Alex Surprenant

CS 405

8/5/25

Data Breach Case Study

**Name of Case:** Colossal data breach exposing 4 Billion user records  
**Link to case:** <https://www.csoonline.com/article/4003037/colossal-breach-exposes-4b-chinese-user-records-in-surveillance-grade-database.html>  
**Date:** June 2025  
**Why case made the news:** This case was the largest leak ever discovered exposing highly sensitive personal data to the public with over four billion records being leaked to the public. The data included bank details, home addresses, data from Alipay, and public behavioral profiles.

**Description of the breach:** This incident could be classified as an massive unsecured database breach where, as the data was maintained in large quantities for the purpose of building comprehensive social profiles. It was caused by the database being made publicly accessible and lacked basic security like passwords, which made it totally available to anyone who could find the database over the internet. The nature of the data made it clear that it was gathered in the interest of profiling of Chinese citizens, and anyone else who used the platforms the data was gathered from. This made the database a particularly high value target.

**Identification of threats:**  There a few immediate threats involved in this breach. Right off the bat, the invasion of peoples privacy and safety, as the data involved included home addresses and personal behavioral profiles. The affected people will now be susceptible to identity theft due to the exposure of their personal data and banking and payment information. Long term threats can include the potential for people to be targeted for blackmail with there personal data, or be specifically targeted to scams that are tailored to their personal situations.

**How developers could have prevented this:**  This database lacked even basic security measures to prevent the breach from occurring. A developer should have implemented access controls and authentication for access, as well as restricting access to the database through firewalls. Data should have also been encrypted with multiple levels of encryption. Policies that can be implemented to prevent this in the future would be data governance policies for procedures for data handling, and least privilege access policies to ensure users have the minimum access they require.

**Summary:**

* **Authentication:** The breach shows that the database had no basic authentication. Password implementation and authentication policies would have been a baseline to help prevent this attack.
* **Authorization:** Effective access control mechanisms will restrict sensitive data from being viewed and modified by non-authenticated users. Data access should be limited using role-based controls.
* **Accounting:**  Detailed records should be kept for who gained access to the system and its data. This will help security teams in the future who are attempting to intercept suspicious activity.
* **Defense in depth:** This breach is a clear representation of why multi layer security is important and should be utilized. Multiple security layers could have contained the breach before it ever got out of hand.

Resources:

Staff, C., Singal, N., Thomas, P. A., & Sharma, A. (2025, August 7). *Colossal breach exposes 4 billion Chinese user records in surveillance-grade database*. CSO Online. https://www.csoonline.com/article/4003037/colossal-breach-exposes-4b-chinese-user-records-in-surveillance-grade-database.html