# INFO202

## Horror-story analysis

**Title:** Why Facebook's Latest Privacy Snafu Is Particularly Gross

**Group Member:** Yuming Chen 320180939611

Chunyao Dong 320180939690

Ruyu Lin 320180940000

Huiyi Liu 320180940030

**Date:** 24th April, 2020

**1. Brief Introduction:**

In 2018, Facebook was stung by the privacy disclosure scandal with Cambridge Analytica. One year later, Facebook once again broke out in the information security scandal. According to the story, in March 2019, Brian Krebs, a network security journalist, reported that Facebook had been storing hundreds of millions of users' passwords in plain text on internal company servers. These passwords were searchable by more than 20,000 Facebook workers. Facebook later confirmed the news and said it had fixed the problems.

**2. What are/were the digital materials at issue?**

In our opinion, the digital materials at issue were user passwords which are encrypted data item. As we all know that password is a memorized secret, typically a string of characters, used to confirm the identity of a user. Although password cannot guarantee absolute security, password is still the only way to verify the user's identity in most software application at present. This means that password is the only key to user privacy. If someone's password is leaked, his/her privacy will no longer be secret. Especially in Facebook, such a big social network company which has a large number of users, in order to maintain users' confidence and trust, they have a strong responsibility to protect user password. However, Facebook has extremely careless mistake in the management of user passwords which may bring a great dangerous to user privacy.

**3. What went wrong (or could go wrong) with the digital curation?**

We think the Facebook might have serious vulnerability in the digital preservation which is one of the most important steps in the digital curation and it will bring serious security threats to users' privacy. According to the report, Facebook had been storing hundreds of millions of user passwords in plain text on internal company servers. This is very disturbing news and the mistake Facebook made is very terrible and dangerous. In Brian Krebs' article, a Facebook software engineer said the passwords were "inadvertently recorded.". Moreover, it is reported that the vulnerability may date back

to 2012. This shows that Facebook may have had such a serious security vulnerability a long time ago. And we believe the vulnerability might happen in the process of Facebook collecting and storing new user account information which may be part of digital preservation.

**4. What are the consequences of the poor data handling to the people responsible for the data?**

Facebook was stung by the privacy disclosure scandal with Cambridge Analytica in 2018 and it had an extremely bad influence on the Facebook. Brian Krebs's report might significantly increase the negative impact on Facebook. To conclude it, we think the bad consequences are reflected in three parts:

1) Economic loss

After this series of public opinion disturbance, Facebook's market image has been greatly damaged, and the capital market began to distrust Facebook. Facebook's stock has plummeted, with hundreds of millions of dollars of market value disappearing, causing huge economic losses.

2) Official investigation and punishment

Facebook has been closely scrutinized over a number of privacy and security scandals that have exposed the company to criticism from customers, as well as inquiries and fines from multiple regulators, particularly the European Union.

3) Users' trust and confidence

The whole point of a password, after all, is that it's kept secret so that other people can't access your account and it is why users trust Facebook as a place to have deeply personal conversations, make business deals, plan protests, stalk our crushes, join private discussion groups on sensitive topics, use credit cards, and communicate under our own names. If the Facebook be careless about user privacy, the user would not trust Facebook and move to other social network applications.

**5. What are the consequences of the poor data handling for users or potential users?**

The consequences for users or potential users may be a disaster. Facebook has a very large chunk of those users live in less affluent countries. For many, using the internet over their phone and via Facebook may be their primary way of getting online and doing business. If their password is leaked and some bad guys get their password, it may not only cause the personal information disclosure, but also cause many significant economic losses. Especially the people who do not live in affluent countries, they may even have no chance to do something to protect their privacy and property security in Facebook with their password leakage.

**6. Could this problem have been avoided? How?**

Different from the previous privacy disclosure scandal, people believe this vulnerability was far more likely the result of carelessness than malice, but it reflects the Facebook's terrible attitude to user privacy. We think it is not only the company that needs to improve themselves, but also needs society's monitoring and government's regulation. GDPR is a great example which government introduce policies to require company to protect user information security. It will promote the company like Facebook to attaches more importance on data security and take more action on monitoring and data management.

**7. How does this case relate to the readings and lectures so far?**

Our course indicates that one of the data curation's five main goals is to ensure the protection, especially for private data. However, as a social network company holds a large number of private information, Facebook stored hundreds of millions of user passwords in plain text on internal company servers which were searchable by more than 20,000 Facebook workers. It made no effort on ensuring the security of data, which reflects it takes no count of data curation and data preservation.

The course involves the personal data issue, which faces the challenge of securing it physically overtime and protecting privacy. In this case, after the problem had been

discovered by Facebook company, it had not fixed the problem until a reporter made the information public two months later. This makes Facebook lose a lot of users' trust. Just as Dale said, 'Curation in a digital world isn't a luxury, it's a necessity.' Facebook shall realize the significance of data curation and work on it, instead of being particularly careless with users' privacy or conceal the fact.