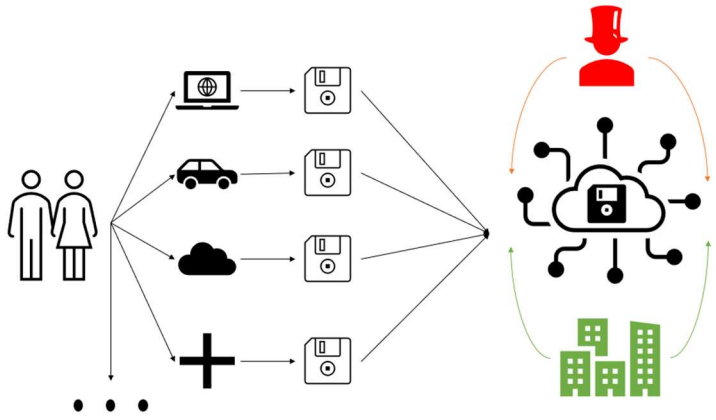
The Netflix Prize Data Breach

ME555 - Ethics in Robotics and Automation

Rucha Patil

Introduction

We have entered a world of digitization where most of our activities are integrated with computer systems. With digitization `comes the data that we enter these systems. From health records, addresses, phone numbers, credit card details, ethnicity, etc. to something which we might consider trivial such as restaurant reviews or movie ratings, this data once on the internet is always on the internet. Leakage of this data can lead to identity theft, theft of intellectual property, credit card fraud, etc., or just for the sake of privacy. Hence, the protection of this data is extremely important. One of the largest voluntary data breaches that took place in recent years is the Netflix Prize Data breach when even though all the measures were taken to anonymize the data to be released, several identities were revealed, resulting in a huge lawsuit against Netflix [1, 3, 7, 2]. This Case-Study discusses the happenings of the Netflix Prize Breach and the Ethical Implications of the same as described more in detail in the following sections. There are multiple ethical issues and angles to be taken into consideration which is also discussed.



Case Description

Timeline

In October 2006, Netflix released data of around half a million users which consisted of ratings of over 100 million individual movie ratings for a competition [3, 2, 1]. At the time Netflix provided DVDs in addition to its online services. The recommendation system algorithm used by them is called the CineMatch which is basically a collaborative filtering algorithm. Despite improving in accuracy over its course, it plateaued. To improve the accuracy of the system, Netflix launched the competition called the Netflix Prize which challenged the researchers to improve the accuracy of this recommendation system by a

benchmark of 10% and offered a prize of $1M. They provided the researchers with anonymized data of around 100M users.

The competition ran for around 3 years and received 44,014 submissions from 5169 teams [1, 7]. Every year in this competition only three teams were able to achieve accuracy higher than that of CineMatch. In 2009, two teams achieved the set benchmark of 10% and met the additional requirements as well. In September of the same year, the teams engaged in a reenactment of an artificial intelligence penalty shootout. The victory was close, in the tradition of penalty shootouts. The outcome for the runners-up, "The Ensemble," was identical to that of the winners. The Netflix Award, however, went to "BellKor's Pragmatic Chaos" since they sent in their results 20 minutes sooner.

Following the success of this competition, Netflix announced its sequel. The major change was the change in Dataset. The new data even included details of the users such as ages, genders, ZIP codes, genre ratings and previously chosen movies[1].

Netflix did try to ensure privacy by anonymizing the data, and by replacing usernames with pseudonyms, however 2 researchers Narayanan and Shmatikov [5] were successful in de-anonymizing a part of this data by linking these to public ratings on IMDB. After, it was also linked with amazon reviews which lead to identity disclosure [6]. Following multiple class action Lawsuits against Netflix in 2009 and an inquiry by the federal trade commission[?], the second round of this competition was canceled[7]. The data was taken down by Netflix, however, it is still available on the internet[8].

After a couple years, Netflix announced that the winning algorithm won't be implemented due to the engineering costs associated with it and due to the change in the mode of operation. That is, Netflix's major business was shifting to online streaming services than offline DVDs and Netflix thought that the winning algorithm could not be applied to change in the data [1]

About the Data

The data can be considered a matrix where each Netflix user rated movies from 1 -5. If we could predict the missing values from this matrix for the non-rated movies, we would have a great movie recommender system, which was the goal of the competition. The problem is called Collaborative Filtering or Matrix Completion. The overall structure of the Data looks as follows[2]

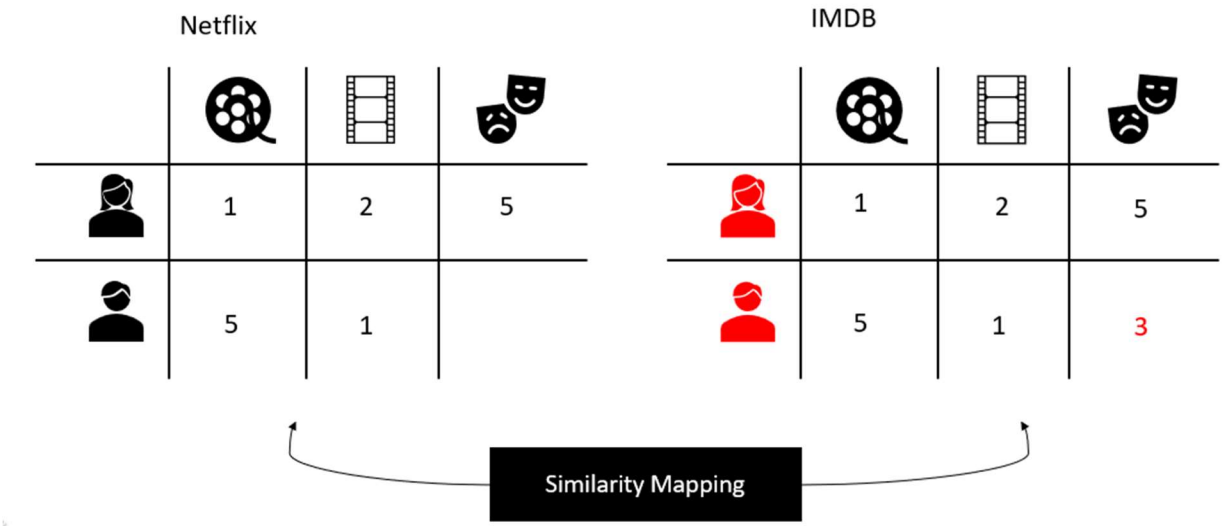
1. Training set (99,072,112 ratings not including the probe set; 100,480,507 including the probe set)
2. Probe set (1,408,395 ratings)
3. Qualifying set (2,817,131 ratings) consisting of
    a. Test set (1,408,789 ratings), used to determine winners
    b. Quiz set (1,408,342 ratings), used to calculate leaderboard scores

How does deanonymization work?[4]

Though multiple methods are available for the same, the method implemented by Narayanan and Shmatikov is called similarity mapping.

The database may be seen as a N M matrix, where each row represents a record linked to a certain person and each column represents an attribute. Each record may be seen as a point in the multidimensional attribute space, with each attribute acting as a dimension. With hundreds to millions of characteristics, such as the Netflix reward dataset, preferences databases are inherently sparse, meaning that each record only includes values for a tiny subset of the attributes. Often, the distribution of support sizes for qualities follows a power law with heavy or long tails. This indicates that although the columns corresponding to "unpopular" items have minimal support, most of the non-null entries in those columns are made up of those "unpopular" things.

A pair of characteristics (or, more broadly, a pair of records) are mapped to the range [0, 1] using the similarity measure. It expresses how we naturally think of two values as being "similar." Afterwards, this similarity metric is evaluated and contrasted. The algorithm was made to operate on databases that had been "sanitized" and made anonymous by their publishers, in this case Netflix.



Stakeholders

Netflix

As the company was at the center of all the happenings, it was the key stakeholder. The company faced reputational damage, legal and regulatory implications, and financial losses because of the breach.

Customers

The customers who trusted the company with data were also key stakeholders. Everyone holds the right to privacy, the right to security. As a result of the breach, their identities were exposed, and their data became vulnerable to various malicious purposes. These could become a victim of identity theft and fraud.

Partners and vendors

Stakeholders included any suppliers or partners who collaborated with Netflix and had access to the data set. Their connection with Netflix and their own reputation in the business may have been impacted by the incident.

Employees

There were also stakeholders within the Netflix staff. Their jobs may have been affected by the breach, which may have resulted in changes to their job responsibilities, a decline in morale, or a loss of faith in the firm.

Competitors

Stakeholders in the streaming sector might include more businesses. Their ability to compete with Netflix may have been harmed by the incident, which may have harmed Netflix's reputation or raised industry concerns about data security and privacy.

The participants

The researchers who participated in the Netflix Prize challenge had access to the data set and may have used it to develop algorithms and models. The breach potentially compromised the integrity of their work and could have resulted in financial or reputational damage for them.

Government Regulators

The government regulators who oversee privacy and data protection laws were also stakeholders. The breach potentially violated laws and regulations regarding data protection, and regulators could have acted against Netflix for any violations. As the authority who should've prevented this from happening, took too long to respond or act in the wake of such a scenario.

Shareholders

The Netflix stocks would've been affected because of this breach. The broken trust of the consumers and the public, in addition to the multiple class action lawsuits, must have resulted in a blow to the shareholders as the stocks of the company went in loss.

The Public

The incident may have garnered media notice, sparked consumer worry or indignation, or undermined public confidence in technology and online services.

Law enforcement agencies

Law enforcement authorities could be seen as stakeholders, depending on the particulars of the breach. They could investigate the incident to see whether any laws were broken or to find and bring to justice those in the wrong.

Insurance companies

Stakeholders may include insurance firms that offered coverage to Netflix or other impacted parties. Due to the breach, they can suffer financial damages or be required to settle lawsuits.

Ethical Issues Discussion and Analysis

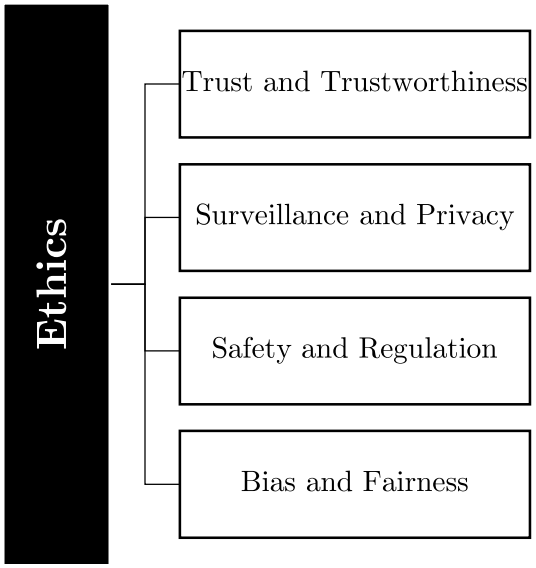


Figure 1. Different aspects in ethics

We can approach the Ethical Issues from four angles of Trust & Trustworthiness, Bias & Fairness, Privacy & Surveillance and Safety & Regulation.

Trust and Trustworthiness

Who owns the data generated by users' ratings on Netflix? Do users have a say in how their data is used, or do they lose control over their data once they submit it to Netflix? Were users able to contest or appeal decisions made by the algorithms?

What role do companies like Netflix have in promoting ethical data practices and privacy?

Utilitarian Perspective

While considering from the Utilitarian point of view, the ownership of the data would not hold high regards as the focus would be the benefit of the masses in the society. Thinking from the perspective of above questions, if the data is going to be used for good or resulted in the public good for the society, the question of ownership becomes irrelevant. Due to the release of the data, there was a huge amount of research conducted in the field of

recommendation systems. Netflix received more than 44000 submissions, which is a huge amount. It would have taken decades to generate this much research on this topic. In addition to that it is due to this competition that we were able to find out that such attacks and deanonymization was possible. So, the consumers might not hold the right to question the use of this data. Hence, from the utilitarian perspective there is no foul in the release of the dataset.

Deontology Perspective

From the Deontology point of view, the things that are wrong are wrong despite it bringing different benefits to the society. From this perspective the release of the dataset was wrong. The possibility that peoples or organizations could suffer harm because of their revealed movie-watching habits is not supported. A person's movie interests, for instance, might expose their political or religious beliefs, sexual preferences, or other sensitive information, which could be exploited against them or do them harm. A deontological perspective would reason that users should have complete control over their data as it is their personal information. Users should be able to decide how their data is used and could opt-out of data collection if they choose to do so.

Bias and Fairness

Is the dataset in the recommendation systems fair or biased? What kind of bias is laced in them and is it possible to get rid of it? Did Netflix really map the demographic appropriately? Doesn't it really lead to people data feeding ? Is it okay to employ biased algorithm?

There are multiple types of biases that are prominently seen in recommender systems.[8]

1. Clickbait Bias : A ranking mechanism that has clicks as positive feedback will be skewed in favor of clickbait. This is harmful because a strategy like that would encourage consumers to click on even more clickbait, amplifying the harm it does.
2. Position Bias : Position bias refers to when consumers begin to blindly accept the ranking they are being provided and the top-ranked items become the ones that generate the most interaction, not because they are the greatest content for the user, but rather just because they are listed highest.
3. Popularity Bias : Popularity bias is the inclination of the model to provide higher ranks to products that are more well-liked overall (because of having received more user ratings), as opposed to being based on their actual quality or relevance for a specific user.
4. Single interest Bias : Even though a person may have a variety of interests, a rating algorithm developed to optimize viewing time may overvalue drama films because

that is what the individual is most likely to watch. This is single-interest bias, which occurs when a model fails to recognize that people have a variety of interests and preferences by nature.

5. Duration Bias : Longer videos always tend to be watched for a longer time, not necessarily because they're more relevant, but simply because they're longer.

There are techniques to mitigate these types of biases, however it is difficult to completely eliminate them.

Utilitarian Perspective : From the Utilitarian perspective, it would be acceptable to employ a decently performing algorithm. For example, an algorithm that has an accuracy of 85% provides benefit to approximately 85% of the population. Hence, for the majority of people it would be positive. And it is with more usage and experimentation that we would be able to find the better alternative. So, deploying the current algorithm would be acceptable. Also looking at the content, people prefer watching content which is biased to their thinking, but some content might be providing benefit to the society if watched, for example an environmental awareness documentary. So, utilitarian perspective will call for provided such recommendations as well.

Deontology Perspective : From the deontological perspective, it would be wrong to deploy an algorithm that does not take minorities into account and doesn't consider everyone equally. It would also not be acceptable to recommend content which might not be based on their conditioning, for example the environmental awareness documentary. Deontology requires absolute respect for the individualism and privacy of a person.

Surveillance and Privacy

Did Netflix obtain informed consent from its users to release their movie rating data as part of the Netflix Prize contest? Did users have a choice to opt-out of having their data included in the dataset?

Utilitarian Perspective : Due to the release of the data, there was a huge amount of research conducted in the field of recommendation systems and Netflix received more than 44000 submissions which would have taken decades to generate this much research on this topic. In addition to that it is due to this competition that we were able to find out that such attacks and deanonymization was possible. Hence, the benefits outweighed the negatives. However, utilitarianism would ask the companies to ask for informed consent and not bury the privacy information in long privacy policy detailed documents.

Deontology Perspective : From the deontology point of view, the release of the data should not be done and the obtaining informed consent from users and respecting their

autonomy is paramount. Netflix should have clearly communicated to users that their data would be used for research purposes and given them the option to opt-out if they did not want to participate. Moreover, the deontological perspective would argue that users have a fundamental right to privacy and are adequately protected.

Safety and Regulation

Did Netflix take adequate steps to protect users' data from unauthorized access, theft, or misuse? Did Netflix comply with relevant privacy and data protection laws and regulations?

Who bears responsibility for the harm that has been caused? Is it the responsibility of Netflix or the Consumers?

What mechanisms exist to hold companies and researchers accountable for the ethical implications of their data practices and research activities?

Currently there exist guidelines published by the FTC in united states for Data security and privacy. However, they are guidelines to be followed at the discretion of the companies. There exist data privacy laws across the states but there is not a single law centrally implemented in USA[9].

Utilitarian Perspective : From utilitarian perspective, the law can be considered hazy and insufficient in a sense. Just because something fits the box set by law, may not mean that it is the ideal thing to do as the law surrounding the AI ethics and technology is still in development and incomplete due to the rapid development of technologies in the last decade. Hence, it is important for the companies to think about their actions extensively before they take any actions like this and be held accountable and responsible for their actions.

Deontology Perspective : From deontology perspective, Netflix followed all the necessary procedures, and the legal procedures were met. Deanonymization was done to protect privacy which was the benchmark at the time. So, one may not be able to blame them. It might be a failure of the regulatory system who failed to recognize the potential pitfalls of the same.

Individual Perspective and Discussion

Trust and Trustworthiness

I feel that in the current state of the capitalist economy and all the companies aiming to maximize their profits, it is really essential to protect our own privacy and be aware citizens. However, a significant portion of the responsibility lies with the companies and the regulators as just the general public opinion is not enough to drive such decisions. And it is extremely difficult to navigate the privacy policies. That is, even if we notice some loophole in it, the applications today do not let us proceed to the next step without accepting it. We are forced to accept or not to use the application. And is it really feasible to give up on using these applications as they become more and more integrated with out day to day lives. Can we really avoid filling hospital records in the fear of our sensitive information leaking? In a way we are forced to trust these organizations and accept the policies as they are without question. This needs to change and we need to make a choice to opt- out of mandatory voluntary data collection.

Bias and Fairness

Bias is an integrated part of our daily life. We humans are conditioned to bias, and in a way, our identities are a bias. Without bias, all humans would be the same. Bias adds uniqueness to us. It is impossible to make a perfect system free of bias. All the systems are going to have a bias. But we need to try to make these systems as close to perfect as we can. It is unacceptable for the systems to exhibit discrimination of any kind against any kind of groups. Hence, I believe that such systems should be deployed but should be constantly under research and be monitored for their behavior and be improved consistently. For example, ChatGPT that was launched showed inappropriate responses in some situations. Does that mean that the ChatGPT should not have been deployed? As a process of improvement, the involvement of the public was necessary. Same was true with the Netflix case. The involvement of the public sector was necessary to understand some key points in my opinion, else it would've been very difficult to understand something like this could have been possible. We need to be aware and understand that such bias exists.

Surveillance and Privacy

I believe there need to be stricter laws for data protection and privacy and that companies should not be allowed to track the personal information of people. One method would be

to create and mandate third-party data security organizations so that all the necessary tracked data cannot be utilized by these companies for their own benefit. This would also avoid occurrence of situations like this where liability and accountability are hazy. Data collection cannot be avoided as we progress in digitization. Hence instead of trying to avoid it altogether, we need to adopt policies that would avoid situations like the Netflix prize breach from happening.

Safety and regulation

I think that the current law and regulations are unable to keep up with the rapid developments of technology and a lot more investment in regulation is needed to protect the citizens from potential pitfalls of the same. Citizens often place their absolute faith in these organizations hence they should be responsible and accountable towards the public. That is, whenever we see the label that a certain medication or food item is FDA approved, there is a certain amount of trust established. Hence these organizations need to maintain their standards for the benefit of the public.

References

1. Rahman, W. (2020, June 18). The Netflix prize-how even AI leaders can trip up. Medium. Retrieved February 25, 2023, from https://towardsdatascience.com/the-netflix-prize-how-even-ai-leaders-can-trip-up-5c1f38e95c9f

2. Wikipedia Contributors. (2019, September 24). Netflix Prize. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Netflix prize Ravens, E. L. T. -. (2022, July 2). Data Privacy — The Netflix Prize competition. Medium. https://medium.com/@EmiLabsTech/data-privacy-the-netflix-prize-competition-84330d01cc34

3. Netflix: Designing the Netflix Prize Case Solution And Analysis, HBR Case Study Solution Analysis of Harvard Case Studies. (n.d.). Www.thecasesolutions.com. Retrieved February 25, 2023, from https://www.thecasesolutions.com/netflix-designing-the-netflix-prize-167891

4. Narayanan, A., Shmatikov, V. (2006). How to break anonymity of the netflix prize dataset. arXiv preprint cs/0610105.

5. Archie, M., Gershon, S., Katcoff, A., Zeng, A. (n.d.). Who's Watching? De-anonymization of Netflix Reviews using Amazon Reviews. Retrieved February 25, 2023, from https://courses.csail.mit.edu/6.857/2018/project/Archie-Gershon-Katchoff-Zeng-Netflix.pdf

6. Solon Barocas, Moritz Hardt, Arvind Narayanan (2019). Fairness and Machine Learning: Limitations and Opportunities. fairmlbook.org.

7. Netflix Prize data. (n.d.). Www.kaggle.com. https://www.kaggle.com/datasets/netflix-inc/netflix-prize-data

8. Makadia, A. (2020, January 17). Biases in Recommender Systems: Top Challenges and Recent Breakthroughs. Towards Data Science. https://towardsdatascience.com/biases-in-recommender-systems-top-challenges-and-recent-breakthroughs-edcda59d30bf

9. Osano. (n.d.). Data Privacy Laws: A Comprehensive List. https://www.osano.com/articles/data-privacy-laws