

ENGLISH TASK:

The Digital Privacy Paradox: Personal Data Protection in the Age of Social Media

Produced By

Athallah Zaki Ramatiansyah

1202230051



Rapid Digital Transformation

Background

- Internet & social media reshape communication globally.
- Data flows across borders instantly, turning personal information into a valuable digital asset (“new oil”).
- However, widespread data collection poses significant privacy risks.

Key Question:
How can we protect privacy rights while benefiting from digital technology?



Global & Regional Data Breach Trends (2025)

Worldwide Breach Facts

- Nearly 94 million records leaked in 2025 so far. [Statista](#)
- Average global cost of a data breach: ~USD 4.44 million. [Sci-Tech Today](#)
- Human error accounts for ~60% of breaches. [Sci-Tech Today](#)

Regional Insight - APAC

- ~40% of online users in Asia Pacific experienced unauthorized access to their personal information.

Indonesia: Internet Usage & Security Incidents

APJII Survey and Kontan.com

80,66%
Indonesia internet
users

22,12% **14,36%**
Users

Online Fraud

10,89%
Users

Malware and viruses

- Data theft / hacking / phishing



Personal Behavior & Data Sharing

Why Users Share Data

- 23.90% share personal data for promotions/discounts. [GoodStats Data](#)
- 16.45% share for contests/giveaways. [GoodStats Data](#)

Implication:

Users often volunteer sensitive information without fully understanding privacy risks.

Privacy Paradox

Definition:

Users express concern about privacy but often neglect protective practices for convenience.

Example User Behavior

- Weak or reused passwords
- Clicking unknown links
- Accepting easy login options

Global Reminder:

16 billion login credentials were uncovered exposed online, including credentials tied to major platforms like Facebook & Google.

Core Concerns

Main Issues:

- Increasing volume & sophistication of data breaches.
- Users often unaware of privacy implications.
- Legal frameworks (especially in Indonesia) are not yet comprehensive.

Resulting Risks:

- Identity theft
- Financial loss
- Loss of trust in digital systems

Key Theoretical Concepts

Privacy as a Fundamental Right

- Defined as control over personal data sharing, storage, and disclosure.
- Closely linked to self-determination and autonomy.

Legal vs Behavioral Gap

- Even where laws exist, weak enforcement and low user literacy amplify privacy risks.

Key points

Policy & Practice Recommendations

For Governments

- Strengthen comprehensive data protection laws
- Mandate transparency & accountability
- Ensure breach reporting requirements

For Service Providers

- Implement privacy by design
- Provide clear user consent options
- Use encryption & strong authentication

For Users

- Use unique, strong passwords
- Enable two-factor authentication
- Be cautious sharing personal information

Conclusion:

Core Message

Personal data protection requires a multi-stakeholder approach:

- Individual awareness
- Organizational accountability
- Robust national regulation

If privacy is left to chance, millions will remain vulnerable.

*Any
Question?*