

Required Coversheet

INFO30006 Group Assignment #2 Group Submission

Paper Title: Is Privacy Dead? – A technical evaluation on the methods and tools that destroy and protect privacy.

Group Name: Team Macro Hard

Student Names and Student Numbers:

Albert Dong	1269104
Eugene Yap	1353623
Andi Yan	1182512
Zac Davidson	1353326

Tutorial Day and Time: Tuesday 11:00AM

Tutor: Isaac Morris

Word Count (maximum 4000 words, with a 10% margin): 4100

Topic Selection: 'Privacy is dead'. Evaluate technical methods that destroy privacy against those that protect it to assess the accuracy of this claim.

We confirm this report layout is one-inch margins, in at least 12-point font, as a .pdf. The title page, abstract (half page or less), the references which are listed at the end, and the Table of Contents are not included in the word count.

Yes ☒

No ☐

We agree as a group that our paper and slides can be used in future teaching at the University as an example of an excellent assignment essay:

Yes ☒

No ☐

CONTENTS

CONTENTS.....	1
INTRODUCTION.....	2
BACKGROUND.....	2
ANALYSIS.....	2
1.1 What has changed technologically in the last decade that impacts privacy?.....	2
2.1 State of the art PETs their impact on surveillance technologies.....	4
3.1 The Technical Battle Between Privacy and Surveillance.....	6
4.1 An insight on the future of AI Tools and Methods.....	8
DISCUSSION.....	9
1.2 What has changed technologically in the last decade that impacts privacy?.....	9
2.2 Are modern PETs sufficient enough to offset the impact of surveillance technology?.....	11
3.2 What is the overall trajectory of the battle between privacy and surveillance technologies?.....	11
4.2 What is the future relationship between AI and Privacy?.....	13
REFERENCE LIST.....	15

INTRODUCTION

There have been growing concerns surrounding the security of privacy in the technological space. According to a study conducted by The International Association of Privacy Professionals (IAPP), 68% of consumers worldwide are concerned or very concerned about their privacy on the Internet (Manjarres, 2024). Despite the advent of privacy enhancing technologies that seek to protect privacy, there are still vulnerabilities in certain contexts. So while privacy is not “dead”, it is not completely protected either, and there is currently a back and forth between the attackers and defenders of privacy. This report will provide a comprehensive overview of whether privacy can be preserved in an increasingly monitored digital age.

BACKGROUND

In light of rapid digital advancements in data collection, storage and analysis capabilities, widespread surveillance has caused calls of concerns for privacy enhancing technologies PETs to make significant advancements in protecting the privacy of individuals to which their sensitive information is used for training machine learning ML models (Soykan, E.U., et al., 2022). Differential privacy and homomorphic encryption HE stand as two of the best methods of preventing membership inference attacks and exposing sensitive data. In addition, transport layer security TLS is also one of the best methods to prevent adversarial interference and secure email privacy (Kisselburgh & Beever, 2022). The technical battle between advancements in PETs and surveillance technologies is arduous and constantly evolving, where surveillance capabilities and data storage are growing at alarming rates. Whilst there are several tools and methods helpful in shaping a secure and private future in AI such as data minimisation and federated learning, PETs alone are not sufficient enough to completely uphold individual privacy rights.

ANALYSIS

1.1 What has changed technologically in the last decade that impacts privacy?♥

Privacy is not dead, however, there are contexts in which effective privacy is not upheld. This is exemplified when sending sensitive information via emails.

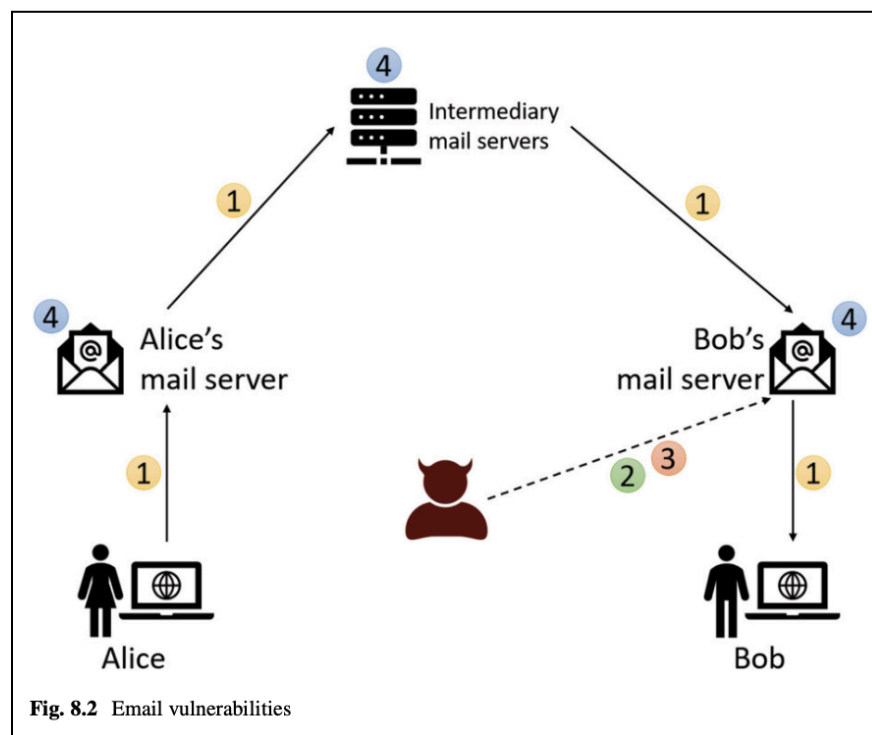



Figure 1: Email vulnerabilities including (1) unsecured links, (2) message forgeries, (3) malicious content, and (4) untrusted servers (Kisselburgh & Beever, 2022).


When emails were originally designed, security was an afterthought. The lack of encryption meant that emails containing private information were vulnerable to eavesdroppers while in transit and sensitive messages stored in the server were also susceptible to unauthorised access.

These emails are usually stored indefinitely, and this long-term storage presents privacy risks even if the data is compromised well in the future (Kisselburgh & Beever, 2022). 

There are technologies that have been utilised to counteract some of these threats to privacy when using emails (Clark, van Oorschot, Ruoti, Seamons, & Zappala, 2018). These include “transport layer security (TLS) encrypted email messages during transmission between communication links, sender policy framework (SPF) that lets the domain owner specify the legitimate servers that send email messages for that domain and domain keys identified mail (DKIM) which includes a signature on each email message from a domain to guard against message forgery” (Kisselburgh & Beever, 2022).

Recent studies show that these techniques are not universally implemented, leaving a significant vulnerability in the secure email infrastructure (Foster, Larson, Masich, Snoeren, Savage, & Levchenko, 2015). Even if these vulnerabilities are dealt with, servers still have access to plaintext emails, and the threat of disclosure to hackers or government surveillance remains (Kisselburgh & Beever, 2022). So while there are privacy enhancing techniques in place to protect privacy, it is not completely effective as there are still scenarios where sensitive information may be vulnerable.

2.1 State of the art PETs their impact on surveillance technologies

Although methods such as differential privacy are ineffective at preventing large entities to gather attributes unique to the individual, PETs are still irreplaceable in the surveillance landscape and still offer security over individual privacy rights. 

Customer data is constantly being extracted and used as part of collaborative ML training. With the landscape of ML becoming increasingly complex, even to the stage of multiple parties collaborating to train on the same models, sensitive information pertaining to innocent individuals also become increasingly vulnerable to threats and attacks.

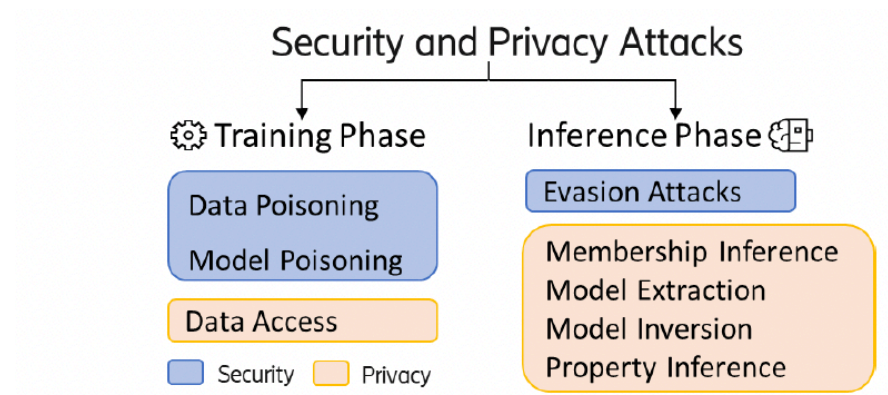


FIGURE 2. Classification of Security and Privacy attacks.

Figure 2: Potential security and privacy attacks on ML models (Soykan, E.U., et al., 2022).

One of the most common and potent attacks to threaten individual privacy are membership inference attacks. According to Soykan et al., membership inference attacks are a complex method of inferring whether a specific record belongs to a ML training dataset. Adversarial attacks alter gradient values, which are vectors that determine magnitude of adjustment to minimise loss, on interested data points. If the modification to these data points result in a significant reduction in the gradients queried from other participants, then adversaries can reasonably assume membership and extract that information.

The most notable methods and tools that have been developed to protect the security and privacy of sensitive information from threats like membership inference attacks are differential privacy (DP) and homomorphic encryption (HE).

Differential privacy (DP) is a statistical method in which the ML algorithm introduces a mathematical white noise to the individual data points to hide any revealing information about the model parameters in the ML model. While the statistical properties of the data do not change, it still prevents any specific individual to be identified from any data point. The sampling distribution of the noise can be calculated in various ways, but the most popular is using a Gaussian distribution. A specific application of DP is central DP which can be represented as:

$$M(D) = f(D) + N(0, \sigma^2)$$

Figure 3: Formula for algorithm to satisfy Central Differential Privacy (Soykan, E.U., et al., 2022).

Where randomised algorithm M on dataset D satisfies differential privacy if the Gaussian distribution is applied to the query function f . Soykan, et al. concludes that both applications of differential privacy, central DP and local DP, can prevent malicious membership inference attacks, with a trade-off to the accuracy of the model.

Homomorphic encryption (HE) allows computation on ciphertexts without access to the secret key or need for decryption (Soykan, E.U., et al., 2022). Algebraic algorithms in the HE systems allow functions to be performed directly onto the encrypted data, and decrypted results look as if

the functions were performed over plain text. There are different HE classes for different encryption requirements: partial, somewhat and fully. However, to utilise HE systems, parties must organise beforehand to distribute keys beforehand to decrypt the results, and it could be extremely computationally intensive. 🚩

In addition, (Him, H., et al., 2020) the advancement in intelligent cloud-based CCTV surveillance technologies and video analysis technology have increased concerns surrounding individual rights to privacy in public areas. Therefore, the importance of video anonymisation grows each passing day. Video anonymisation contains multiple different classic techniques, such as blurring, mosaicking, cutting out and covering (DAminio, et al., 2012).

Modern day surveillance footage also encrypts these regions of interest (ROI) and stores it alongside the video stream itself. This allows for the sensitive information to pass through networks without the threat of adversarial interference. However, there is also an element of trust that public and private owners of CCTV cameras will protect the privacy of individuals through these methods.

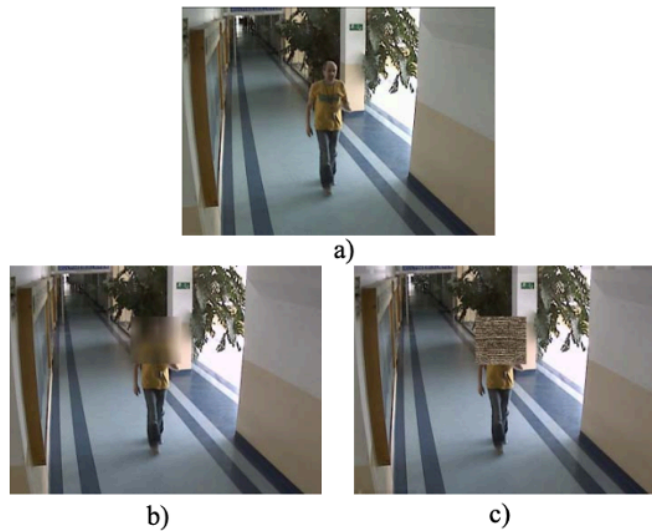


Figure 4: a) original footage, b) anonymised blurring, c) anonymised cutting (Darminio, et al., 2012).

3.1 The Technical Battle Between Privacy and Surveillance

Surveillance technologies have become increasingly sophisticated, driven by improvements in data collection and machine learning. Governments and corporations deploy a range of tools to gather vast amounts of personal data, often without individuals' direct knowledge or consent. These technologies are pervasive, and their sheer scale presents a significant challenge to individual privacy:

Surveillance systems thrive on the ability to collect enormous volumes of data, which are analysed using machine learning algorithms to derive insights and predictions. The scope of this data collection has expanded beyond mere web tracking (e.g., cookies and fingerprinting) to include mobile data, social media interactions, and even biometric information (Zuboff, 2019). This mass collection allows organisations to construct detailed behavioural profiles of individuals, offering unprecedented precision in predictive analytics. The capabilities of these

technologies enable a form of surveillance capitalism where privacy is commodified and sold, often at the cost of informed consent.

The proliferation of **facial recognition technology** in public spaces introduces a new level of surveillance. These systems, often coupled with AI-powered biometric databases, make real-time identification of individuals feasible, thereby removing any semblance of anonymity in public spaces (Sanchez-Monedero & Dencik, 2020). From a privacy perspective, this represents a significant threat as it allows for continuous monitoring without individuals being aware or able to opt out. The scalability of biometric surveillance, particularly when linked to broader state-level databases, makes it increasingly difficult for PETs to counteract its impact. ▼

Cross-device tracking, enabled by techniques like browser fingerprinting and device matching, has further weakened traditional anonymization methods. Users' online activities across various platforms and devices are linked to form a comprehensive profile, circumventing privacy defences such as VPNs or incognito browsing (Narayanan & Shmatikov, 2010). Even anonymized data sets, once thought to offer some level of privacy, are increasingly re-identified through data aggregation techniques, rendering them ineffective.

A number of privacy-enhancing technologies (PETs) can be used to counter these surveillance mechanisms. These technologies aim to protect personal data and user privacy, even in hostile surveillance environments. However, while promising, their effectiveness and accessibility are subject to several limitations. ▼

End-to-end encryption (E2EE) remains one of the most effective means of securing communications from unauthorised access. Apps like **Signal** and **WhatsApp** use encryption to ensure that only the intended recipients can read the messages (Green & Miers, 2015). However,

the growing pressure from governments worldwide to create "backdoors" into encrypted communications, under the guise of law enforcement or national security, poses a direct threat to encryption's integrity (Abelson et al., 2015). If governments succeed in mandating backdoors, encryption as a defence mechanism could be substantially weakened, exposing private communications to mass surveillance.

However, the efficacy of anonymization is not absolute in techniques like **differential privacy**. Studies have shown that with enough auxiliary data, even anonymized datasets can be reverse-engineered to re-identify individuals (Narayanan & Shmatikov, 2010). This undermines the argument that anonymization alone is sufficient to safeguard privacy in the face of advanced re-identification techniques. It also has its advantages, the Australian healthcare sector is already starting to recognise the importance of its application, with one of the first uses being linked to the development of the COVID-19 Real-Time Information System for Preparedness and Epidemic Response (CRISPER). CRISPER's interactive mapping tool allows users to interrogate data based on time *and* place *and* source of infection, and answer questions specific to their information needs. (Dyda, et.al). This highlights the need for a multi-layered approach to data privacy, where anonymisation can be complemented with other techniques to ensure comprehensive protection.

Tools like **Tor** and **VPNs** allow users to mask their IP addresses and encrypt their internet traffic, offering significant protection from web-based tracking. However, advanced surveillance techniques like browser fingerprinting and data aggregation can sometimes defeat these measures (Pugliese et al., 2021). This raises the question of whether even the most widely adopted PETs can keep pace with the sophistication of surveillance technologies. While Tor and

VPNs offer valuable privacy protections, they are often vulnerable to state-level actors or well-resourced corporations with access to more advanced tracking mechanisms.

Despite these technological advancements, PETs remain difficult for the average user to implement effectively. Encryption, anonymization, and tools like Tor require a certain level of technical expertise, meaning that while these solutions exist, they often remain inaccessible to the broader public. Furthermore, the widespread adoption of PETs is essential for their effectiveness; for instance, encryption only works if both parties in a communication use it consistently. Similarly, without a critical mass of users adopting tools like Tor, individual users may stand out as anomalies, making them easier to track.

While privacy-enhancing technologies offer powerful defences, their success is limited by usability, technical complexity, and scalability. In contrast, surveillance technologies are often passive, seamless, and pervasive—integrated into everyday systems that require no effort from the surveillance. Therefore, the balance between privacy and surveillance heavily favours the latter, particularly when considering the structural, legal, and resource advantages that governments and corporations hold in the realm of data collection and analysis.

4.1 An insight on the future of AI Tools and Methods

A shift towards **Data Minimisation** is highly encouraged to counter the exponential growing trend to gather as much data as possible, especially through online services and large technology companies. As one of the seven principles of the GDPR, as stated in Article 5(1)(c) of the GDPR which says that personal data shall be: “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)” (ICO, 2023).

With data breaches becoming more common, the risk of storing vast amounts of personal information is significant. Collecting only the minimum necessary data can help mitigate these risks and reduce the potential harm in case of unauthorised access. AI systems then can be adapted to be computationally and more memory efficient using this limited data.

Federated learning is a machine learning technique that trains an algorithm across multiple decentralised edge devices or servers holding local data samples, without exchanging them. With the decentralisation of servers, users can also achieve data minimization by reducing the amount of data that must be retained on a centralised server or in cloud storage. (Anand, 2019)

Federated learning can then be utilised to further enhance privacy minimising the need for large-scale transfers. Furthermore, the sense of trust and security between consumers and business can further strengthen and this would ultimately lead to wide implementation of healthy practices in a future where privacy is a major concern.

DISCUSSION

1.2 What has changed technologically in the last decade that impacts privacy?

In the last decade, technology has rapidly advanced and many of these changes have impacted the privacy of its users. This advancement in commercial online technology has led to more threats to privacy than ever before, and with this proliferation of privacy threats there has been a calling for more and more privacy enhancing technologies to fight back against these threats and protect its users to ensure that privacy is not dead.

One of the biggest changes that has impacted privacy is the advent of social media. There are more people using social media now than ever before and as such, there has never been a greater amount of personal information pervading the internet. More personal information online has led to more attackers who threaten the privacy of online users and this has called for increasing amounts of privacy enhancing technologies to protect personal information.

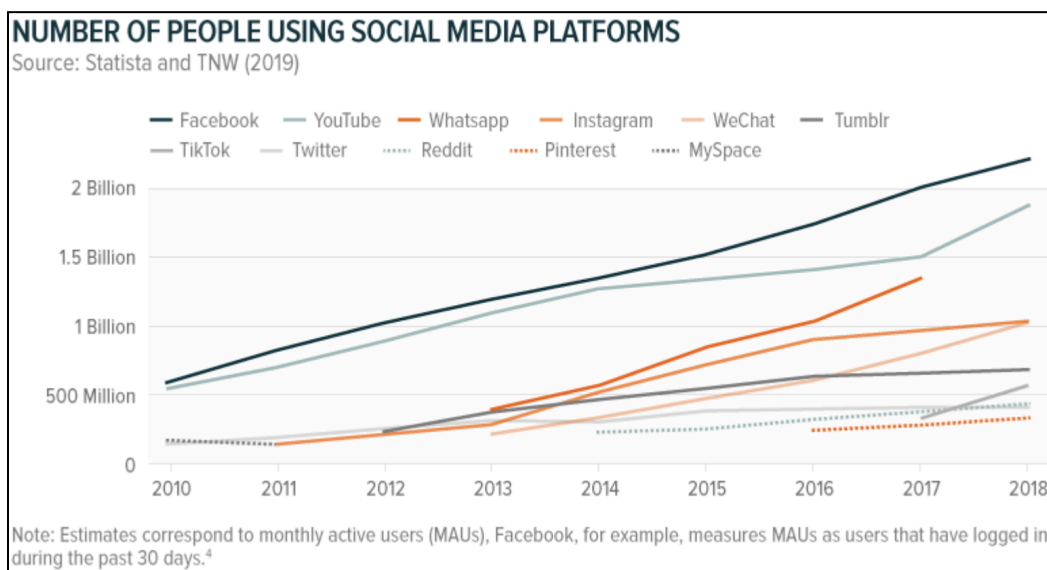


Figure 5: The number of people using social media platforms (Palandrani, 2020).

The question remains as to why social media has exploded in popularity in the way that it has, from a technological point of view. One of the reasons for this social media boom is the introduction of 4G networks. Mobiles upgrading from 3G to 4G networks benefitted many industries including smartphone manufacturers, social media, e-commerce and streaming media (Palandrani, 2020), and as these industries grew, more resources were invested into the online experience for users. Faster internet speeds, more and more digital devices, improved app

functionalities and increasingly accessible communication pathways all proliferated the amount of users online. This rise in the number of users has led to more and more concerns surrounding companies having unwarranted access to personal user information.

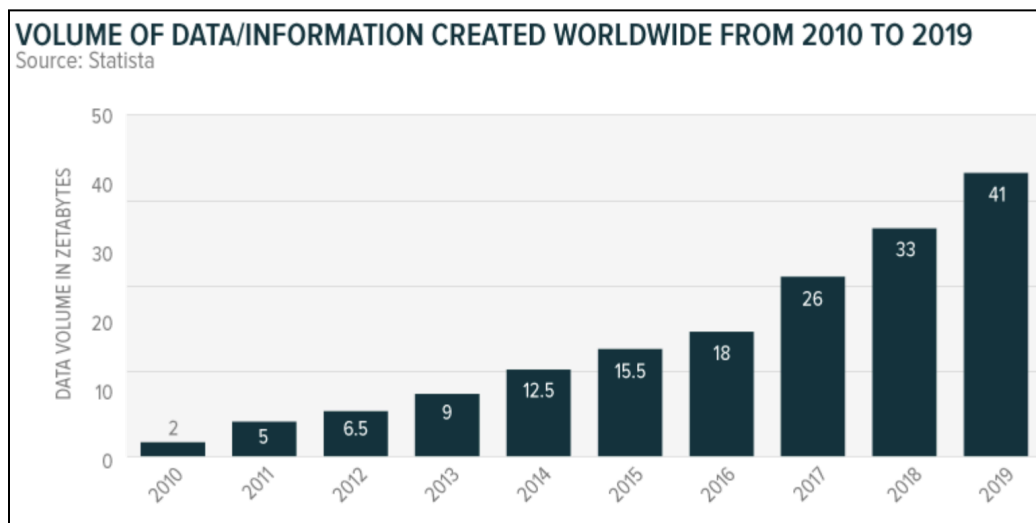


Figure 6: The volume of data/information created worldwide from 2010 to 2019 (Paladrani, 2020).

In the last decade, the scale of big data has increased significantly. Companies have tried to exploit this abundance of data by collecting, processing and analysing it to optimise business decisions and maximise profits. Personal information is used by companies to create targeted ads for users and improve recommendation systems that are specific to the user. The many benefits that this mass amount of personal information provides to businesses comes at the cost of user privacy, as it becomes increasingly at risk as businesses pursue more and more amounts of information, sometimes without the consent of the user. Various technological changes have been a factor in this boom of data generation. Improved cloud computing being one of the major reasons, as it has eliminated the need for physical infrastructure to store large amounts of data. It also granted global accessibility to businesses and users, allowing them to collaborate with

anyone around the world and work remotely. Another reason as to why big data has scaled so significantly is simply due to the improvements in physical hardware, with increases in computing power allowing for efficient data storage and processing. Furthermore, with technology being more reliant on ML/AI, the demand for large datasets that improve the accuracy and efficiency of these models has never been greater. All the aforementioned technological advancements have culminated to surge the volume of data being generated online.

In response to the amount of personal information that is being threatened by attackers, companies, and governments alike, privacy enhancing technologies (PETs) have been developed in the last decade to counteract these threats. The new protective technologies that have emerged include secure messaging, secure email, HTTPS, two-factor authentication and anonymous communication (Kisselburgh & Beever, 2022). These PETs were created to ensure that privacy of users is upheld, however, with so many new threats arising daily, the back and forth between attackers and defenders is constantly ongoing, and as much as these PETs help to protect users, new and innovative technologies that threaten privacy are emerging just as quickly as these PETs are.



2.2 Are modern PETs sufficient enough to offset the impact of surveillance technology?

State of the art privacy enhancing technologies (PETs) today may be able to offset the impact of CCTV surveillance technologies, however we cannot fully rely on it to protect users from being profiled by large organisations. As technically impressive and effective DP and HE are, the substantial computational requirements, as well as its futility against large organisations that

collect and collate big data to build profiles of individuals. Whilst CCTV surveillance may currently have sufficient encryption and measures to protect sensitive information pertaining innocent individuals, data stores and resource utilisation still exceeds a sustainable amount. While sufficient for protecting against adversarial and honest-but-curious attacks, PETs cannot prevent government agencies from ordering internet providers to have a wiretap and control interface architecturally built into their network services (Bellovin, S.M., et al., 2016). Therefore, advanced PETs including DP and HE are capable of defending against adversarial attacks, however government surveillance may be impervious as they could request wiretapping be built into the network services themselves. ▼

3.2 What is the overall trajectory of the battle between privacy and surveillance technologies?

The claim that “privacy is dead” reflects the growing ubiquity of surveillance technologies, but it is not entirely accurate. While surveillance technologies have certainly outpaced many privacy defences, privacy-enhancing technologies (PETs) remain robust. ▼

On the surveillance side, the ability of governments and corporations to collect, store, and analyse vast quantities of personal data suggests that privacy is under greater threat than ever before. **Big data analytics**, powered by artificial intelligence, makes it possible to analyse personal information at scale and identify patterns or behaviours that would otherwise remain hidden (Zuboff, 2019). Similarly, **facial recognition** and **biometric surveillance** systems allow for real-time identification and tracking of individuals, effectively diminishing the anonymity once afforded in public spaces (Introna & Wood, 2004).

The rapid development of high-resolution surveillance cameras has significantly enhanced the accuracy and effectiveness of facial recognition systems. Modern surveillance cameras now capture video in resolutions such as 4K and beyond, allowing for clearer, more detailed images. This higher resolution enables facial recognition algorithms to work with more precise data, improving the ability to identify individuals even in challenging conditions such as poor lighting, crowded spaces, or long distances.

The increasing deployment of high-resolution cameras enables more effective facial recognition in real-time. As the resolution improves, algorithms can detect finer facial details, making it easier to identify and track individuals across various locations. This development represents a critical advancement for law enforcement and corporate surveillance but poses significant privacy concerns, as the ability to remain anonymous in public spaces becomes increasingly difficult. (IPVM, 2021)

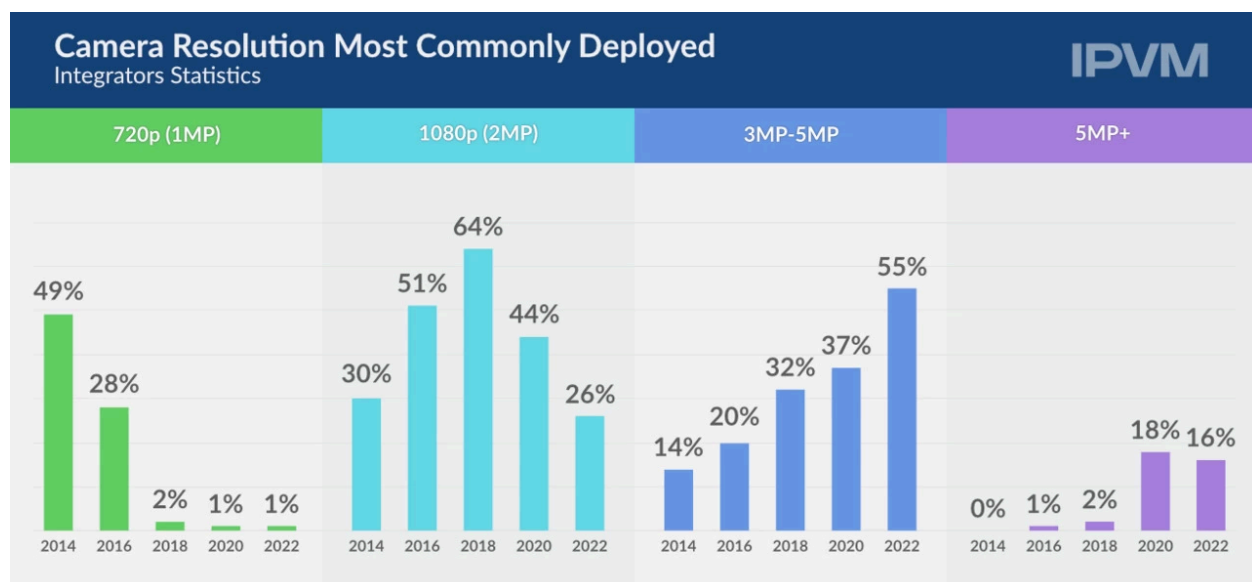


Figure 7: Statistics on camera resolutions deployed (IPVM,2021)

As PETs continue to develop in response to these challenges. **End-to-end encryption** remains one of the strongest technical safeguards against surveillance. Modern cryptographic techniques, like **homomorphic encryption** and **zero-knowledge proofs**, offer promising advancements in preserving privacy while still allowing for data computation and verification (Gentry, 2009). These methods could enable privacy-preserving transactions, voting systems, and other sensitive operations in the future.

One key challenge is the **widespread usability and adoption of PETs**. Encryption is effective, but only if users employ it correctly, and its widespread use is hindered by concerns over usability and convenience (Abelson et al., 2015). Similarly, technologies like **Tor** and **VPNs** offer significant protection but are not immune to advanced tracking techniques, such as **browser fingerprinting** (Pugliese et al., 2021). Additionally, **state-level actors** increasingly push for weakened encryption or backdoors in encryption technologies, further undermining privacy efforts (Abelson et al., 2015).

An effective measure is limiting the sharing of personal data in everyday activities. For instance, individuals can opt out of **loyalty programs** or use alternative payment methods like cash to avoid the accumulation of purchase history and personalised profiling (Clarke, 2020) Disabling location services and Bluetooth on smartphones also helps reduce the risk of location-based tracking via Wi-Fi beacons or mobile apps (Narayanan & Shmatikov, 2010).

Regulatory frameworks, such as **GDPR** in Europe offer a partial solution by limiting corporate data collection practices and ensuring greater transparency (Voigt & von dem Bussche, 2017). However, such regulations are geographically limited and often difficult to enforce on a global

scale. Since AI development is progressively changing, these regulations will likely impose heavier restrictions on how AI can process sensitive data and contain user control over data usage. This is especially important in high-risk AI systems that include law enforcement, healthcare and critical government infrastructure. This legislative effort seeks to put forths guidelines to protect privacy and foster transparency. Moreover, many users continue to prioritise convenience over privacy, willingly sharing personal information in exchange for services, further weakening the effectiveness of PETs.

In conclusion, privacy is not entirely dead, but it faces significant challenges. Surveillance technologies continue to advance rapidly, often outpacing the development and adoption of privacy-enhancing solutions. Yet, PETs are constantly evolving and with proper implementation and broader public awareness, they can provide meaningful protection against many forms of surveillance. Whether privacy will survive in the long term depends on technological innovations, regulatory frameworks and a shift in user behaviour toward prioritising privacy over convenience.

4.2 What is the future relationship between AI and Privacy?

The future relationship between AI and Privacy evolves in a challenging yet collaborative nature as it becomes more integrated into everyday life. Balancing innovation with the protection of individual rights and governmental laws will shape this future dynamic.

Privacy norms are encouraged to be modified by AI, creating a commensalistic relationship. AI can enhance transparency by clearly communicating to users how their data is being used and offering choices about what data they are willing to share. Autonomous privacy management

tools involving the usage of AI could also help individuals manage their privacy by automatically adjusting privacy settings based on behaviour, preferences, or legal requirements. An application in the real world utilises a privacy recommendation model for images using tags and an agent (Kurtan & Yolum, 2020) to make editing privacy settings easier and more convenient. They may also be able to detect unusual data usage patterns and provide real-time alerts, empowering individuals to take control of their information. All methods and new developments surrounding AI systems should and will require industry standards and best practices to ensure that privacy is baked into the design of AI from the outset, rather than being an afterthought.

At the current moment, there are quite robust data and privacy laws that cover the majority of the AI privacy regulatory landscape, but education and awareness of these laws plays a much more critical role in guiding the future of privacy and AI. This privacy-centric approach is essential to educate AI developers on the importance of data privacy, so developers can understand the potential risks of data misuse and be trained on how to integrate privacy-by-design principles into AI systems. The increase of broader public education about AI and privacy will empower consumers to make informed decisions about their data and advocate for their privacy rights. This collaborative movement between governments around the world, large multinational corporations, and the greater society can assist in creating a balanced relationship between AI and privacy, which in turn leads to more innovative, privacy-enhancing technology to solve the future complications of the digital world.

REFERENCE LIST

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., ... & Schneier, B. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 1(1), 69-79.

<https://doi.org/10.1093/cybsec/tyv009>

Anand, C. (2019). ISACA.

<https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/more-responsible-data-us-age-through-privacy-enhancing-technologies#:~:text=the%20other%20parties.->

Bellovin, S.M., Blaze, M., Clark, S., & Landau, S. (2012). Going bright: Wiretapping without weakening communications infrastructure. *IEEE Security & Privacy*, 11(1), 62-72.

Clark, J., van Oorschot, P. C., Ruoti, S., Seamons, K. E., & Zappala, D. (2018). Securing email.

Clarke, R. (2020). Profiling: A hidden challenge to the regulation of data surveillance. *Journal of Law, Information and Science*, 15(2), 7-15.

DArminio, P., Iglesias, R.B., Cichowski, J., Dalka, P., Ellwart, D., Pedagadi, S., Orwell, J., Kroener, I., & Neyland, D. (2012). Technologies for Granting Balance between Security and Privacy in Video-Surveillance. *IEEE Access*.

Durumeric, Z., Adrian, D., Mirian, A., Kasten, J., Bursztein, E., Lidzborski, N., ... & Halderman, J. A. (2015). Neither snow nor rain nor MITM...: An empirical analysis of email delivery security. In *Proceedings of the Internet Measurement Conference (IMC)*. New York: ACM.

Dyda, A., Purcell, M., Curtis, S., Field, E., Pillai, P., Ricardo, K., Weng, H., Moore, J. C., Hewett, M., Williams, G., & Lau, C. L. (2021). Differential privacy for public health data: An innovative tool to optimize information sharing while protecting data confidentiality. *Patterns*, 2(12), 100366. <https://doi.org/10.1016/j.patter.2021.100366>

Dwork, C. (2006). Differential privacy. In *Proceedings of the 33rd International Conference on Automata, Languages and Programming (ICALP)* (pp. 1-12). Springer.
https://doi.org/10.1007/11787006_1

Foster, I. D., Larson, J., Masich, M., Snoeren, A. C., Savage, S., & Levchenko, K. (2015). Security by any other name: On the effectiveness of provider based email security. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)*.

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing* (pp. 169-178). ACM.
<https://doi.org/10.1145/1536414.1536440>

Green, M., & Miers, I. (2015). A formal analysis of the Signal messaging protocol. In *Proceedings of the 2015 IEEE European Symposium on Security and Privacy*.
<https://doi.org/10.1109/EuroSP.2016.13>

ICO. (2023). Ico.org.uk.
<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/8-data-minimisation/#:~:text=What%20do%20you%20mean%20by>

Introna, L. D., & Wood, D. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society*, 2(2/3), 177-198.

<https://doi.org/10.24908/ss.v2i2/3.3372>

IPVM. (2021). History of video surveillance. Retrieved from

<https://ipvm.com/reports/history-video-surveillance>

Kisselburgh, L., & Beever, J. (2022). The Ethics of Privacy in Research and Design: Principles, Practices, and Potential. In: Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., & Romano, J. (Eds.), *Modern Socio-Technical Perspectives on Privacy*. Springer, Cham.

Kurtan, A. C., & Yolum, P. (2020). Assisting humans in privacy management: an agent-based approach. *Autonomous Agents and Multi-Agent Systems*, 35(1).

<https://doi.org/10.1007/s10458-020-09488-1>

Manjarres, S. (2024). Data Privacy Dilemma: How to Address Growing Concerns in an Extremely Online World. WatchGuard Block.

Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of "personally identifiable information." *Communications of the ACM*, 53(6), 24-26.

<https://doi.org/10.1145/1743546.1743558>

Palandrani, P. (2020). A Decade of Change: How Tech Evolved in the 2010s and What's In Store for the 2020s. Global X.

<https://www.globalxetfs.com/a-decade-of-change-how-tech-evolved-in-the-2010s-and-whats-in-store-for-the-2020s/>

Pugliese, A., Verdoliva, L., Poggi, G., & Cuomo, G. (2021). Browser fingerprinting against VPNs: Analyses and techniques. *Future Internet*, 13(6), 145. <https://doi.org/10.3390/fi13060145>

Sanchez-Monedero, J., & Dencik, L. (2020). The politics of deceptive boundaries: Rethinking AI ethics and data privacy frameworks in the age of predictive policing. *Patterns*, 1(2), 100017. <https://doi.org/10.1016/j.patter.2020.100017>

Soykan, E.U., Karacay, L., Karakoc, F., & Tomur, E. (2022). A survey and guideline on privacy enhancing technologies for collaborative machine learning. *IEEE Access*, 10, 97495-97519.

The President and Fellows of Harvard College. (n.d.). Harvard University Privacy Tools Project. <https://privacytools.seas.harvard.edu/differential-privacy>

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer International Publishing. <https://doi.org/10.1007/978-3-319-57959-7>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.