Fenglei Gu

fg1121@nyu.edu

CS 060 – Database Design and Implementation

10 Sep 2019

Article 1: Wang, Lin. "Data reportedly leaked from a company focusing on public safety and security with AI technologies, alerting the alarm of the security of facial recognition)." Beijing: People's Daily Online[1], 26 Feb 2019.

In this article, People's Daily, a press affiliated to the Communist Party of China, reported that SenseNets, an IT company headquartered in Shenzhen in southern China, had recently been suspected to have leaked approximately 6.8 million entries of data, including National ID information, images for facial recognition and their corresponding locations of image shooting, affecting more than 2.5 million citizens in the country. It is also reported that facial recognition technology is the major research field of SenseNets, and local police detachments in many provinces have contracts with SenseNets to improve local public security.

Nowadays, facial recognition has become increasingly popular, from various types of mobile payment, to library entry, and even "automatic law enforcement[2]," while concerns about privacy have been raised by many. On the one hand, considering the uniqueness and immutability of biometric information, including but not limited to fingerprints, facial and iris characteristics,

[1] http://it.people.com.cn/n1/2019/0226/c1009-30901727.html

[2] A kind of technique firstly adopted by local traffic police in Shanghai, in which street cameras capture the faces of pedestrians who cross a street when red light is on, and then those law-breakers will receive tickets, based on their facial information recorded in National ID database.

ordinary customers should try their best to avoid submitting their biometric information to any person or entity. On the other hand, stricter laws should be made requiring any organization collecting or using their customers' biometric information to install more advanced protecting technologies for their databases; while there should be strict law enforcement punishing those irresponsible companies.

Article 2: Hua, Shen. "Lack of protection for data, Leakage of information of millions of citizens in Xinjiang." District of Columbia: Radio Free Asia[3], 18 Feb 2019.

In this article, Radio Free Asia (RFA), a press aimed at promoting democracy in Asia, reported the same event as in Article 1. RFA reports that Victor Gevers, a researcher working for a Dutch non-profit organization called GDI Funds, claims to have discovered significant loopholes in the server and databases of SenseNets. It is reported that by analyzing the data, Gevers found that there were more than 6.7 million entries of real-time location information received by the server in the latest 24 hours, most of which showing locations in Xinjiang. Gevers also found that about 99% of names in the database are Muslim-styled names, such as "Maimaiti" and "Mahemuti"[4]. Meanwhile, Gevers found in their log file that the database was downloaded days ago, and a note was left asking for a ransom of 0.6 bitcoins. RFA also reports that Shuguang Zhou, a network engineer living in Taiwan, has noticed that SenseNets uses MongoDB for their databases.

It is doubtable whether it is appropriate for the government to have the biometric and other private information of local residents stored in the database owned by a commercial company.

[3] https://www.rfa.org/mandarin/yataibaodao/shaoshuminzu/hc-02182019113010.html

[4] These are variants of "Muhammad" in Chinese.

In the meantime, this issue indicates that improper or abused usages of big data can also pose significant threat to freedom and human rights, as local government in Xinjiang can use these technologies to monitor the behaviors of local residents.

Article 3: Wang, Li. "Leakage of data of China Railway customers, probably due to credential stuffing." Shanghai: Shanghai Observer[5], 29 Dec 2018.

In this article, Shanghai Observer reported that 600 thousand entries of China Railway passenger data were leaked. China Railway claimed that these data were not leaked from their official website, but from third-party websites. Experts suggest that these data might be derived from "credential stuffing," in which hackers steel the usernames and keywords from one website and then try to use these credentials to unlock their credentials in another website, with assumption that a user would use the same keyword for all the sites.

This gives us a lesson that it is better not to use the same passcode for different websites; particularly, we should pay special attention to "less reliable" websites which are more vulnerable to attacks.

Nevertheless, some still reckon that these data were leaked due to the "struts2" existed in the subdomain and subsite of China Railway's website 12306.cn. However, critiques argue that these data were not stored in any subdomain, but in root domain of China Railway. As far as I

[5] https://www.shobserver.com/wx/detail.do?id=124462

am concerned, there might be multiple reasons for this issue, but what we should do is to enhance vigilance.