

Privacy



By Jalyin G. , Antonio L. ,
Justin K.

What is Privacy? Why is it Important?

1

Cases: Neighbors

2

What do we as a society want? What do we not want?

3

Table of Contents

4

Cases: FB and the end of privacy

7

Conclusions / Final statements

6

Privacy, Autonomy, explore/exploit dilemma, descriptive privacy

5

Protecting privacy today

What is Privacy?

Why is Privacy Important?

1

First and foremost, It is a fundamental human need

2

Personal Identity and Freedom

3

In a digital world, it protects identity theft and misuse of personal information

4

It maintains Professional and Personal boundaries

5

It allows you and your identity to be you

6

It gives control over what personal information we want to share and with whom

What is Privacy?



What We Do Want?

- We want control
- We want privacy to be someone
- We want to project ourselves as someone
- We want privacy to be someone else
- New ways of experiencing, existing, and acting in the world

What Do we NOT want?

- We don't want to have our personal information sold and in the public without our consent
- We don't want to have no control
- We don't want to be neutral / personality-less
- We don't want to have privacy exploited

Privacy Case : Ashley Payne + Others



Ashley Payne is an infamous Privacy case

Ashley lost her job as a teacher after posting a photo on social media of her drinking alcohol on vacation

Other General Examples of Privacy Cases

Homeowners HOA

A woman posting a rant about her neighbourhood's Homeowners Association (HOA) on a private Facebook page. However, someone found the post and showed it to the board, leading to fines and restrictions.

College Applicant Rejected

A high school senior had their college offer rescinded because the university found offensive jokes on their social media from many years ago.

Job Offer Rescinded

A job candidate tweets about how they "hated" the company but wanted the salary. The company's hiring manager finds the tweet and withdraws the offer.

Privacy as a Tool

The ability to control access to personal information allows individuals to manage how they are perceived in different settings.



What We Do Want?

- The ability to decide who knows what about us
- Privacy to separate personal and professional identities
- We want to project ourselves as someone.
- Protection from misjudgement or unwanted exposure
- Freedom to express different aspects of ourselves

What Do we NOT want?

- Personal information being exposed without consent (This also leads into the issue of big tech monetizing our private info)
- Being forced into a single, rigid identity
- Having no control over how we are perceived
- Fear of judgment affecting our careers or relationships

The Panopticon Effect

Constant surveillance influences behavior, limits freedom, and discourages individuality.



What We Do Want?

- Freedom to act without feeling constantly watched
- The ability to express our opinions without fear of punishment
- A society where people are judged by their actions, not their private lives
- Protection from excessive government or corporate surveillance

What Do we NOT want?

- A world where we modify behaviour due to fear of being monitored
- Losing authenticity because we feel pressured to conform
- Privacy violations that condition people to act in predictable, 'acceptable' ways
- A culture of self-censorship where people no longer take risks

When Privacy Should Be Limited?

In some cases, privacy violations provide benefits, raising ethical questions about when privacy should be compromised.



What We Do Want?

- A balanced approach that respects both privacy and security
- Transparency in how data is collected and used
- The ability to opt-in or out of surveillance-based benefits
- Clear guidelines on when privacy should be compromised for safety

What Do we NOT want?

- Unchecked government and corporate surveillance
- Data collection without clear consent or control
- A society where safety is used as an excuse to eliminate privacy
- The risk of misuse of private data leading to discrimination or harm

Zuckerberg's View on your Privacy

1

"You have one identity" – Zuckerberg argues that having multiple identities lacks integrity.

2

Facebook's culture encourages full transparency, reducing the ability to separate personal and professional lives.

3

Loss of privacy means more accountability, but it also limits self-expression.

4

Online behavior becomes permanent, making it harder for individuals to experiment with new aspects of their identity.

5

People modify their behaviour when they know they are being watched, similar to the Panopticon effect.

6

Contrast with traditional privacy views, where individuals could manage different personas in different contexts.

- Facebook's approach challenges the idea that privacy allows people to explore and change freely.
- Raises ethical concerns: Should we always be forced to be the same person in every space?

The Ethics of Privacy Degree

"You have one identity. The days of you having a different image for your co-workers, and for the other people you know, are coming to an end. Having two identities for yourself is a lack of integrity."

This 2010 quote from Mark Zuckerberg summarizes a critical foundation in the belief of his social media platform, Facebook

The Three Claims (Psychological, Empirical, Ethical)

Psychological Claim – What does this mean for people?

Vertical diminishment of multiple identities – Different sides of your current life meshing together

Horizontal diminishment of multiple identities – Facets of your present getting to know facets of your past

Empirical – What is actually happening in the world? (Objective)

The days of separate spheres of influence and personalities is effectively coming to an end. Facebook walls compile all facets of a person's life into one feed and display it for all viewers whether it be family or faculty. This makes it nearly impossible to keep parts of one's life private/secret to one group or another.

Ethical – Do we as a society want this?

You must be who you are. You have one identity and as long as you are on Facebook, that should be the identity that you are upholding. Multiple identities are an objectionable stance to authenticity and integrity. Being who you are is GOOD.

The Implications/Qualms of Total Integration & Integrity on Facebook

- The end of shame ?
- Is this authentic and complete persona showcased online, the same as a persona showcased in real life?
- Should we know who we truly are?
- Qualms about authenticity:
 - Is authenticity = integrity?
 - Is identity change possible?

Singular Identity vs Multiple Identities



What Does Facebook Want?

- The essential death of online privacy
- You must be who you are
- The amalgamation of all spheres of your life
- No separation of identity

Authentic Identity Representation | Transparency Center - Meta

We believe that authenticity helps create a community where people are accountable to each other, and to Meta, in meaningful ways. We want to ...

What Do Multiple Identities Allow?

- Expression of freedom
- Expression of new ways of living in the world
- Maintenance of professionalism in workplaces
- Security of privacy
- Separation of different lives

A Facebook Scenario

Alvin, a nonbinary person who goes by a chosen name different from their legal name

- Alvin joins Facebook in order to stay in touch with an LGBTQ+ support group
- Alvin's account is flagged as Facebook's integrity policy requires users to use their "real"/legal name
- Alvin's account is locked for violation of the integrity policy, needing to further verify their identity in order to get their account back

Problems & Harms

- Alvin's legal name does not match their lived identity.
They lose access to their support group.
They don't feel comfortable sharing their legal identity publicly.
- Alvin risks losing their account permanently.
Potential feelings of exclusion and erasure from online spaces.
- If spaces like Facebook are meant to foster community, should they be able to uphold such a rigid integrity policy when marginalized groups may be disproportionately harmed?

Protecting Privacy



Privacy-By-Design

- When we design AI systems and how data is to be not only collected but used, strategies are employed to maximize user privacy protection
- Data Minimization
Take minimum amount of data required to do a task --> use the data to only complete said task --> delete the data when the task is complete

Ex. An AI chatbot used for online banking asks a user for the last 4 digits of their account number and a one-time passcode sent via text in order to check their account balance; Instead of asking for the full account number or any further personal details, the AI asks for only the minimum necessary information to verify identity

- Differential Privacy

Adding randomness (within limited parameters) to a dataset in order to block access to identity

Ex. A tech company gathering user search queries adds randomness to each user's data before storing and analyzing; The tech company can still analyze general search trends without tracing a search history back to a specific user

- Obfuscation

Maintaining privacy by releasing a vast amount of information, making it impossible to decipher a relationship between a user and the data

Ex. Browser add-ons which visit random webpages make it more difficult for network companies such as Verizon and other service providers to monitor trends and relationships

Protecting Privacy Pt. 2



Ownership

- Data Ownership

Letting individuals monetize their own personal information by giving them tools to do so

Ex. A user allows for a sleep study to be done on them and monitored within their home for one hundred dollars

Privacy bred from economic control over the information circulated about the user

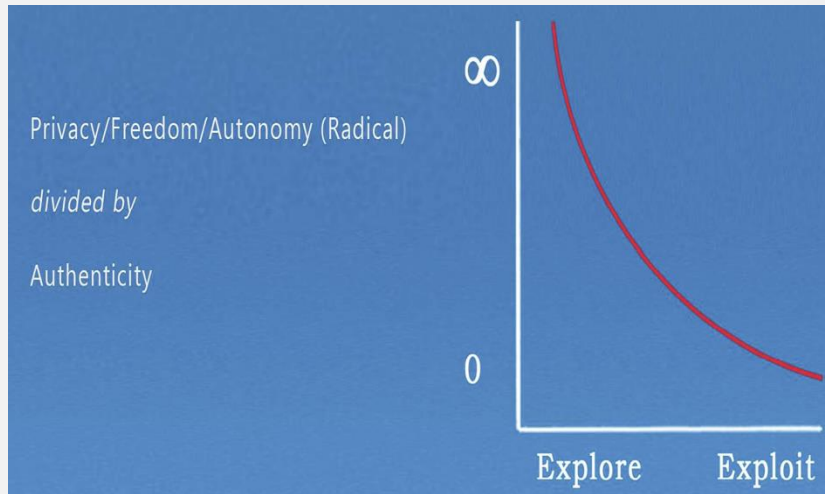
Questions to be asked?

Does society have a genuine claim to ownership of one's personal information, and to what extent?

Do we maintain a degree of ownership even after selling our personal information? (Does PI = art?)



Explore/Exploit



Autonomy vs. Authenticity

When one knows very little about a user (ex. Predictive analytics) and is trying to find out more information, explorative tactics will be used which maximizes autonomy and privacy through lack of known information

When we collapse the machinations of user data into an amalgamation of ideas of who a user really is for the sake of authenticity, it can be defined as a more exploitative tactic (ex. Facebook, collapsing the barriers of privacy)

Finding Yourself vs Being Told Who You Are



**Thank
You**