Day:_____ Date:_____

Topic:
Technology is a Threat to privacy.

Outline

I. Introduction

a) Hook

b) Define technology and privacy in contemporary society

c) Thesis statement

II. How Technology Threatens Privacy.

a) Social Media Apps Quietly Track Everything we Do.

* Reference: Apple's 2024 App Tracking Report revealed that 80% of apps tracked users even when tracking was turned off.

b) Free Wi-Fi and Apps Steal Data in exchange for "Free Services".

* Reference: Google Play removed 90* malware apps in 2024 for data Theft.

Day:_____ Date:_____

c) Location Tracking Threatens Physical Privacy and Safety.

* Reference: Google Location History Case (2023)

d) Deleted Data Never Fully Disappears.

* Reference: Meta Transparency Report 2024.

e) Data breaches leak sensitive Personal Information to Hackers.

* Reference: Pakistani telecom data leaked over 2.7million customers

III. Counterargument: Technology also Protects Privacy

a) End-to-end Encryption and Data Protection Laws (GDPR, Pakistan)

IV. Solutions to Protect Privacy in the Age of Technology

a) Strong data protection laws and ~~protection~~ enforcement

Day:_____ Date:_____

b) Global Cooperation against cross-border data abuse.

V. Conclusion

The Essay

"We are living in an age of surveillance, not an age of privacy."

—Edward Snowden

The digital age has connected our devices but disconnected our privacy. In contemporary society, technology is not confined to mere collection of devices, instead it is an ecosystem of interconnected digital structures that collects, processes, and transmits vast amount of data every moment. Privacy, in this environment, not only refers to physical boundaries but also to digital autonomy, protecting individual's personal information from unauthorized surveillance, tracking, and intrusion by

Day:_____ Date:_____

governments, corporations, or malicious actors. As technology has spread everywhere in our lives and interferes in each doing by humans, so it causes threat to human privacy. Modern technology has improved communication, healthcare, banking, and education, but it has also opened the door to privacy violations in human history. Every app we use, every website we visit, every location we pass, and even our conversations are quietly recorded, tracked and stored by companies and digital devices. Social media listens to our habit, smartphones gather our movements, and governments monitor online activity in the name of security. As a result, personal boundaries that once protected our private lives no longer exist in the digital world. Therefore, while technology has brought convenience and progress, it had also become a powerful threat to privacy that affects every individual in everday life.

To begin with, the biggest threat to

Day:_____ Date:_____

personal privacy comes from social media apps that quietly track people even when they are not using the apps. Facebook, Istagram, TikTok, and X constantly collect a user's location, contacts, browsing history, and even typing pattern in the background. As it is said:

"The surveillance state grows in silence."

-Glenn Greenwald

The quote is telling the truth. And, People always wonder why they suddenly see advertisements that perfectly match something they recently searched, talked about, or even thought about. This is due to real-time tracking, that has become so common that it now feels normal, even though it is a serious invasion of privacy. According to **Apple's App Tracking Transparency Report** (2024), almost 80% of apps continued tracking users despite tracking being turned off. Similarly, in 2023, **Meta** was fined €1.2 Billion by

Day:_____ Date:_____

the European Union for illegally transferring and storing user data. These examples show that social media platforms do not just connect people; they also quietly watch and record their everyday lives.

Furthermore, privacy is also threatened when people use free wiFi-networks and free mobile apps that secretly steal personal data in exchange for "free services". The following quote defines portrays true picture of free services as:

"If you are not paying for the product, you are the product!" (Andrew Lewis)

Many users, especially in Pakistan, download free VPNs, free wi-fi logins, video-downloader apps, photo editors, and cleaner tools without realizing that these apps often collect sensitive information such as contacts, photos, message logs, and even passwords. The promise of something "free" makes users ignore the hidden cost: their

Day:_____ Date:_____

own privacy. This concern is not theoretical. In 2024, Google Play removed more than 90 malware apps that had been downloaded by millions of people worldwide. Likewise, the Kapersky Cybersecurity Report warned that the majority of free VPNs contained spyware capable of tracking user activity. These reports show that free digital services often operate on a dangerous model - where the user unknowingly pays with their personal data instead of money.

In addition, another serious threat to privacy comes from location tracking, which can endanger both physical safety and personal freedom. Apps like Google Map and Uber or Careem (ride-hailing apps) silently logs exact location of a person, how much time he/she spent at a particular location, and complete travel history is stored in those apps. This data, though convenient for services like route suggestions, can be misused and a source of threat to individuals'

Day:_____ Date:_____

privacy. As Edward Snowden warned, "Arguing that you do not care about the right to privacy because you have nothing to hide is no different than saying you do not care about free speech because you have nothing to say." This emphasizes that privacy is a universal right, not a privilege. Many users feel safe, thinking that turning off location settings ensures security, but the **Google Location History Case** (2023) proved otherwise when the company was forced to pay $391 million for secretly tracking users even when the "location off" option was enabled. In simple words, people were "sleeping with one eye open", without realizing their movements were constantly monitored. The danger is subtle yet pervasive: every visit to a cafe, office, or park is recorded, creating a digital footprint that can be exploited for identity theft.

Moreover, the illusion that deleting

Day:_____ Date:_____

data removes it completely poses another serious threat to privacy. Many users believe that once they delete chats, emails, or photos, their information is gone forever. This is not true. As Bruce Schneier, a cybersecurity expert, aptly said, "Data is like water: it finds its way back, no matter how hard you try to block it." According to **Meta Transparency Report** (2024), deleted data may remain in "back-end systems" for up to 90 days or longer. Many tech companies often store multiple backups of the files on servers, meaning that deleted data can remain accessible for days, weeks, or even months. In this way, many users are living under a cloud of suspicion without realizing their data (deleted) can resurface at any time. This vulnerability is especially dangerous when sensitive information such as personal conversations, financial statements, or private images are recovered and misused. **Google's Data Retention Practices** provides a strong ground to tech companies to store data even

Day:_____ Date:_____

after users delete emails or files from Gmail or Drive: So, deletion does not guarantee complete data removal. Therefore, digital permanence makes privacy a fragile concept. In the digital era, deletion is rarely final, and true privacy requires vigilance and protective measures beyond mere deletion.

Finally, perhaps the most alarming threat to privacy comes from data breaches, which can expose highly sesitive information to hackers and cybercriminals. Over the past two years, banks, hospitals, telecom companies, and government databases such as NADRA have been repeatedly targeted. A stark example occurred in March 2024, when a Pakistani telecom company experienced a data leak affecting over **2.7 million customers**, exposing their private information to potential misuse. Globally, the 2023 **Data Breach Report** identifies identity theft as the fastest-growing cyber-crime. Once the information of the user

Day:_____ Date:_____

is compromised, the reversal is not possible, unlike changing a password. Many users are sitting ducks, as their personal data flows through digital networks, often without their knowledge or consent. The consequences of such breaches extend beyond financial loss- they can lead to blackmail, fraudulent identities, and long-term psychological stress. In a world dominated by technology, data breaches make privacy one of the most fragile aspects of modern life. It highlights the urgent need for stricter security protocols, user awareness, and regulatory oversight.

Admittedly, technology has also introduced several tools and legal frameworks aimed at protecting privacy. End-to-end Encryption in messagin apps like whatsApp and Signal ensures that only the sender and recipient can read the messages, making unauthorized access difficult. Similarly, data protection laws such as the EU's GDPR and Pakistan's Personal Data Protection Act

Day:_____ Date:_____

(PDPA 2023), provide a regulatory mechanism that increase transparency and give users control over their personal information. The developments like public awareness seminars, digital literacy webinars, and app permissions suggest that technology does not solely compromise privacy. Many tech-savvy individuals now cover their tracks by adjusting privacy settings and using encrypted options. However, while these measures are helpful, they only address the part of the problem. As Bruce Schneier notes, 'Privacy is not an absolute right, it is a continuous struggle', showing that sophisticated tracking, large-scale data collection, and breaches still occur even after the protection and legal framework. End-to-end encryption cannot protect meta data, cloud backup remain vulnerable, and legislation enforcement in developing countries like Pakistan is still weak. Thus, although technology provides tools for privacy protection, these safeguards are not enough to neutralize the pervasive threats. Privacy continues to be at risk, and

Day:_____ Date:_____

proactive measures at the personal, corporate, and governmental level remain crucial.

Consequently, addressing the threats posed by technology requires strong, proactive measures to safeguard personal privacy. One of the most effective solutions is the **enactment** and **enforcement** of the **dat protection laws** - modeled on frameworks like the European Union's GDPR. Countries such as Germany, France, and the Netherlands have established independent data protection authorities to ensure companies adhere to privacy regulations. The most recent example of Australia banning children under 13 from accessing social media platforms is a case in point. In addition to legal safeguards, governments and corporations must adopt a "privacy by design" approach. In this way, the security features will directly integrate into the apps, websites, and digital services - rather than treating privacy as afterthought. Users, too, play a crucial role by enabling strong

Day:_____ Date:_____

passwords, using two-factor authentication, and limiting unnecessary permissions such as "Accept all cookies" on websites. The digital world is a double-edged sword, offering convenience while constantly threatening privacy. Thus, a combination of legal frameworks, informed users, and technological safeguards is essential to defend privacy in the age of technology.

Moreover, protecting privacy in the digital age requires strong international cooperation because digital data does not respect national borders. When data travels across countries, local laws become insufficient. This is why nations must work together to build global privacy standards and international norms against data exploitation. The European Union GDPR has already set a global benchmark, influencing over 40 countries - including Japan, Brazil, South Korea, and South Africa. International Organizations such as United Nations, OECD, and ITU have repeatedly

Day:_____ Date:_____

stressed the need for cross-border cooperation. For example, the EU-US Data Privacy Framework (2023) was created to regulate how American tech companies handle European citizens data and to prevent misuse. Likewise, countries in ASEAN region launched a shared data protection model in 2024 to harmonize privacy rules across Southeast Asia. These steps reflect the idea that "privacy is a global public good", meaning every nation must help protect it. Yet, international cooperation often moves at a snail's pace, while technology evolves at lightning speed. Somehow, strengthening of international norms is essential to safeguard privacy in a world where data flows endlessly across borders.

In conclusion, it is evident that technology, despite its countless benefits, has created an environment where personal privacy is constantly at risk. From social media surveillance and hidden data tracking to location monitoring, data breaches, and the

Day:_____ Date:_____

permanent storage of deleted information, the threats are real and deeply embedded in everyday life. Although encryption tools, improved laws, and growing digital literacy offer some protection, they cannot fully encounter the problem that technology is posing. The truth is that, modern technology operates like a silent intruder, entering our lives unnoticed and staying far longer than we intend. Yet, this crisis is not irreversible. As society becomes more dependent on technology, safeguarding privacy must become a shared responsibility- one that governments, corporations, and individuals undertake with seriousness and consistency. The path forward demands vigilance, ethical innovation, and international unity. If these efforts continue, humanity can ensure that technology remains a tool for progress rather than a gateway to deeper surveillance.