Unit 4 Seminar - Breach Analysis Case Study

Case Study: Facebook Data Breach

1. **What types of data were affected?**

The Facebook data breach affected many categories, including phone numbers, complete names, addresses, email addresses, and other user profile information uploaded to a hobby hacking site. Personal data from 533 million Facebook users across 106 countries is included in the hacked data (Bowman, 2021).

2. **What happened?**

It was discovered in 2019 that political consultancy firm Cambridge Analytica had inappropriately accessed millions of Facebook users' personal information. Facebook had permitted a third-party app to access user data, which is how Cambridge Analytica acquired its information. Afterwards, Cambridge Analytica used the information to target people with political adverts (UpGuard, 2019).

3. **Who was responsible?**

The data misuse was Cambridge Analytica's fault. However, Facebook's careless handling of user data also drew criticism (Confessore, 2018).

4. **Were any escalations(s) stopped - how?**

In 2019, two Facebook app datasets containing information of over 530 million users were exposed to the public. In April 2021, the data was posted for free, indicating criminal intent (Hill & Swinhoe, 2022). As Graham-Harrison & Cadwalladr (2018) state, despite knowing about the data leak for months, Facebook did not alert users until 2019. Due to this delay, Cambridge Analytica could keep using the information for its objectives.

5. **Was the Business Continuity Plan instigated?**

It is unclear whether Facebook's Business Continuity Plan was initiated in reaction to the data hack, according to Bowman (2021).

6. **Was the ICO notified?**

Sky News (2019) reported the data breach to the UK Information Commissioner's Office (ICO) in 2018. The ICO fined Facebook £500,000 for its involvement in the violation.

7. **Were affected individuals notified?**

Facebook came under fire 2019 for failing to alert consumers to an earlier data incident. Culliford (2021) said that Facebook did not notify its users about the incident until 2019. Facebook must notify any unauthorised access to data on 500 or more users within 30 days of the incident's confirmation under the July 2019 FTC settlement terms.

8. **What were the decisions' social, legal and ethical implications?**

The Facebook data breach had several social, legal, and ethical ramifications. The hack damaged Facebook's reputation and sparked questions about internet data privacy. Facebook was also chastised for its lack of openness and for not doing enough to safeguard user data (OECD, 2019).

9. **If you had been the ISM for the organisation you selected, what mitigations would you have put in place to stop any reoccurrences?**

To prevent the data leak from happening again, I would have put in place several mitigations if I had been Facebook's ISM, as Sanders (2019) pointed out. These countermeasures would have consisted of:

- **Boosting data privacy regulations:** Facebook's data privacy regulations lacked sufficient clarity and user data protection. It would have been evident to users what data was being gathered and how it was being used if I had created more thorough and approachable policies.
- **Improving data access controls:** Cambridge Analytica could obtain user data without authorisation because Facebook's data access rules were insufficiently

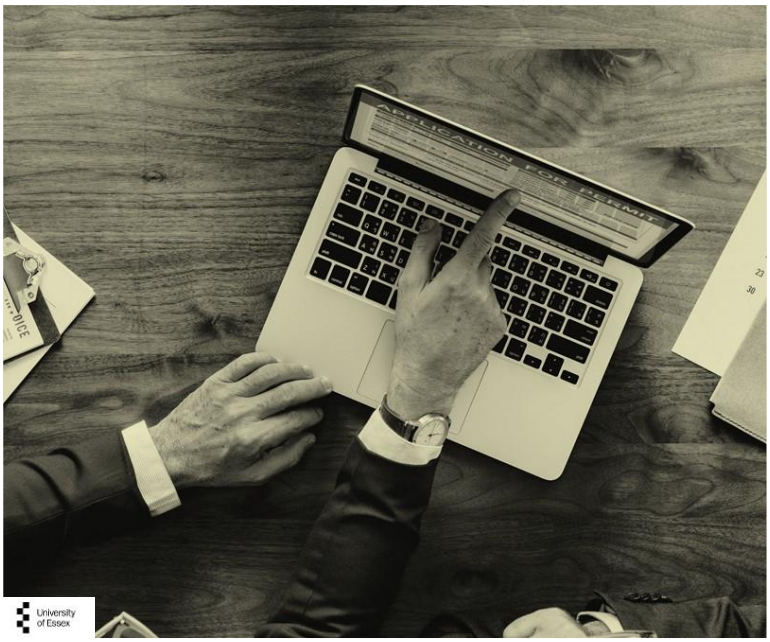
strict. More strict data access rules, which would have only permitted users to share their data with reliable apps and services, are what I would have put in place.

- **Raising user knowledge of data sharing:** Many Facebook users were unaware of how their personal information was exchanged with unaffiliated apps and services. To raise user awareness of data sharing, I would have put in place various strategies, like offering consumers more choices over sharing their data and more information about how it was being used.

- **Regular security audits:** The data hack remained undiscovered for several months because Facebook did not regularly check its systems. If it were up to me, a routine security audit programme would have been implemented to find and fix any weaknesses an attacker may exploit.

Egan (2020) raised a significant issue regarding the gathering and use of personal data by businesses in a recent piece. The question of enabling people to make knowledgeable decisions about their data is constantly debated worldwide. People have a fundamental right to know how their information is gathered and used. But current notices and policies about privacy can be hard to find, laden with legalese, or just plain unclear. Policies about privacy are not enough to inform people about their data. Businesses need to develop creative ideas for empowering people to make privacy decisions that suit their needs. To successfully communicate about privacy, companies need to acknowledge and accommodate the broad spectrum of users of digital services.

Slide presentation:



What happened?

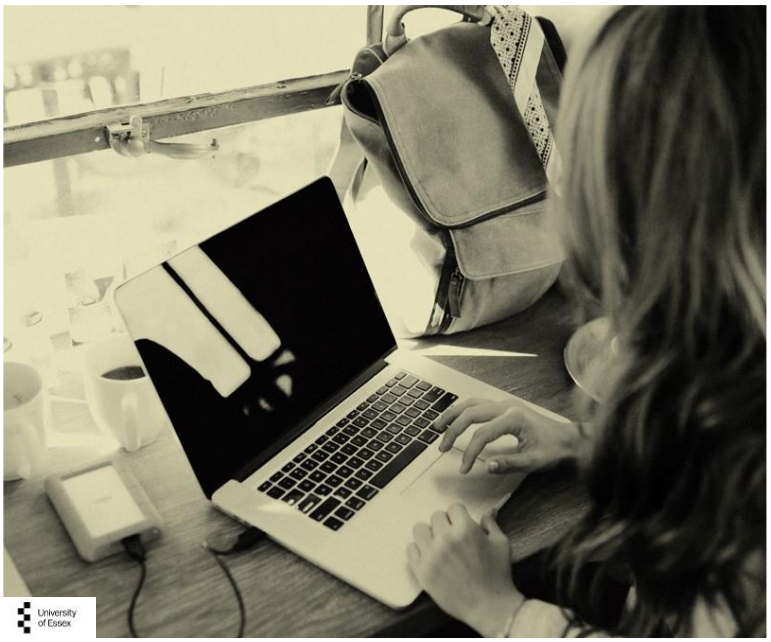
In 2019, political consultancy firm Cambridge Analytica had inappropriately accessed millions of Facebook users' personal information. Facebook had permitted a third-party app to access user data, which is how Cambridge Analytica acquired its information. Afterwards, Cambridge Analytica used the information to target people with political adverts.

What types of data were affected?

- Personal data from 533 million Facebook users across 106 countries was hacked.
- The data include:
  - Phone numbers,
  - Complete names
  - Addresses
  - Email addresses
  - User profile information


What were the social, legal and ethical implications of the decisions made?
The Facebook data breach had several social, legal, and ethical ramifications. The hack damaged Facebook's reputation and sparked questions about internet data privacy. Facebook was also chastised for its lack of openness and for not doing enough to safeguard user data.
University of Essex


ISM mitigation plans to stop any reoccurrences?
Boosting data privacy regulations
Develop more comprehensive and user-friendly policies in compliance with GDPR to clarify what data is collected and how it's used.
Improving data access controls
Implement stricter data access controls to allow data sharing with trusted apps.
Raising user knowledge of data sharing
Implement measures to increase user awareness of data sharing, providing users with more information about how their data is being used and giving them more control over how it is shared.
Regular security audits
Implement programs of regular security audits to identify and address any vulnerabilities that attackers could exploit.
University of Essex



Takeaway

The collection and use of personal data by businesses has grown to be a severe problem. Individuals are entitled to know how their data is used, yet privacy regulations frequently must be clarified and challenging to understand. Companies must devise innovative solutions that enable consumers to make knowledgeable privacy decisions in order to address this. Sufficient user accommodations are essential for effective privacy communication.

References:

- Bowman, E. (2021). *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users*. [online] NPR.org. Available at: https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users.
- UpGuard (2019). *Losing Face: Two More Cases of Third-Party Facebook App Data Exposure*. [online] Upguard.com. Available at: https://www.upguard.com/breaches/facebook-user-data-leak.
- Confessore, N. (2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. [online] 4 Apr. Available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
- Hill, M. and Swinhoe, D. (2022). *The 15 most significant data breaches of the 21st century*. [online] CSO Online. Available at: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html.
- Graham-Harrison, E. & Cadwalladr, C. (2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. [online] The Guardian. Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
- Bowman, E. (2021). *After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users*. [online] NPR.org. Available at: https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users.
- Sky News (2019). *Facebook agrees £500k fine over Cambridge Analytica scandal*. [online] Available at: https://news.sky.com/story/facebook-fined-500k-over-use-of-personal-data-11849056.
- Culliford, E. (2021). Facebook does not plan to notify half-billion users affected by data leak. *Reuters*. [online] 8 Apr. Available at: https://www.reuters.com/article/us-facebook-data-leak/facebook-does-not-plan-to-notify-half-billion-users-affected-by-data-leak-idUSKBN2BU2ZY/.
- OECD (2019). *Risks and challenges of data access and sharing | Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies | OECD iLibrary*. [online] www.oecd-ilibrary.org. Available at: https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en.
- Sanders, J. (2019). *Facebook data privacy scandal: A cheat sheet*. [online] TechRepublic. Available at: https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.
- Egan, E. (2020). *Communicating Towards People- Centered and Accountable Design About Privacy: J U LY 2 0 2 0 C H A R T I N G A W AY F O R W A R D*. [online] Available at: https://about.fb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf.