

# Privacy Impact Assessment

# YouTube's

# Recommender

# System

---

Milton Ossamu Tanizaka Filho

Carlos Sebastian Michels Alfaro

Privacy and Big Data - KU Leuven

4th January, 2021

**KU LEUVEN**

## Contents

<b>Introduction</b>	<b>2</b>
<b>Application description: YouTube</b>	<b>2</b>
High Level Functionality	2
Data collection and Implementation of the Recommender System	6
Stakeholders	9
<b>Privacy Impact Assessment of YouTube's Recommender System</b>	<b>10</b>
Introduction and High Level Analysis	11
Trust Assumptions	12
Definition of Threat Models and Types of Attacks	13
Figure 10. Threat model of injection attack against recommendation models	13
User Activity Controls	13
Assessment of YouTube's Recommender System Privacy Aspects	16
Account Integration	16
Wealth of Collected Data	17
Data Retention Periods	17
Data Storage	18
Third-Party Sharing	18
Analysis on Controls	18
Analysis on Consent	19
Friendly Interface for the Privacy Policy	19
Legal Analysis	20
Ethical Analysis	21
Recommendations	21
Incognito mode	21
Data retention	21
Minimum data collection and usage	22
Objective of the recommendation	22
<b>References</b>	<b>23</b>

## Introduction

YouTube was created in February 2005 with the purpose of allowing anyone to upload and share videos. The streaming platform rapidly grew and its immense success attracted attention from companies such as Google, which acquired YouTube in November 2006 (Hosch, 2009).

In order to monetize and improve YouTube, Google implemented many features such as the recommendation system, which is an algorithm that generates personalized content to the user based on their interests. According to Google, over 70% of the content watched on YouTube was triggered by its recommendation algorithm (Popken, 2018).

Even though recommendation engines can offer convenience, it raises many ethical and privacy concerns relating to addictiveness, inappropriate content, and personal data collection.

## Application description

A recommender system algorithm attempts to **offer specific content** by **comparing the user** profile with some **reference characteristics**. The way YouTube categorizes relevant content for each user is dynamic and has evolved along the time; at the early stages it was based on view counts, then duration was included into account (Cooper, 2020). The current version of the recommender system is run on a deep neural network algorithm that also considers as input users behaviours (Kumar, 2020) such as:

- clicks, watches, etc.
- likes, dislikes, dismissals, etc.

## Functionality

According to YouTube, the algorithm is “real-time feedback loop that tailors videos to each viewer’s different interests.” It decides which **videos and advertisements** will get suggested to individual users.

As for **videos**, the algorithm’s goals are twofold: find the right video for each viewer, and get viewers to keep watching (i.e. maximize engagement time). Therefore, the algorithm monitors user behavior and interactions as closely as it evaluates video performance.

The two most important places the algorithm impacts are **search results** and **recommendation streams** (Cooper, 2020):

**Search results** may differ for each user based on the inferences from the recommendation system. For example, if a user watches a lot of sports videos and searches for 'cricket', YouTube might recommend videos featuring the sport cricket rather than nature videos with crickets in them (YouTube official site, 2020: YouTube Search). This is shown in Figure 1 below.

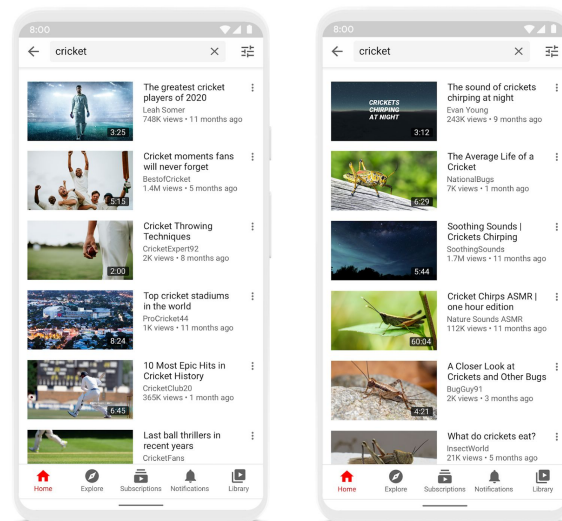


Figure 1: Search result examples for the query of “cricket” - source: YouTube

**Recommendations** appear both on YouTube's homepage and in the 'Up next' section as a suggestion of what to watch next when a user is watching a video (YouTube official site, 2020: Recommended videos). Recommendations will play automatically (Autoplay default option). Inferences will also be used for ad personalization (if Ad personalization is on - default option). An example of them is shown in Figure 2.

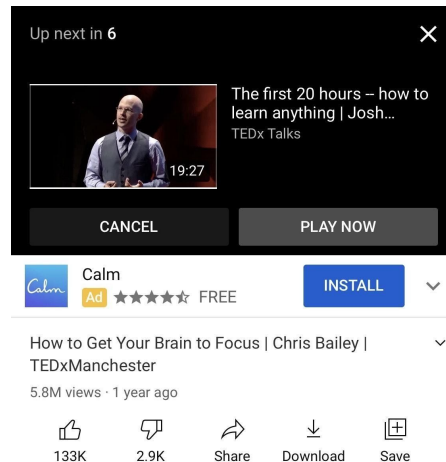


Figure 2: Example of how 'Up next' video and Ad recommendation

The recommender system considers watch and search history (if enabled - default) and channel subscriptions. Context and user information is also considered (e.g. country and time of day). For example, this helps to filter locally relevant news. Also, YouTube's recommender considers whether others who clicked on the same video watched it to completion – a sign that the video is higher quality or enjoyable – or just clicked on it and shortly after starting to view the video, clicked away. (YouTube official site, 2020: Recommended videos) A high level diagram of the recommender system interactions is illustrated in Figure 3 below.

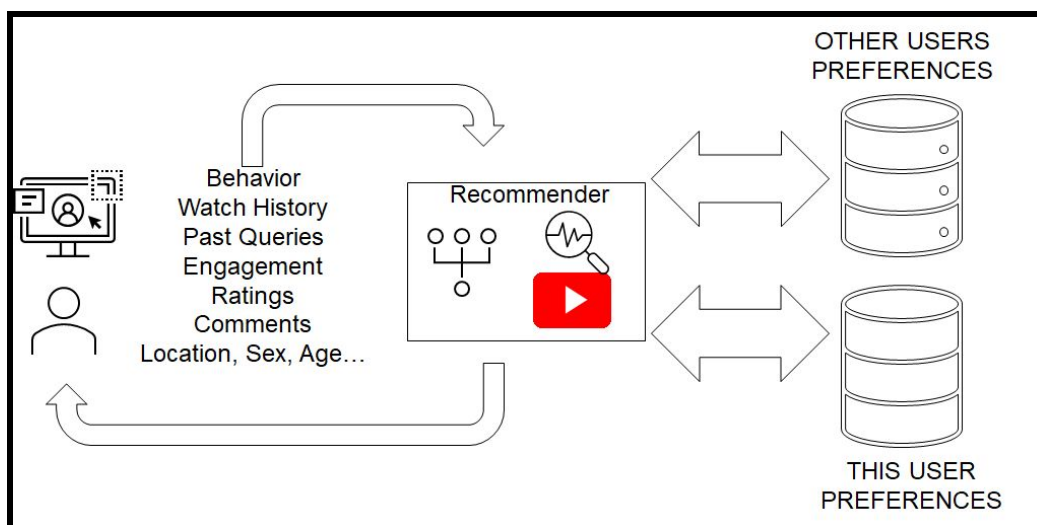
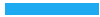


Figure 3: General Illustration of YouTube's Recommender System.



The same data collected about the user may be used to recommend **advertisements** to the user. In 2014, the platform introduced an optional **YouTube Premium** subscription, allowing viewers ad-free videos and some additional functionalities. YouTube Premium users only see branding and promotions from content creators; while the interruptions by ads before and during a video, including video overlay ads, are disabled.

## Data collection and Implementation of the Recommender System

YouTube's recommendation system is constantly improving. Covington et al. (2016) described the most recent algorithm, which consists of two neural networks as shown in Figure 4 below.

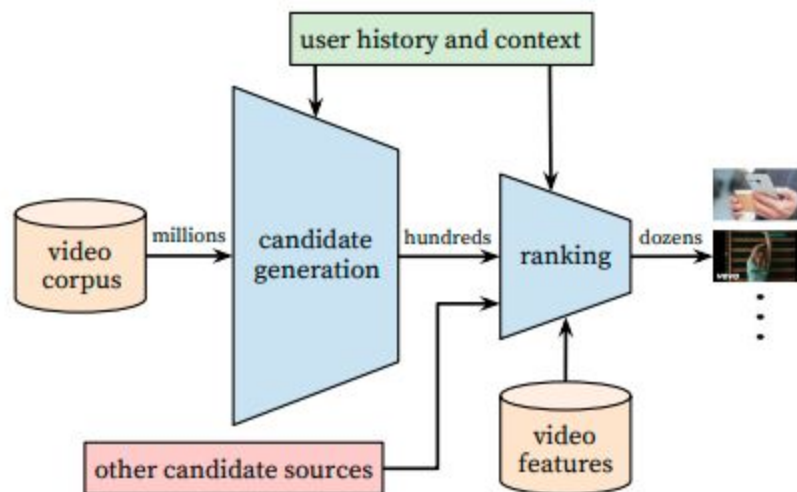


Figure 4: Recommendation system architecture demonstrating the “funnel” where candidate videos are retrieved and ranked before presenting only a few to the user.

The candidate generation network receives millions of videos and events from the user's activities as inputs and outputs a subset of relevant videos. Personalized content is performed with collaborative filtering, which considers similarity between users by their video watches, search queries and demographics. This network uses explicit inputs such as thumbs up/down, and in-product surveys as well as implicit data like completion and repetition of videos, geographic region, device, gender, logget-in state, and age.

The ranking network receives a small set of possible relevant videos along with other sources (Davidson et al., 2010) ; the highest scoring video is presented to the user.

More details of the information collected are displayed in Figure 5 (explicit/implicit data).

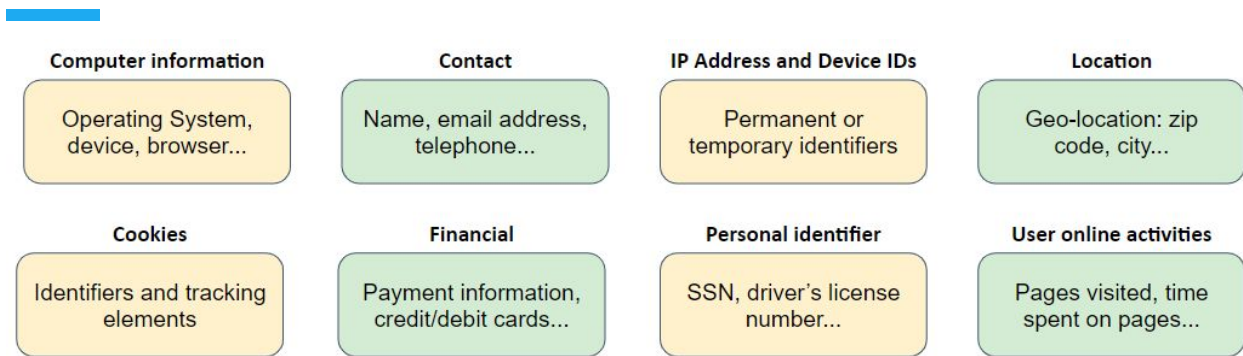


Figure 5: Type and info of the data collected

The type of data collected and where it is employed can be easily visualized on the flowchart of Figure 6 (<https://priebot.org/polis/sis>). Most of the data is used for analytics research, followed by additional service features. Applications are illustrated in figure 7.

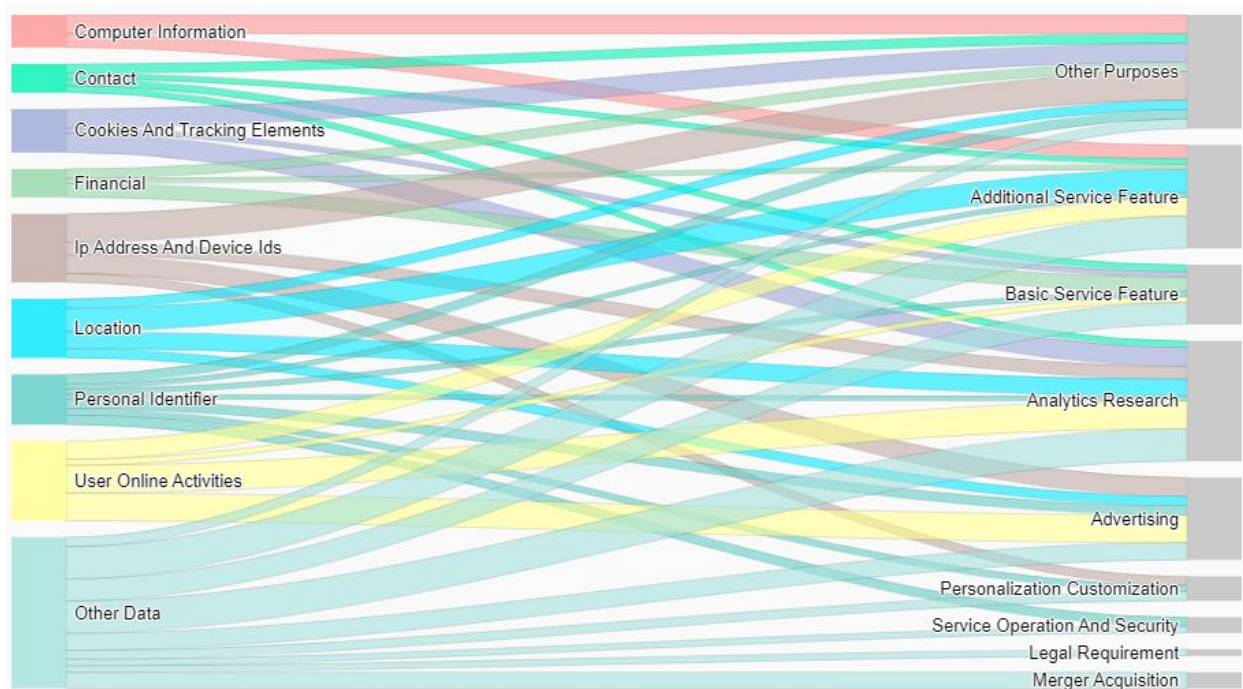


Figure 6: Flow diagram expliciting flow of data for each application



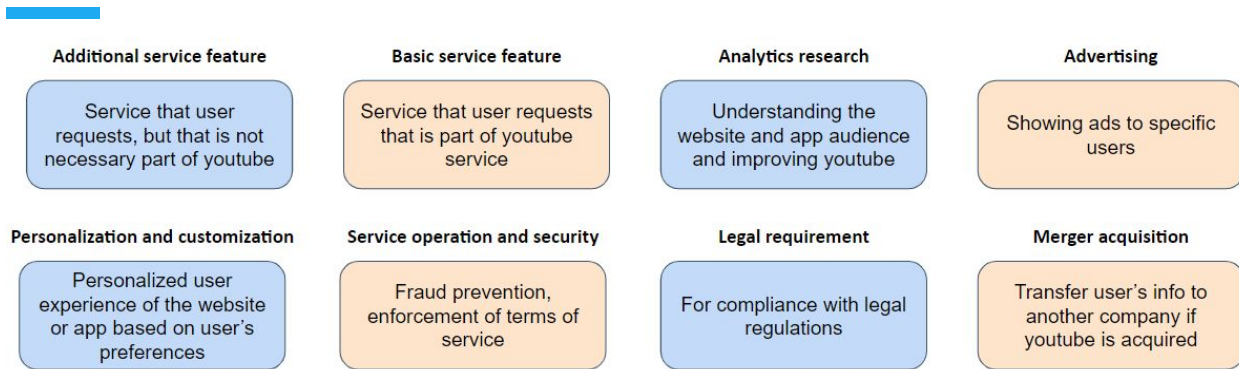


Figure 7: Type and reason to collect data

YouTube also shares data with third parties. The data shared are:

- Cookies and tracking elements: user identifier and info are shared to advertisers, so they can better direct specific ads and videos; they are also used in analytics research to better understand the audience, analyze traffic, and optimize product design.
- User online activities: information such as number of pages visited and general user behavior can also be used by advertisers for the same purposes

## Stakeholders

The stakeholders are the users, YouTube, creators, advertisers and regulators. Both users and creators are stakeholders with privacy needs.

This PIA focuses on 'signed in' users. Users interact with YouTube and the creators by providing attention (i.e. activity time) and in some cases subscribing to services or buying products. In turn, they will receive recommended video content and ads.

Content creators are users who actually upload videos. They receive payments from YouTube and Advertisers. There is also a data exchange among them. Content creators must comply with YouTube's terms of use.

Service provider is represented by YouTube, owned by Google. The service provider provides the platform and user base to content creators and advertisers. YouTube interacts with regulators by participating in the regulatory process and through compliance. Regulators impose legal framework and supervise compliance for the platform

Another group of stakeholders are the advertisers who pay to promote their products and services through the recommender system or directly through content creators.

YouTube also interacts with all stakeholders by supervising compliance with the Terms of Service and Community Guidelines.

The relations and flows between stakeholders, as well as the place of YouTube's recommender system are shown below in the 'Figure 8: YouTube stakeholders'.

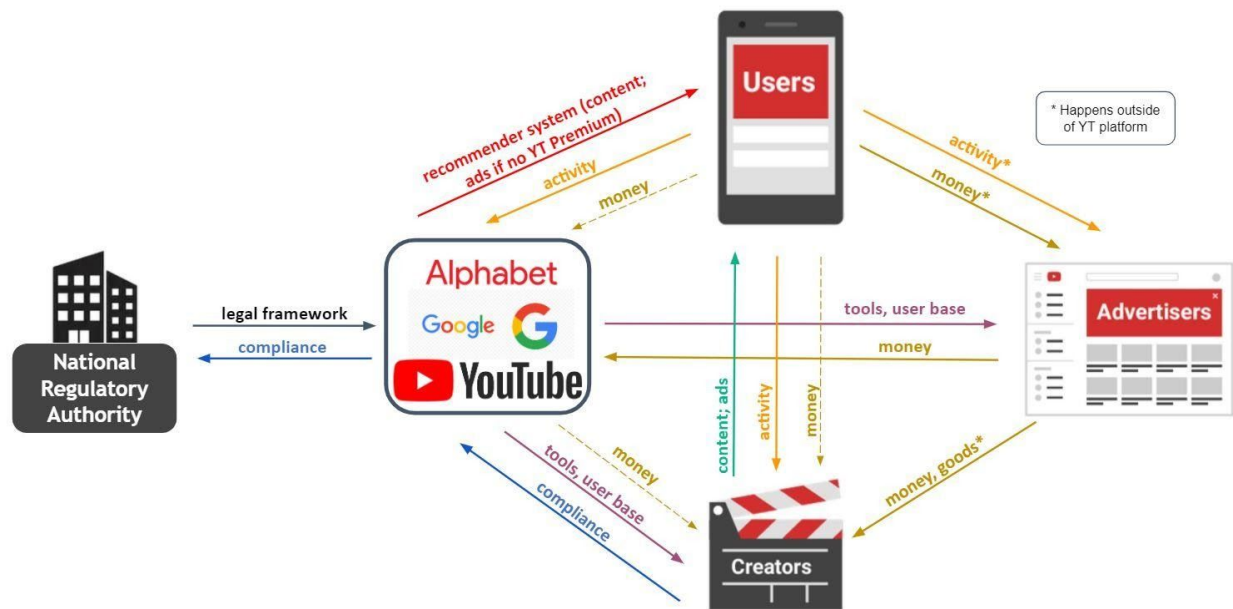


Figure 8: Relationship between privacy-concerned stakeholders for youtube (dashed line is optional)

# Privacy Impact Assessment of YouTube's Recommender System

## Introduction

Recommender systems have already been scrutinized for privacy and unethical practices (Tufekci, 2018) (de Leon, 2019) (Roose, 2019). This PIA considers a broad definition of privacy, where actions that intend to influence the user's behaviour are considered a form of attack (privacy is an enabling right to human autonomy, hence actions or systems that could hamper self-determination could be privacy-threatening).

Recommender systems are subject to privacy concerns as their main aim is to guess the user's preferences. Therefore a privacy attack in the recommender system could disclose the users' personal interests and affiliations (sensitive information). This information may be abused (e.g. sold to third-parties), stolen by an adversary (security breach on the recommender system) (Wang et al., n.d.) or inferred by comparing with complementary information (e.g. channel subscriptions).

Privacy concerns can also be thought of influencing the users' behavior via exposure to extreme, biased or inappropriate content. This has been a controversial aspect of YouTube's recommendation system. We identify the 2 different ways privacy can be violated:

- **Identification of User's preferences:** The recommender system information is undeniably sensitive. It embeds users' preferences and affiliations. If an adversary is able to link preferences to specific users (leakage, using external info), this could be used to infer the users' opinions on sensitive topics (e.g. political party affiliation) and discriminate against them.
- **Behavior Influence:** The recommender system tries to maximize screen time (and not to recommend content based on "quality"). This can lead to extremist, biased or inappropriate content being overly recommended (Nikas, 2018) (de Leon, 2019). The more the user is exposed, the more the algorithm learns to recommend extreme content. The disproportionate exposure to extreme content can act as a positive feedback loop and influence the user behavior (echo chamber) (Chaslot, 2019) (Jiang et al., 2019). We state that recommender system biasing or influencing users' behavior can be seen as an attack on users' privacy. This kind of attack is illustrated on figure 9.

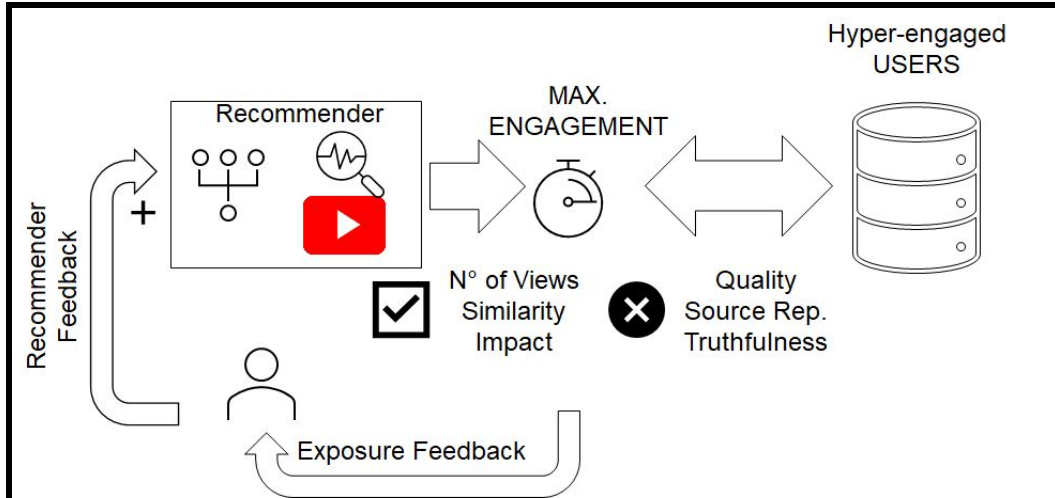


Figure 9: Illustration of positive feedback loop for extreme content due to the algorithm engagement time maximization.

Hence, a **privacy-preserving recommender system** not only reduces to minimum the possibility and consequences of sensitive data leakage (e.g. our preferences), but also includes **privacy-preserving goals in its recommendation algorithm** to avoid harmful positive feedback in content exposure. This written assignment intends to elaborate on both topics.

## Trust Assumptions

Google provides several measures to ensure the data of its services are protected. Some of them are data encryption, safe browsing, and 2 step verification. Access to personal information is restricted only to Google employees, contractors, and agents that are subjected to strict contractual confidentiality obligations.

In case of data leakage, the encryption prevents that attackers have access to the information as it is assumed that the encryption cannot be broken. Also, information is only shared and used according to YouTube's policy.

In this PIA it is assumed that barriers protecting user privacy and data put in place by YouTube and the user (e.g. user password is strong and confidential) hold true, as well as confidentiality instructions are obeyed. It is also inferred that Google is committed to communicating any suspicious activity to warn the user.

## Threat Models and Types of Attacks

The candidate generation step of YouTube's recommender system applies collaborative filtering to learn similarities among users based on their patterns. However, this technique enables an adversary to perform passive privacy attacks. This allows anyone with little amount of the background knowledge of the victim to infer a user's transaction and behavior (Chen et al., 2014).

Users and creators are subject to attacks, since anyone could use their auxiliary public information like videos uploaded, playlist, channels, or discussion to combine with users collaborative filtering and identify the user. Normally "less conventional" users are easier targets of such attacks.

Figure 10 illustrates an attack on a recommender system. The adversary could use a local model (a.k.a. surrogate model) to craft fake data and inject them into the training data that will feed the neural network model and produce biased outcomes. In practice, the model will produce biased recommendations that may influence the behavior of the victim (Tang et al. 2020).

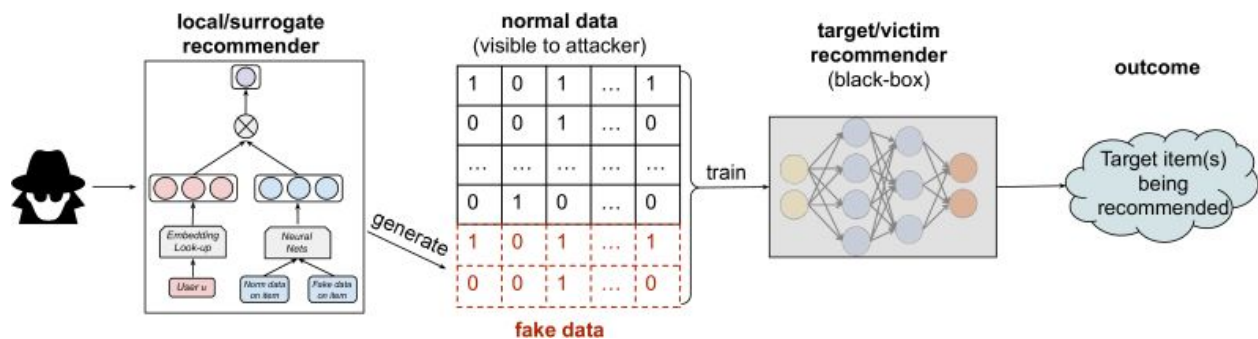


Figure 10. Threat model of injection attack against recommendation models (Tang et al. 2020)

Finally, Google's account integration and unique username could allow to cross-correlate information between Google services (public and/or leaked - e.g. reviews on Google Maps, visited places) with YouTube.

## User Controls

A logged in user can access several controls in their youtube account. The user can access privacy controls through their YouTube and Google account configuration (including “Your Data in Youtube”).

On YouTube level the user can:

- Subscribe to YouTube premium service (which could be considered a kind of opt-out as limits the ad recommendation functionality of the Recommender System)
- Activate, deactivate and delete watch and/or search history (all history or individual searches). This option is activated by default (less private)
- Set up an auto-deletion period for the watch and search history (3, 18 or 36 months). This option is deactivated by default (less private)
- Change privacy level of videos, reproduction lists and subscription. Content is set up public by default (less private)
- Administrate comments (only public)
- Download YouTube dashboard containing data on personal comments, uploaded videos and channels the user is subscribed to.

On Google level, the user can change the following settings for all google services:

- Web & App Activity,
- Location
- Ad personalization
- Download all the user information

An interesting option is to take a guided privacy checkup to manage privacy settings. This is a way to educate users on the most-suitable privacy settings. During the execution of this PIA, Google updated the Privacy Checkup functionality to include personalized privacy suggestions.

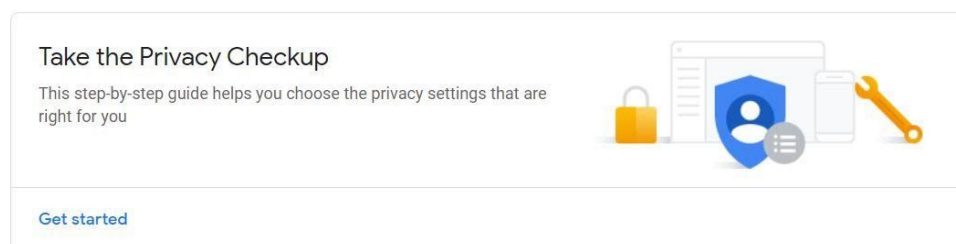



Figure 11. Privacy Checkup on the official site of Google Account settings

The YouTube Kids offers additional privacy settings and controls, but is out of the scope of this PIA.

← Remove YouTube content



Hide or delete your content from YouTube

You're about to hide or delete your YouTube content for **Sebastian Michels Alfaro** ([sebastianmichelsa@gmail.com](mailto:sebastianmichelsa@gmail.com)).

Please choose one of the options below.

I want to hide my channel

I want to permanently delete my content

This will permanently delete the YouTube data associated with **Sebastian Michels Alfaro** ([sebastianmichelsa@gmail.com](mailto:sebastianmichelsa@gmail.com)).

Select all of the following to confirm that you understand.

☐ The following will be **permanently deleted**:

- Your 2 videos
- Your 3 playlists
- Your 56 subscriptions to other channels
- Comments that you made on YouTube
- Your replies and thumbs-up on comments
- Your messages
- Your search and watch history

[DELETE MY CONTENT](#)

Figure 12. Functionality to remove YouTube content



## YouTube's Recommender System Privacy Assessment

This section will analyze privacy concerns regarding YouTube's recommender system.

### Account Integration

A key aspect from the privacy point of view is the integration between Google services accounts. Collected data and inferences from the recommender system could be shared seamlessly between different services. In fact, Google's privacy policy is unique for most services. Unique user identifier between accounts leads to enormous inferences possibilities when combining data.

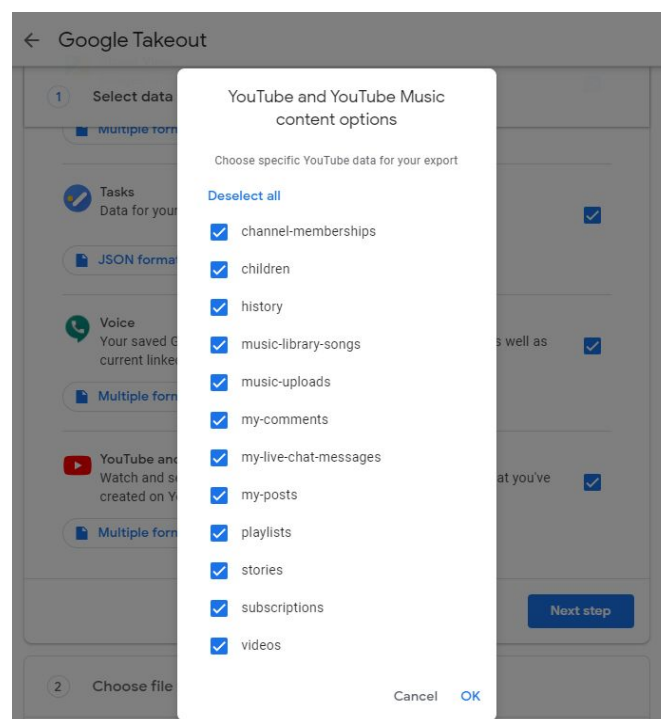
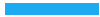


Figure 13: Integrated environment for personal data management.

The recommender system could infer preferences from the users' complete Google account activity. Potential leakage becomes more dangerous as data is not limited to one service but to the Google account.

### Data Collection

YouTube and Google collect an immense wealth of data. This data includes several unique identifiers and pseudo identifiers that would allow easy identification of a user (e.g. name, email, telephone number, country of residence, address, financial information). Collected data includes most of the user interaction within YouTube, including explicit and implicit preferences.



Only a fraction of the data collected serves the purpose of providing a service feature (incl. content personalization). Most data (including personal identifiers, location, activity...) is also purposed for analytics research, advertising and monetization purposes,(i.e. core service features or experience could be maintained with less data collection).

## Data Retention Periods

According to Google's privacy policy, data retention periods will depend on the type of data. Some data retention period is controlled by user deletion (i.e. indefinitely if user does nothing), other data has a predetermined expiration timeframe and other data is retained until the deletion of the linked Google account (i.e. indefinitely). Google also mentions that in some cases data is not deleted but anonymized (for example, by deleting IP addresses).

Normally, search history and activity can be deleted by user controls. Technical data such as browser data, cookies, IP address will be deleted or anonymized after a predefined period. Personal identifier, business data, and user analytics (how often you search a term, but not what you searched) is kept until Google account deletion. Google's policy states that *"We keep some data for the life of your Google Account if it's useful for helping us understand how users interact with our features and how we can improve our services"*.

Recommendations and preferences inferred through the recommender system are constantly generated and updated (Davidson et al., 2010)<sup>1</sup>. In summary, in YouTube most of user sensitive data is stored indefinitely<sup>2</sup>.

## Data Storage

Even though some data is stored locally, most of data is stored in YouTube's servers so it can be shared across different user devices and sessions. Recommendations and user inferred preferences are also stored remotely. Data copy and dissemination reduces de control over the user's personal data (privacy concern).

---

<sup>1</sup> As the recommender system is constantly evolving, we assume this still holds true.

<sup>2</sup> Other services like Google Analytics have a different data retention period, for example 26 months <https://support.google.com/analytics/answer/7667196?hl=en>

## Third-Party Sharing

YouTube claims they don't sell or share your personal information with companies, organizations, or individuals outside of Google. However, the privacy policy includes several exceptions:

- User has given explicit consent for sensitive data sharing
- External data processing (trusted partners), based on instructions of compliance (external service providers)
- When data disclosure is justified for legal reasons (e.g. fraud detection)

Finally, YouTube may share “non-personally identifiable information” publicly or with their partners (e.g. advertisers). Non-personally identifiable information is information that no longer reflects or references an user's individual identifications. However, as history has demonstrated (e.g. Netflix - IMDB attack), it is extremely difficult to anticipate all kinds of attacks that could allow to reconstruct personal identifiers from anonymized datasets. This is a privacy concern.

## Consent

User consent is requested in the terms of use of Google services. However, Google privacy policy is redacted in a broad way to avoid the recurrent request of consent (Mattan, 2019). According to Mattan, consent “*no longer effectively protects personal privacy in our present data-rich world*”. This is a concern as third-party sharing is authorized via consent of the user (probably given automatically when agreeing with the terms of services).

## Privacy Policy

We find the Privacy Policy is clear and accessible for an average user. The text is well structured, it offers some visuals and there are video explanations of key concepts.

However, given the myriad of privacy contracts we are exposed, research shows that most people don't bother with privacy policies<sup>3</sup>. Anyhow, YouTube makes available a wide range of material to educate its users regarding privacy and data collection. However, it is very likely that the average user has limited knowledge about the general privacy aspects concerned by the

---

<sup>3</sup> [This article](#) affirms that more than 91% of users don't read privacy policies. [This other article suggests](#) that reading a privacy policy takes around 20 minutes.

terms of service and the recommendations provided ( exposure to biasing content, sharing of information to advertisers and creators, etc. )

## Anonymization Techniques

Google mainly applies two anonymization techniques across its products in order to protect data of its users (Google, 2020).

- Generalizing the data: Google holds much personal data of individuals that could be easily used to identify the user. Generalization aims to remove or replace a portion of the data to difficult the identification of the user. Some techniques applied are k-anonymity and l-diversity, to mitigate the risk of sensitive information being used to reveal individuals.
- Adding noise to data: Google has its own [open source differential privacy algorithm](#) that adds mathematical noise to data. It was designed to not interfere in measuring overall trends, but it has a counterpart of making the dataset less useful than the original one.

## Legal Analysis

GDPR is the applicable framework as YouTube has economic activities within the EU geographical area and the recommender system relies on automatic data collection systems.

Google is the main responsible for users' data (controller). Third parties can act as data processors. In the case third parties are located outside the EU, GDPR demands that data protection warranties apply (e.g. contracts). Google claims they provide "industry-standard contractual protections" to be compliant with data protection laws, including GDPR.

Regarding GDPR's purpose limitation principle, the purpose of data collection is explained in the privacy policy, however a key aspect is its broadness, justified by the wealth of services provided (account integration). According to the GDPR, the purpose of data collection should be "explicit, specific and legitimate". Explicitness and legitimacy are probably not arguable, but specificity is. The privacy policy is outlined in a high-level way that hinders challenging the data collection.

A similar phenomena occurs regarding "Data Minimization", as collected data shall be "limited to what is necessary in relation to the purposes". It is possible to argue that core functionalities, including the recommender systems are still possible with much less data. However, data minimization could restrict the recommender system functionality. In our opinion, high-quality recommendations are possible with less data or account integration.

GDPR states that data processing is legal only in certain circumstances. User's consent is a key enabler of legality of data processing. Consent is requested when accepting Google's terms of

services “for all services included in this privacy policy”. Google says explicitly that they will ask consent “whenever data usage goes beyond the privacy policy or the privacy policy is updated”.

Legality of data processing under GDPR also comes from the “legitimate interest of the controller”. YouTube users must be above 13 years (legitimate interest is not applicable when the data subject is a child). A separate service with special privacy provisions is available for children.

Special categories (e.g. racial or ethnic origin, political, religious or philosophical beliefs) of data shall not be processed. The Recommender System can infer this information from user activity (e.g. political affiliation can be inferred from reproduction history). This data is not disclosed as preferences are kept inside the recommender system algorithm, so it does not fall directly under GDPR.

Article 12 established that information related to data processing shall be transmitted in a “concise, transparent, intelligible and easily accessible form, using clear and plain language”. This is achieved within the policy of Google, as we already discussed in a previous section.

The storage limitation principle (“data to be retained no longer than is necessary for the purposes for which the data were collected”) is not respected, as most of the data is retained indefinitely. However, it can always be argued that to provide recommendations it is necessary to have the full history of data.

Default settings in user controls are set to the least private setting. However, as watch and search history and user activity are not directly disclosed (unless anonymized), GDPR does not force privacy by default. However, subscriptions and reproduction lists are displayed publicly in an automatic way. This seems in contradiction with privacy by default principle.

## Ethical Analysis

YouTube’s recommender maximizes user attention by optimizing engagement functions (clicks, time spent) and satisfaction objectives (likes, dismissals). However, the objective of a recommended content may raise the ethical question of whether the recommendation tries to entertain or deliberately tries to manipulate the user. Quality or truthfulness of the content is not taken into account into the recommendation itself.

According to a former engineer at YouTube<sup>4</sup>, AI is not built to help customers get what they want, but to get them addicted to YouTube. This is of special concern for vulnerable users (e.g. teenagers).

Moreover, a search can quickly drift from naive or mild content towards extremist or conspiratorial material.

The above poses strong ethical concerns and conflict of interest between the users and Youtube (e.g. wellbeing vs monetization). This has been recognized by Youtube, and attempts for correction have been done. Youtube states their recommendation systems are audited to ensure and correct unintended biases (e.g. genders or political perspectives).

## Recommendations

In this section some recommendations and improvements are presented in order to mitigate the main privacy issues that were raised along the PIA.

### Incognito mode and privacy by default

YouTube provides an incognito mode, when it is activated, YouTube does not use any personal data to influence the user experience. This is only available on mobile devices. The recommendation is to allow incognito mode on any device without relying on the browser. The user shall be asked for every session if incognito mode is desired.

Finally, all privacy related settings should be set at maximum by default.

### Data retention

To allow users automatic deletion of their account data by a certain period (not only watch and search history). Impact on the Recommender System would be limited since recent data is preferred by the algorithm.

### Minimum data collection and usage

The recommender system uses a variety of data. However, one may not be comfortable sharing a location to bias a recommendation. “Privacy by Design” best practices suggest that one could be able to select which information is shared to get recommendations, so the system will only use the minimum data that the user allows.

---

4

<https://singularityhub.com/2019/10/17/youtubes-algorithm-wants-to-keep-you-watching-and-thats-a-problem/>

## Objective of the recommendation

The current version of the recommender system suggests contents according to YouTube's criteria. It is recommended enabling users to choose which criteria is included in the recommendation, to better control and avoid undersided suggestions.

It is recommended that wellbeing of the user is included in the goal of the recommender system (e.g. stop recommendations after 1 hour of activity). A measure of truthfulness of the content could be included to reduce recommendations that spread misinformation (we imagine this is very challenging to implement). This could be thought as a privacy-oriented objective function of the recommender system.

## Mandatory privacy check up

To make the privacy check up mandatory for all users for the first time and every time the privacy policy and terms of service change. This could be complemented by a mandatory 5 minutes video that explains the privacy policy and ethical issues of the recommender system.

## Conclusions

YouTube has enabled new dimensions on content and information sharing. Its recommender system is able to deliver high-quality content tuned to each individuals' preferences. However, strong privacy concerns arise as recommender systems infer users' preferences and for that purpose, collect immense amounts of data. Furthermore, attacks that can be used to influence users' behavior via the content they receive.

The broadness of provided services hinders some data protection principles such as data minimization and storage limitation. YouTube's privacy policies are high-level and englobe a variety of activities and services. Google's account integration is central to this issue.

Ethical concerns also arise from this recommender system as increased exposure to biased, extreme or untruthful content. Similarly, as engagement time maximization could be completely opposite to the users' real wellbeing.

Several recommendations were made to minimize data collection, reduce retention times, and improve the quality of recommendations with a perspective on quality and user wellbeing.

## References

- Chaslot, G. (2019, July 13). The Toxic Potential of YouTube's Feedback Loop. Wired.  
<https://www.wired.com/story/the-toxic-potential-of-youtubes-feedback-loop/>
- Chen, R., Xie, M., & Lakshmanan, L. V. S. (2014). Thwarting Passive Privacy Attacks in Collaborative Filtering. Database Systems for Advanced Applications, 218-233.
- Covington, P., Addams, J., & Sargin, E. (2016). Deep Neural Networks for YouTube Recommendations. RecSys.  
<http://static.googleusercontent.com/media/research.google.com/en//pubs/archive/45530.pdf>
- Cooper, P. (2020, August 18). How Does the YouTube Algorithm Work? A Guide to Getting More Views. Hootsuite. Retrieved 10 25, 2020, from  
<https://blog.hootsuite.com/how-the-youtube-algorithm-works/>
- Davidson, J., Liebald, B., Liu J. and others. (2010, April 24). The YouTube Video Recommendation System
- de Leon, H. The Ethical and Privacy Issues of Recommendation Engines on Media Platforms. Towards Data Science.  
<https://towardsdatascience.com/the-ethical-and-privacy-issues-of-recommendation-engines-on-media-platforms-9bea7bcb0abc>
- Google Account site / Data and Personalization section, accessed on Nov 15, 2020  
<https://myaccount.google.com/data-and-personalization>
- Google Privacy Policy, accessed on Nov 15, 2020 <https://policies.google.com/privacy>
- Google promises to give users more control of data, accessed on Nov 15, 2020  
<https://www.ft.com/content/65a20d1c-7159-11e9-bf5c-6eeb837566c5>
- How Ads Work on YouTube (2019) by YouTube Creators  
<https://www.youtube.com/watch?v=WPR9PCoeqog>



Hosch, W. L. (2009, August 06). YouTube. Britannica. Retrieved 10 25, 2020, from

<https://www.britannica.com/topic/YouTube>

Kumar, A. (2020, January 30). YouTube's Recommendation Engine: Explained. Hackernoon.

Retrieved 10 25, 2020, from

<https://hackernoon.com/youtubes-recommendation-engine-explained-40j83183>

Official site: YouTube Search, 2020

[https://www.youtube.com/intl/en\\_be/howyoutubeworks/product-features/search/#overview](https://www.youtube.com/intl/en_be/howyoutubeworks/product-features/search/#overview)

Official site: YouTube Recommended Videos, 2020

[https://www.youtube.com/intl/en\\_be/howyoutubeworks/product-features/recommendations/#overview](https://www.youtube.com/intl/en_be/howyoutubeworks/product-features/recommendations/#overview)

Nikas, J. (2018, February 7). How YouTube Drives People to the Internet's Darkest Corners. The Wall Street Journal.

<https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478>

Popken, B. (2018, April 19). As algorithms take over, YouTube's recommendations highlight a human problem. NBC News. Retrieved 10 25, 2020, from

<https://www.nbcnews.com/tech/social-media/algorithms-take-over-youtube-s-recommendations-highlight-human-problem-n867596>

Roose, K. (2019, June 8). The Making of a YouTube Radical. The New York Times.

<https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html>

Tang, J., Wen, H., Wang, K., (2020, August 11) Revisiting Adversarially Learned Injection Attacks Against Recommender Systems. RecSys.

Tufekci, Z. (2018, March 10). YouTube, the Great Radicalizer. The New York Times.

Using YouTube Premium benefits, accessed on Nov 13, 2020:  
<https://support.google.com/youtube/answer/6308116?hl=en>

Wang, C., Zheng, Y., Jiang, J., & Ren, K. (n.d.). Toward Privacy-Preserving Personalized Recommendation Services. *Engineering*, 4(1), 21-28.