, subtly manipulating choices while harvesting sensitive information. thus while the digital economy provides valuable services the lack of regulation and ethical oversight turns data collection into a significant privacy threat.

Despite the claim that digital technologies improve governance and increase transparency. in practice these systems often create serious privacy risks for example centralized Data bases like NAdra can become targets for hackers, leading to mass data leaks furthermore well intentional e-governance platforms may store excessive personal information giving government or unauthorized individuals. the ability to monitor citizens. Thus improvents in efficiency and transparency must be balanced with robust safeguard to protect individual data from unintended exposure

Although algorithms AI and tracking tools are often presented as neutral technologies in realities they deliberatly designed to collect and exploit user data for instance cookies location tracking and personalized recommendation systems prioritized data harvesting over privacy. As a result personal information is continously monitored analyzed and monetize ~~limiting~~ Limiting individual control.

To conclude this essay, technology as it is currently designed and deployed, clearly poses a significant threat to personal privacy Surviellence systems, data harvesting algorithms and insufficiently regulated digital platforms allow government and corporations to collect, store and exploit sensitive data. However these risks do not mean technology must be rejected outright with ethical design strong legal framework and increased digital literacy among users it is possible to enjoy benefits of modern services