Yuqing Zhai

09/25/2024

In July of 2024, the data breach of AT&T text and call records poses all customs privacy into risk. [1] Although only the metadata, which does have directly personal identifiable information is leaked, its potential consequence is severe. In the essay, it will first provide by ground by analyzing the data breach by Hartzog's theory and Nissenbaum's theory of privacy. It will then use virtue ethic to show that AT&T, Snowflake, FCC's practice is unethical. It will then explore the potential consequence and potential better privacy protections measures that could be employed in the future.

The text and call records are leaked by one of AT&T's storage service provider, Snowflake. Fortunately, the leaked information only the metadata of the text and call records, which means that hackers could not know exactly which person that have used a certain number, but the text and call history between numbers are still present for almost all AT&T customer. [1] These data, however, with some online database, could be easily used to identify person. In this case, it is obvious the information is **nonpublic personal information**, and even though it still requires some database searching, it could still be said this kind of information is a **personal identifying information**.

From Hartzog's privacy theory, the privacy is not absolute hidden of private information, but a level of **obscurity** such that it's difficult to acquire the information and identify the person with it, and with obscurity, the trust is given by individual to others, in this case the AT&T. The users in this case expect that there are certain level of obscurity as AT&T will only keep the information to themselves, unless they are required by the law enforcement for probable reasons. Therefore, they give trusts to AT&T for their phone services. From the Nissenbaum's privacy theory, the privacy is a "**contextual integrity**". The **distribution** and **appropriateness** of such information is based on the norm defined in certain context. In this case, user gives information to AT&T because it's appropriate for AT&T to have such information for their phone services, as keeping this kind of information might be useful for the customer in case they want to recover their call long if they delete it locally, and the data breach is a violation in the norms of the distribution, as no one expect the data should be hacked in order to be distributed.

Using virtue ethic, we could clearly see AT&T's action is immoral. In virtue ethics, whether one is ethical depends on if one has **positive character traits** like courage, honesty and kindness. From Hartzog's privacy theory, user gives trust to the AT&T, we could see a form of promises are built between users and the company. When the data breach happens, AT&T fails to protect the data from users, and break the promise between user. In this sense, AT&T as a company is irresponsible and cannot keep up to

the promises, and therefore, unethical. Moreover, the company Snowflake and AT&T have made a contract where the former will provide secure storage services. When the Snowflake is unable to defend such attack, we see it's also irresponsible to AT&T and thus unethical, as it fails to provide the security needed. Furthermore, we see that it's not the first time this thing have happened [1], the FCC, a federal government entity whose responsibility is to prevent such thing from happening, failed to fulfill the responsibility to its people, as it does not enact required laws to prevent inadequate cybersecurity practices in the companies. [1] Therefore, FCC is also irresponsible and unethical.

As 404 Media further detailed, there could be some geolocation data associate with the numbers in the record. Given that the real person behind the phone number could be easily identified by some public databases, it's concerning that a potential hacker, the Binns in this case, could commit large deanonymization of the dataset, and sell that some criminals that could find target of interest, and trace one's location using the leaked geolocation data, so that serious crime, including kidnapping, human trafficking, and murder. [1, 2] With mass deanonymization, the call and text data could also be used to reconstruct the social relation graph between even real people, and these relation could be used for impersonation, theft, and further serious crimes.

An obvious privacy measures is to store the data encrypted multiple times, where all the encryption keys and data are both required to access the data. Had AT&T stored the user data with multiple encryption keys in different location by different service provider, the hacker will not be able to access the data since they only get the data but not the key. In this case, the AT&T could deprecate the key associate with leaked data, and re-encrypt the data with a new encryption key. Also, AT&T could archive the data, say more than 3 months, and move the data to physically separate from the internet, so that it will be impossible to hack. The data could only be acquired by the user upon a request. Both of measurement could significantly make their database more secure.

Reference

[1]

Cox, J. (2024, July 12). Hackers Steal Text and Call Records of 'Nearly All' AT&T Customers. https://www.404media.co/hackers-steal-text-and-call-records-of-nearly-all-at-t-customers/

[2]

Cox, J. (2024, July 12). American Hacker in Turkey Linked to Massive AT&T Breach. https://www.404media.co/american-hacker-in-turkey-linked-to-massive-at-t-breach/