good use of transitions between paragraphs Rabia 96

score : 41/100

Date:__/__/20__

MON TUE WED THS FRI SAT

add more threats to outline

ESSAY

TECHNOLOGY IS A THREAT TO PRIVACY

OUTLINE

INTRODUCTION

1.1 : HOOK

1.2 Background

1.3 Thesis.

2. HOW TECHNOLOGY IS A THREAT TO PRIVACY

2.1 Data harvesting as a threat to privacy

2.1.1 Social media platforms

2.1.2 Mobile app permissions.

2.2 Exploitation of user data by corporations

2.2.1 Sale of data to third party

2.2.2 Banking and financial threats

Date:___/___/20___

MON TUE WED THS FRI SAT

2.3 Government Surveillance poses a huge threat to individuals right to privacy.

2.3.1 Tracking via CCTV, facial recognition.

2.3.2 Suppression of dissent

Case in point - China Israel.

2.4 Social media personalities

2.4.1 Platforms pack every like share

2.5 Generative AI threat to Women

2.5.1 AI can create deepfakes

Case in point: Yalda Hakim

2.6 Cybersecurity and data breaches

2.6.1 Databases vulnerable to hacking and ransomware.

2.6.2 Identity theft

Date:__/__/20__

MON TUE WED THS FRI SAT

27 Uses Regulations - lead to privacy issues

laws have not kept pace with tech

2nd 3. Counter Arguments

Technology offers immerse benefits:

personalization, connection.

Conclusion

Final

Date:__/__/20__

MON TUE WED THS FRI SAT

Introduction.

We have never been more connected, yet never more exposed. An age that is marked by constant connection, sharing and information exchange is upon us. Every age, albeit, brings with it its own peril. As people get more interconnected, they also become more vulnerable to the threat of privacy invasion. Every online search, location share, biometric scan or social media interaction becomes a data point at which your information is collected and analysed. From social media companies to advertising agencies, from corporations to state surveillance agencies, the line between connection and surveillance is growing dangerously thin. As such technology has become an omniscient observer of people's lives, in the hands of the wrong people. Not only do the social media data collection and state surveillance

Date:__/__/20__

MON TUE WED THS FRI SAT

pose a risk to an individuals privacy, but it also runs the risk of sharing that data with third parties, thereby putting individuals at the mercy of cybersecurity sharks. Moreover, as Cambridge Analytica scandal proved, data breaches can even be wielded as a sword to threaten democratic norms. With the advent of AI, Generative AI tools and IOT devices can be used ~~to~~ bring harm on people. In the face of such rapid technological change, it is not only pertinent to understand the challenges technology poses to privacy, but also work towards mitigating these risks.

To begin with, data harvestation has become one of the most pervasive threats to personal privacy. shopping Websites, social media websites and others collect enormous amounts of data on an individual to gage their preferences. Users, unaware of the

Date:__/__/20__

MON TUE WED THS FRI SAT

implications share their data. Moreover, in-built and specifically third party apps ask for unnecessary permissions to access individuals private data. All of this data, be it of financial nature, healthcare, political preference general likes and dislikes and psychological nature is used for profiling by corporations. These profiles are then shared with advertising agencies, posing an even greater risk to their privacy. As such, data harvestation leaves users vulnerable to surveillance and manipulation for the benefit of corporations.

Beyond the passive collection of information, corporations actively exploit user data in ways that pose serious threats to privacy, including with the banking and financial sectors. Tech companies routinely track online behaviour. Every click, search, purchase and pause, turn personal habits into a commodity

Date:__/__/20__

MON TUE WED THS FRI SAT

is recorded. This data is often shared with financial institutions. Moreover, banks themselves collect vast amounts of sensitive data, from transaction histories to biometric authentication, which if mishandled or breached can expose individuals to identity theft, financial fraud and long term economic harm. Since corporate and financial databases have become lucrative targets for hackers and breaches, ... individuals become more at risk of financial exploitation and security risks.

In addition to corporations collecting data, government surveillance poses an threat to the privacy of individuals. The nature of state syevellance is often invisible. States often use facial recognition, biometric scans, CCTV's and heat maps to track citizens movements or behaviours. China is one such example. While the chinese government claims to use these mass-surveillance systems

Date:___/___/20___

MON TUE WED THS FRI SAT

for law and order. It is often criticized for doing so at the cost of its citizens privacy. Israel, similarly uses AI tools like Lavender and Red wolf to identify threats. Not only are these technologies used to monitor activity, but they are also used to suppress dissent. As such, the average persons freedom and privacy are increasingly compromised. raises questions about the balance between security and individual rights.

The Cambridge Analytica scandal exposed how data collection can directly threaten democratic processes and allow private entities to gain disproportionate power over collective decision making. By harvesting personal data from millions of social media users without consent, the firm built detailed psychological profiles to target individuals with tailored political advertisements during elections. This manipulation exploited users behavioural patterns, beliefs and emotional triggers, shaping opinions and

Date:__/__/20__

MON TUE WED THS FRI SAT

influencing voting behaviours in ways that would neither transparent nor accountable. Such practices demonstrate that when personal data falls into the wrong hands, it can be weaponized to distort public discourse, polarize societies and undermine the integrity of democratic institutions. In the hands of a few elites, technological tools are used to give unprecedented decision making authority to individuals at the cost of peoples privacy. Social media has become one of the most insidious threats to privacy. Constant sharing on social media platforms of every personal detail leaves us vulnerable to identity theft, phishing and fraud. Moreover, thefs and stalkers can get access to your live activities, thereby ascertaining an individuals location. In addition to that, every post, like comment-or share generates data that is tracked stored and analyzed to expose personal routines

Date:__/__/20__

MON TUE WED THS FRI SAT

relationships and sensitive habits. As such, platforms that are used for self-expression and connection are exploited by bad faith actors.

While generative AI promises innovation, it also introduces new threats to women's privacy. AI-powered tools can create deepfakes and fabricate videos to target women disproportionately for harassment and exploitation.

In the past week, a renowned journalist, Yalda Hakim, was subjected to deep-fake controversy. An interview of her with Imran Khan's sister went viral when turned out be a deepfake clip.

Online platforms can amplify these abuses, spreading manipulated content rapidly and making it difficult for victims to regain control over their digital personas. It is crucial to mitigate these gendered risks; ensuring technological progress doesn't disproportionately compromise the rights and safety of women

Date:__/__/20__

MON TUE WED THS FRI SAT

Even the most carefully collected data is vulnerable to data breaches, making cybersecurity a critical aspect of the privacy issue. Hackers target corporate, government and financial databases to steal sensitive information including login credentials. Weak encryption, outdated softwares and inadequate security protocols often compound these risks. Furthermore, cyberattacks are no longer limited to theft, ransomware and data manipulation threaten both individuals and organizations.

The rapid advancements of technology has far outpaced the development of regulatory frameworks creating significant gaps that threaten privacy. Lax and weak regulations fail to hold corporations/platforms even governments accountable for the collection storage and use of personal data. Europe's AI regulation Act is the first of its kind to keep a

Date:___/___/20___

MON TUE WED THS FRI SAT

a check on companies for privacy. Not many have followed suit. The absence of clear, enforceable rules allows harmful practices to go unchecked. Consequently, individuals are kept exposed.

While technology undeniably poses privacy risks, it is important to acknowledge its immense benefits and the arguments often made in its defense. Proponents argue that digital tools and AI-driven platforms enhance efficiency and access to information, improving quality of life in healthcare, education, business and communication. Personalization in algorithms has helped cater better to every individual's taste. Moreover, an argument could also be made for technological innovations that strengthens privacy such as better encryption. However, a technology is only as good as the people it is employed by. In the absence of responsible governance, ethical design and user awareness, modern technologies carry more risk than reward in the current era.

Date:__/__/20__

MON TUE WED THS FRI SAT

Conclusion

In the digital age technology has transformed the way we live, work and communicate, yet this process comes with profound threats to personal privacy. From mass data collection to financial exploitation, from government surveillance to the hijacking of democracy, individuals are increasingly exposed to unprecedented levels of monitoring. Social media pervasiveness and weak regulation exacerbate these risks.

Although proponents argue that technology offers immense benefits, the current reality paints a different picture. Ultimately, technology is neither inherently good nor bad, it reflects the intentions, ethics and responsibility of the humans who employ it. By combining accountability with technological innovation, however, society can harness technology to protect privacy