

Date: 28 May 2025

Exploratory Study of Manipulative Design

*By Chitra Mohanlal, tech-
researcher*



CONTENTS

1. MANAGEMENT SUMMARY	04
What are the main insights from the study?	04
2. BACKGROUND AND OBJECTIVE	06
Why this study?	06
3. DEFINITIONS	07
What is the scientific and legal framework?	07
3.1 Manipulative design	07
3.2 Deceptive patterns	08
3.3 Attention capturing damaging patterns	12
4. STUDY APPROACH	15
How did we conduct the study?	15
4.1 VLOP's	15
4.2 User flows	15
5. FINDINGS	17
What was the outcome of our analysis?	17
5.1 Facebook	17
5.1.1 Tracking	17
5.1.2 Onboarding	19
5.1.3 Settings and receiving of notifications	20
5.1.4 Browsing content	22
5.1.5 Deleting account	27
5.2 Snapchat	32
5.2.1 Onboarding	32
5.2.2 Settings and receiving of notifications	36
5.2.3 Browsing content	37
5.2.4 Interactions	40
5.2.5 Subscribing and cancelling subscription	42
5.3 TikTok	46
5.3.1 Onboarding	46
5.3.2 Settings and receiving of notifications	47
5.3.3 Browsing content	48
5.3.4 Deleting account	50
5.4 Shein	52
5.4.1 Onboarding	52
5.4.2 Browsing content	53
5.4.3 Conducting transactions	54
5.5 Zalando	57
5.5.1 Tracking	57
5.5.2 Onboarding	58
5.5.3 Browsing content	60
5.6 Booking	61
5.6.1 Browsing content	61

6. FOLLOW-UP	62
What will we do with our insights?	62
7. ANNEXES	63
i. Sources	63
ii. VLOPs	65
iii. DSA Article 25	66
iv. UCPD	67
a. Article 5	67
b. Article 6	67
c. Article 7	69
d. Annex 1	71

1. MANAGEMENT SUMMARY

What are the main insights from the study?

This study investigated social media platforms Facebook, Snapchat and TikTok, and e-commerce platforms Shein, Zalando and Booking.com for their use of manipulative design. We distinguished between *deceptive patterns* (deception) and *attention capturing damaging patterns* (distracting users and holding their attention).

Compared to e-commerce platforms, social media more often use *attention capturing damaging patterns* like *infinite scroll*, *casino pull-to-refresh*, and *fake friend notifications*. Understandably, if we look at the purpose of the platforms in question. Social media gain from keeping users engaged on their platforms for as long as possible, so they can show more ads and make more money. E-commerce platforms, on the other hand, profit from users as soon as they complete a transaction.

Still, e-commerce platforms, too, use more and more *attention capturing damaging patterns*. The apps of those platforms generate specific messages to grab the attention of users and make them return to their platforms. Examples are notifications or emails saying “your special offer is ending soon”, “did you forget something?” or “you left something in your cart”. In their app, Zalando also uses *infinite scroll*; users can scroll through outfits of influencers and click on their stories.

The chief forms of manipulative design established by the study are the following:

- Almost all types of notifications on social media platforms are enabled by default. Users must really make an effort to select the notifications they wish or do not wish to receive as it is not really clear how to do this. Moreover, the number of options is overwhelming.
- On Snapchat and Facebook users are constantly lured by red badges (whether or not containing numbers). Usually, those badges suggest new interactions with the user, but these days they are often used to alert users to new content (like videos or comments).
- The *cookie banners* on various platforms are often intended to make users accept all cookies, either by making that option stand out, or by accompanying text arguing why users should select that option. Privacy considerations are secondary.

- *Pre-selection* is used to direct users to a specific option or action. When users create a Snapchat account, for instance, they get pre-selected friend suggestions. There is a risk that without wanting or knowing users get in touch and share content with users they don't know. And when they add information to their Facebook accounts, the default setting is "public" (in small gray print).
- The order in which social media platforms show content (including comments) is decided automatically by profiling recommendation systems. User data and interactions predict the content in which users are interested. Legally, there should be a non-profiling alternative that is directly accessible from the same place where the ranked content goes. Snapchat and TikTok offer the option to disable the personalization of content, but this setting is not easy to find. Facebook allows redirection to other, non-profiling feeds, but these are located elsewhere and cannot be selected as default settings. As to comments sections, Facebook offers the option to sort by "newest first" instead of "most relevant", but that selection cannot be defaulted. Every time new content appears (posts, photos, videos, etcetera), the ranking has been reset to "most relevant".
- Snapchat users get many *fake friend notifications*. Users appear to get messages from friends or people they follow, but it is the platform that generates those notifications. This usually is new content that is available or recommended content.
- Snapchat frequently uses game elements and patterns that cause social pressure (*snap streaks* with friends, designated friendship levels, sharing locations with friends).
- Facebook makes it extremely complicated for users to delete their accounts (*roach motel*)
- Compared to the other e-commerce platforms investigated, Shein clearly uses more *deceptive patterns* like *bait & switch*, *limited time*, *fake scarcity*, *pressured selling* and *forced action*.

2. Background

Why this study?

Various European laws¹ aim at regulating online platforms and counteracting harmful or illegal practices. One such harmful practice is manipulative design that incites users to make choices that are not to their advantage. The Digital Services Act (“*DSA*”) and the Unfair Commercial Practices Directive (“*UCPD*”) explicitly mention and prohibit manipulative design. Future laws (the Digital Fairness Act or “*DFA*”) will provide for measures against addictive design, which can be seen as a form of manipulation.

Regrettably, manipulative design is still applied to the interfaces of online platforms. The guidelines on what manipulative design is, are widely interpretable, which complicates enforcement.

We want to make sure that the enforcement on manipulation by platforms becomes easier, by investigating and identifying types of manipulative design, and by making these more concrete. We also demonstrate the effect of manipulative design on users. To this end we have conducted a first exploratory study.

Objective of exploratory study

Our exploratory study mapped out the types of manipulative design and how these are used on a selection of major online platforms. To this end we analyzed different user flows on the platforms, recording our findings in this report. We determined which of the patterns found we consider most harmful and most urgently require action.

The result will serve as input for follow-up studies that will further investigate a selection of the manipulative practices established, together with users to show the effect on their experiences and behavior. That way we can reinforce enforcement actions and our lobby.

Impact

The study report contributes to public education, awareness and the willingness to take action against the manipulation by online platforms.

¹Examples are the Consumer Rights Act (CRA), Unfair Terms In Consumer Contracts Directive (UTCCD), General Data Regulation Protection (GDPR), Unfair Commercial Practices Directive (UCPD), Digital Markets Act (DMA) and Digital Services Act (DSA). Additional legislation on online platforms is in the pipeline: the Digital Fairness Act (DFA).

3. Definitions

What are the scientific and legal frameworks?

3.1 Manipulative design

Legislation² refers to manipulative design as follows:

DMA (Article 13)

“The gatekeeper shall not degrade the conditions or quality of any of the core platform services provided to business users or end users who avail themselves of the rights or choices laid down in Articles 5, 6 and 7, or make the exercise of those rights or choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users’ or business users’ autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof.”

DSA (Article 25)

“Providers of online platforms shall not design, organize or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.”

UCPD (Articles 6 and 7)

“A commercial practice shall be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise [...]”

“A commercial practice shall be regarded as misleading if, in its factual context, taking account of all its features and circumstances and the limitations of the communication medium, it omits material information that the average consumer needs, according to the context, to take an informed transactional decision and thereby causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise [...]”

The definition of ‘manipulative’ that we use, is based on **scientific**

²For the relevant articles, see annexes ii, iii and iv

literature³,

which in substance describe manipulative design as presenting information and choices on a digital interface in a particular way, steering users towards a specific selection, or depriving users of a free or fully informed decision. This means users make choices that they did not intend to make, that they would not have made, had they not been directed towards that choice, and that are not in their interest. It is usually the providers and/or third parties that benefit, for instance because users take more transactional decisions or share more personal data than intended.

3.2 Deceptive patterns

By *deceptive patterns* – also called *dark patterns* – we mean specific types of manipulative design that in their own way mislead users or let them make unintended choices. Primarily on e-commerce platforms, these patterns have been the subject of a great deal of research, which has identified many specific types of *deceptive patterns*. Social media, too, have started to use these patterns.

Researching and identifying concrete patterns of manipulative designs makes it easier to assess whether designs are actually manipulative, as the descriptions used in legislation are still widely interpretable. The research often comes up with a taxonomy classifying the patterns into categories and subcategories.⁴ Research can help to make the law more concrete.

The categorization also helps policy makers to better understand and compare the underlying effects of the *deceptive patterns*. An example: the classification of certain *deceptive patterns* into the categories *misleading information* and *misleading presentation* makes it clearer

³Based on, inter alia, op [Brignull, \(2015\)](#); [Gray et al., \(2018\)](#); [Lupiáñez-Villanueva et al. \(2022\)](#); [Leiser & Yang, \(2023\)](#)

⁴[Leiser & Yang \(2023\)](#) linked *deceptive patterns* to articles in the UCPD, defining as main categories *Information asymmetry* and *Free choice repression*, which include the subcategories *Active misleading actions*, *Passive misleading omissions*, *Undesirable imposition* and *Undesirable restriction*. These subcategories in turn can be divided into *Misleading information*, *misleading presentation*, *hiding information*, *delaying provision*, *pressure imposition*, *forced acceptance*, *restricting specific users* and *restricting specific actions*. [Gray et al.\(2018\)](#) mentioned as main categories *nagging*, *sneaking*, *obstruction*, *interface interference*, and *forced action*

that there is a link with Article 6⁵ UCPD, which refers to a prohibition of misleading practices.

This study focused on 21 *deceptive patterns* as found in scientific literature⁶. They were selected at the lowest, most specific level, meaning that the (sub) categories to which they might belong were not considered. Below we will explain these patterns:

Roach Motel (1/21)

It is easy for users to register for specific services, but *hidden information* (8/21) and *misdirection by visual interference* (5/21) make it difficult to deregister.

Sneak into basket (2/21)

This is the adding of items to users' baskets, for instance by *pre-selection* (6/21). Users must actively deselect the items from their baskets. Sometimes it is not items that are added, but additional costs (like service fees) that are not visible until checkout. These are called "hidden costs".

Repeated choice popup (3/21)

The same popup displays repeatedly, asking users to make a choice – even if that choice has been made already, or the popup was closed earlier.

Price comparison prevention (4/21)

Several packages / subscription plans are offered, but it is impossible to compare prices because the prices are hidden or because not every package lists its functionalities.

Misdirection by visual interference (5/21)

Visual tricks or illusions direct users to specific clicks. An example: a button appears inactive as it is gray, but is still clickable. Or: certain information or buttons stand out because of color use.

Pre-selection (6/21)

⁵See annex iv.b

⁶Based on, inter alia, [Brignull, \(2015\)](#); [Gray et al., \(2018\)](#); [Lupiáñez-Villanueva et al. \(2022\)](#); [Leiser & Yang, \(2023\)](#)

Users must make choices to continue a process, but one or more of those options have been pre-selected. Users must be aware and deselect any unwanted options.

False hierarchy (7/21)

Options or content are displayed or ordered such that some are highlighted while other ones are overlooked.

Hidden information (8/21)

Users are hindered in finding information, because it is hidden or because the language is obscure.

One such form is *legal obfuscation*: texts are deliberately long, formal, complex or turned into legalese, which makes it hard for users to understand what they are consenting to and what the consequences are.

Trick question (9/21)

Double negatives are used, like “I don’t want notifications” – no/yes.

Sentence constructions can be ambiguous, like “are you certain you wish to cancel” – cancel / ok

It is not immediately clear whether or not to tick certain boxes. For instance: “I do not wish to receive emails about...”

Confirm shaming (10/21)

The wording of the choices offered is not neutral, but contain (judgmental) terms that capitalize on emotions. Some examples:

“No, I don’t want any offers”

“No, I’d rather waste my discount”

“Yes, I want a fully functional website”

“Yes, I want the best experience”

“Are you sure you want to go? We will miss you.”

Bait and switch (11/21)

This practice refers to components that do not work as expected. Like an X that does not close the window, but makes a new popup appear. Or a button that triggers an unwanted download to the user’s computer.

Disguised advertisement (12/21)

Ads are displayed in the same way as the content offered on the platform, without any warning that this is an advertisement.

Pressured selling (13/21)

Whenever users add something to their baskets, a popup urges them to buy more items, for instance by saying that it is cheaper to buy a bundle, or by offering a gift if their purchase reaches a certain threshold.

Forced continuity (14/21)

A trial subscription is offered, which is quietly rolled over into a paid subscription plan.

Fake scarcity (15/21)

False claims are made, alleging that products are scarce or almost sold out, urging users to decide quickly. Examples:

“Low stocks”

“Only 2 left”

“Usually not available”

Limited time (16/21)

Specific time periods are communicated within which offers or functions are available, sometimes by showing countdown timers that manipulate users into deciding quickly.

Social proof (17/21)

Reviews appear to be written by real users but are fake.

Fake discount (18/21)

Products are offered at a discount, but were in fact never sold “at the original price”.

Privacy zuckering (19/21)

Users are tricked into sharing more personal data, for instance by means of *forced action* (21/21), *hidden information* (8/21), *pre-selection* (6/21) and *confirm shaming* (10/21)

Friend spam (20/21)

Users have consented to sharing their contacts with the platform, but the platform uses those data to send messages to those contacts without asking for explicit consent.

Forced action (21/21)

Users are offered options or functions but in fact have to perform certain actions first to use such functions. Examples: users first have to view an ad to get points, download an app to track an order, create an account to get a discount, or share personal data.

3.3 Attention capturing damaging patterns

With the advent of social media have come other (more subtle) forms of manipulation, related to the **distraction, temptation of users and keeping their attention**. That way they spend as much time as possible on the platform. After all, that is how social media make money: the more time on the platform, the more (personalized) ads can be offered, and the more the platform earns. Other platforms (besides social media), too, have started using techniques focusing on attention. Although the impact on mental health requires more long-term research, there are many indications that attention-grabbing technology has harmful effects, including excessive smartphone usage, short attention spans and feelings of anxiety (like *Fear Of Missing Out*)⁷.

Monge Rofarello et al. (2023) call these *attention capturing damaging patterns*:

“Recurring patterns in digital interfaces that exploit psychological vulnerabilities and capture attention, often leading the user to lose track of their goals, lose their sense of time and control, and later feel regret.”⁸

While with *deceptive patterns* it is easier to demonstrate that users are deceived into making choices they did not intend to make, that is more difficult with *attention capturing damaging patterns*. Those patterns **seduce** rather than **deceive** users. They could be in line with the user's objective to find more content or stay up to date. It is debatable,

⁷[Essen & Van Ouytsel, \(2023\)](#); [Monge Rofarello et al. \(2023\)](#); [Soysal, \(2025\)](#)

⁸[Monge Rofarello et al., \(2023\)](#)

therefore, whether we can consider such patterns *deceptive patterns*. Patterns that deceive are easier to ban under the DSA and UPCD than patterns that (in a harmful way) capture attention.

*' Users rarely if ever desire to be deceived, but they do sometimes wish to be seduced.'*⁹

Fortunately, there is legislation in the pipeline that addresses seductive design: the Digital Fairness Act (DFA). *Attention capturing damaging patterns* play a major part as they increase the time spent on platforms and are linked to excessive smartphone usage. This presents an opportunity to include those patterns in this act.

Our analysis considers both types of patterns (*deceptive patterns* and *attention capturing damaging patterns*) as we are convinced that both patterns are manipulative and harmful.

This study covers nine *attention capturing damaging patterns* as found in scientific literature.¹⁰ These, too, are described at the lowest level, i.e. without (sub)categories. Below we will explain these patterns:

Infinite scroll (1/9)

Users can scroll down endlessly, with new content loading automatically. Users do not know what content will appear. This feeds into *Fear Of Missing Out (FOMO)* and *partial reinforcement*, with users occasionally being rewarded (with interesting content) or not; it's basically like a fruit machine that prompts more scrolling.

Casino pull-to-refresh (2/9)

(Mobile only) Users can swipe the top of the page down to refresh the page and load new content. Users do not know what new content will appear. This feeds into *Fear Of Missing Out (FOMO)* and *partial reinforcement*, with users occasionally being rewarded (with interesting content) or not; it's basically like a fruit machine that prompts more scrolling.

Neverending auto-play (3/9)

New videos are automatically played as soon as the current one ends. There is no option to disable *autoplay*, or that option is hidden.

⁹[Monge Rofarello et al., \(2023\)](#)

¹⁰[Monge Rofarello et al., \(2023\)](#)

Guilty pleasure recommendations (4/9)

Personalized recommendations based on what users like or sustains their attention. The recommendations are usually made by profiling algorithms of user interactions.

Recapture notifications (5/9)

Notifications generated by the platform to make users return to the platform. These can be notifications about recommendations, new content or content with which users have not interacted before. When users open the platform, this type of notifications is also used to capture the users' attention and keep them on the platform. These often take the form of red *badges* (whether or not with a number). They draw attention because they stand out visually (*salience bias*) and create a sense of urgency, a task that has not been completed.¹¹ Users likely click because they are curious about the underlying notification, because of *fear of missing out* (FOMO) or because they want to complete tasks.

Playing by appointment (6/9)

Users are incited to use the platform at specific times because otherwise they will lose points, status or other rewards.

Grinding (7/9)

Users must perform the same action repeatedly to collect points or earn other "rewards".

Time fog (8/9)

The users' notion of time is suppressed, for instance because clocks or the play time of videos are not visible. That way not only the users' attention to the platform is retained, but they are furthermore deceived because information is withheld (*deceptive pattern*, form of *hidden information*).

Fake friend notifications (9/9)

Notifications appear to be sent by other users, but in fact are generated by the platform. This makes this pattern not only attention-capturing but deceptive as well (*deceptive pattern*).

¹¹Bartoli & Benedetto (2022)

4. Study approach

How did we conduct the study?

4.1 VLOPs

In this study we focused on Very Large Online Platforms (VLOPs)¹² because they have the largest user numbers and for that reason are the most influential. They were also the first that had to comply with the DSA.

We investigated e-commerce platforms because this is where *deceptive patterns* originated, but also social media platforms because of their increasing impact on and interference in society. In that latter category we expected to find more *attention capture damaging patterns*.

We selected the following platforms:

Social media

- Facebook
- Snapchat
- TikTok

E-commerce

- Shein
- Zalando
- Booking

4.2 User flows

We went through several *user flows* on the selected platforms, using both real personal accounts and research accounts (accounts of fake persons). Where possible, we viewed the flows on desktops and mobiles, generally concentrating on:

- Onboarding, creating an account
- Accepting or refusing tracking;
- Settings and receiving of notifications;
- Browsing content and/or items;
- Interactions with other users;
- Conducting transactions;
- Deleting an account;
- Choosing and cancelling a subscription plan.

¹²See annex ii. VLOPs

We recorded any specific patterns that we identified as a *deceptive pattern* or an *attention capturing damaging pattern*, describing the pattern and making screenshots. We used definitions formulated in the scientific literature and legal guidelines.¹³

¹³See Chapter 3: Definitions within manipulative design

5. Findings

What was the outcome of our analysis?

5.1 Facebook

Manipulative design was found during:

- Tracking
- Onboarding
- Settings and receiving of notifications
- Browsing content
- Deleting accounts

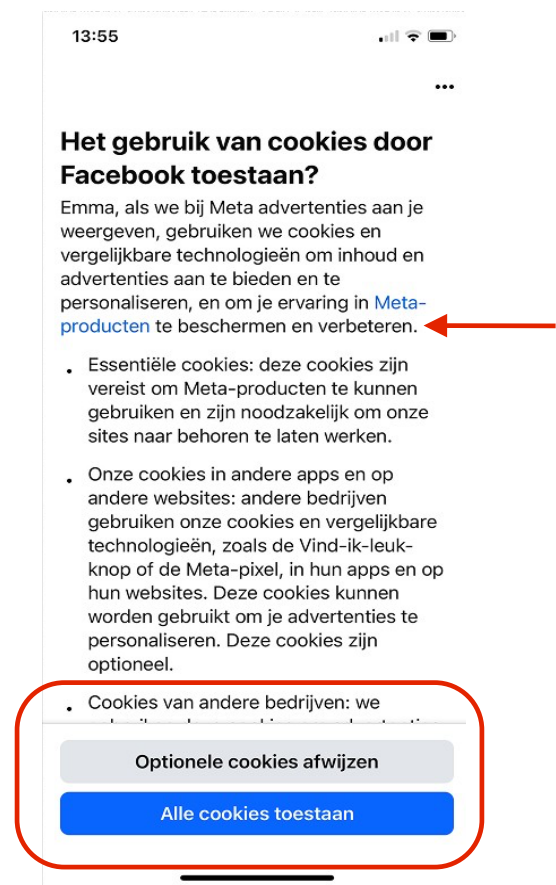
5.1.1 Tracking

Misdirection by visual interference (deceptive pattern)

Its blue color (Facebook's primary color) directs users visually to the button "allow all cookies", while the button "reject optional cookies" is gray. The buttons should be identical in appearance and design, so as not to affect the users' choice.

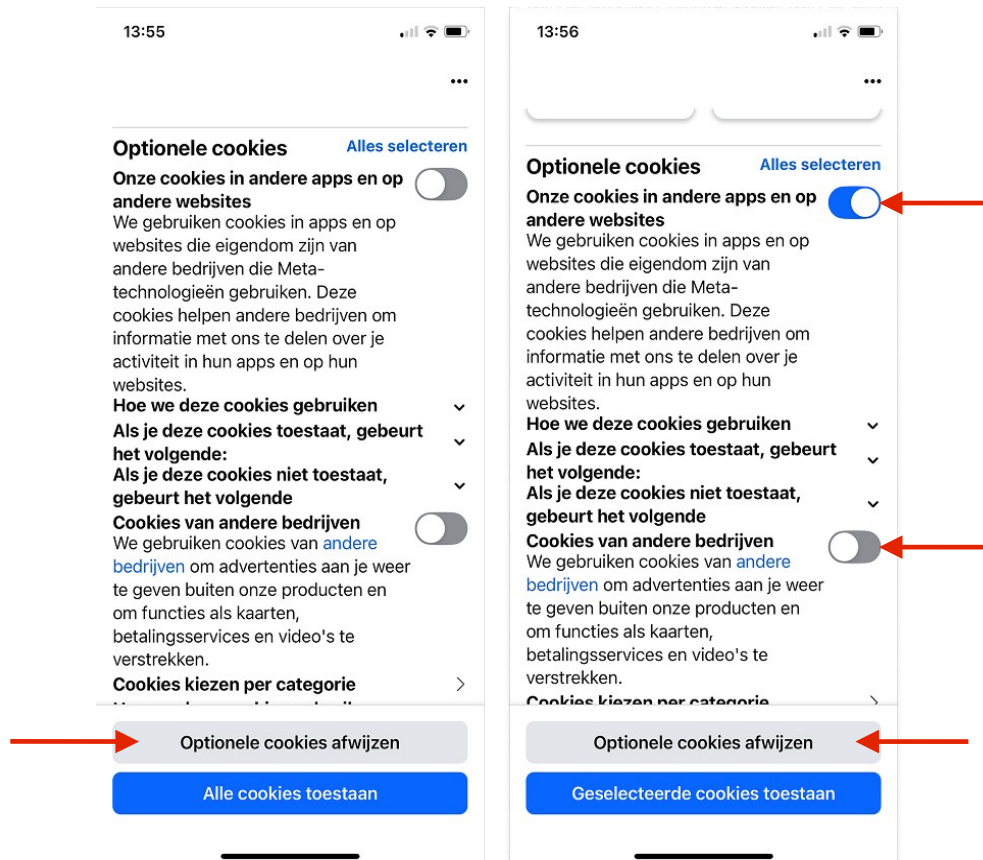
Confirm shaming (deceptive pattern)

The use of the word "protect" in the sentence "we use cookies to protect and enhance your experience in meta products" suggests that allowing cookies is the safe choice.



Trick question (deceptive pattern)

If users choose “reject optional cookies”, they can still choose from two types of optional cookies. It is not immediately clear whether these should be selected to reject or allow those cookies.



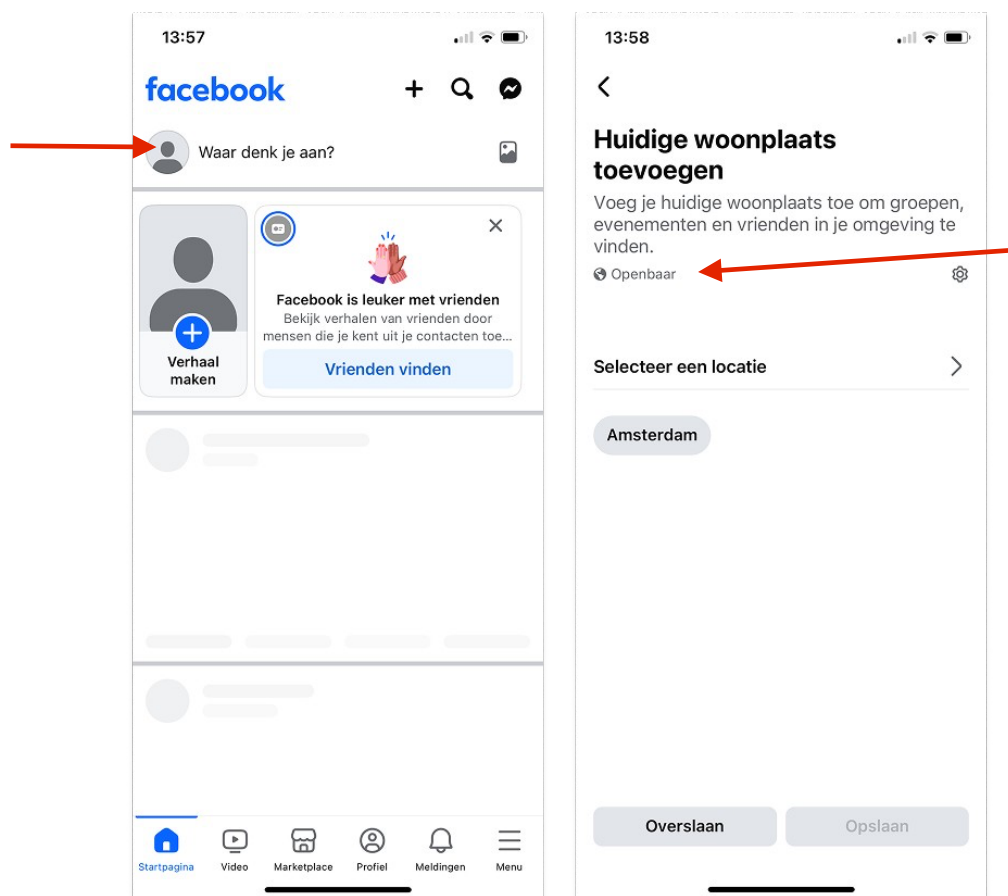
5.1.2 Onboarding

Repeated choice pop-up (deceptive pattern)

As soon as users open the profile page who have not yet entered any personal data, a flow opens where users can fill out their data. Users are asked where they live, where they were born, their school, employer, relationship status, and so on. Although users can skip these questions, the flow will start every time they open their profile. This is also *privacy zuckering*, because it involves personal data.

Pre-selection (deceptive pattern)

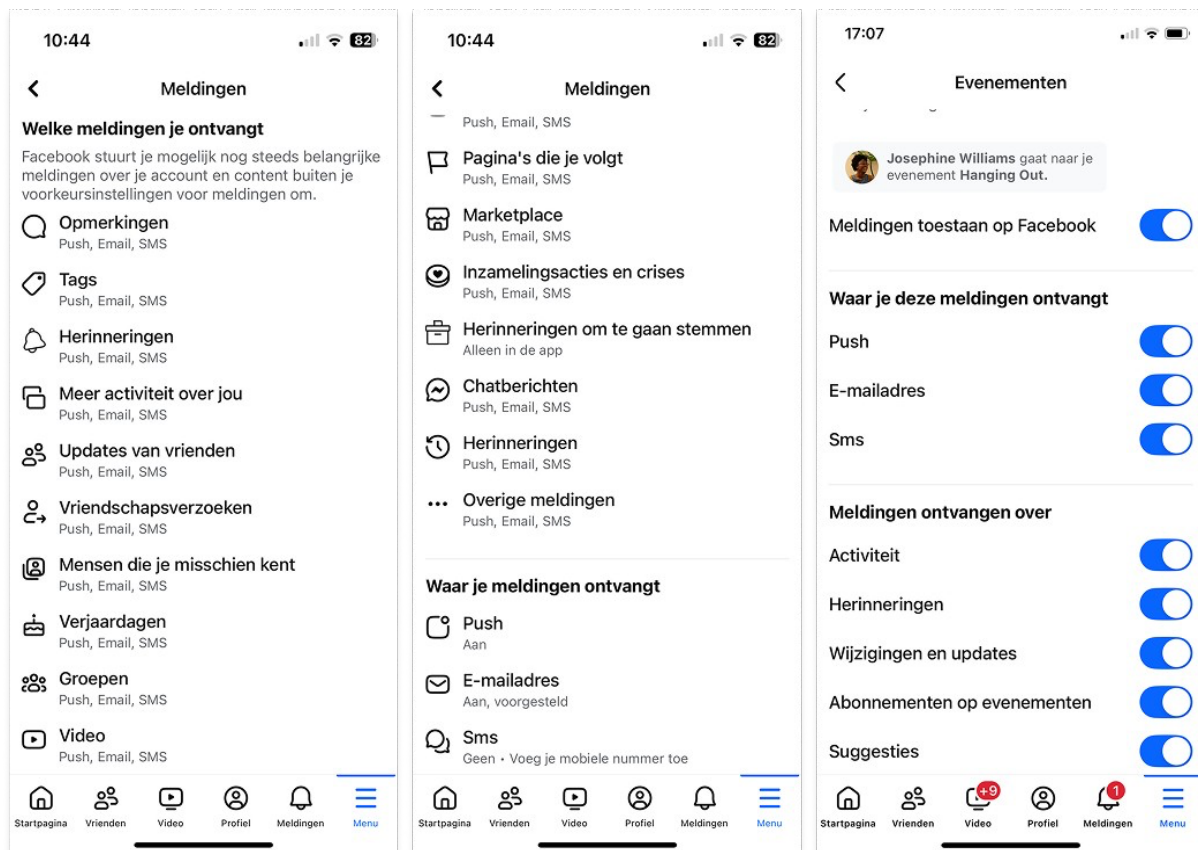
The default setting of profiles (like your place of residence, place of birth, employer or school) is “public”. This means these data are shared with everyone, unless users actively change this setting.



5.1.3 Settings and receiving of notifications

Roach motel (deceptive pattern)

Although the term *roach motel* actually refers to the cancellation of services or subscriptions, it can be used also for the “cancellation” of notifications: by default all notifications are enabled in all kind of ways (push, email and texts). It takes a lot of effort to disable notifications because there are many options for every category. The sheer volume and obscure descriptions call for a great deal of cognitive capacity to determine what specific notifications entail and whether or not you want to receive those notifications.



Types of notifications

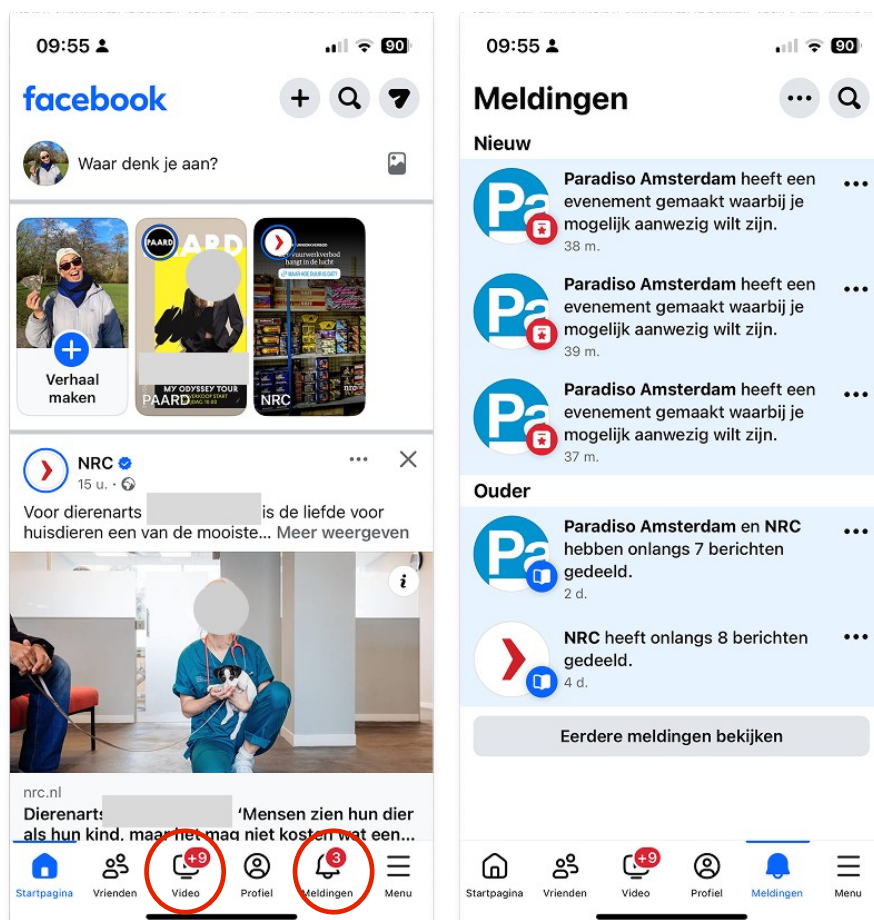
Means of notifications

Options within notification category 'events'

Recapture notifications (attention capturing damaging pattern)

Notifications that are enabled by default include the following: people you may know, event suggestions, market places that might interest you, memories, and other notifications such as breaking news, nearby restaurants, offers that are about to expire. These are all examples of notifications generated by the platform (and are not triggered by interactions with/of users). This is Facebook's way to make users return to the platform.

Once on the platform, users get to see the red *badge* (small red dot, with or without a number) to keep their attention. The badge is usually displayed when there are new interactions with the user or if users are required to take action. Facebook, however, also uses the badge to announce new content, for instance in the menu item "video" for users who have not viewed videos for some time. And there will always be new videos.



Notifications about new events that might interest the user

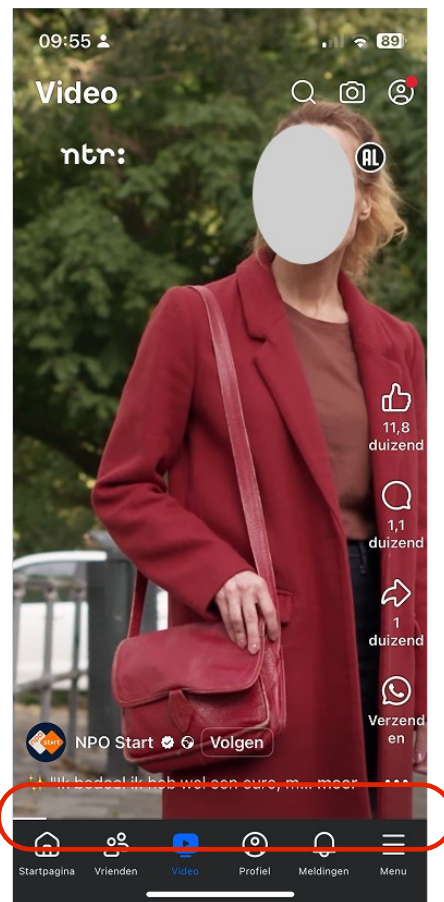
5.1.4 Browsing content

Infinite scroll (attention capturing damaging pattern) & casino pull-to-refresh (attention capturing damaging pattern)

Users can scroll infinitely on the start page. Content is refreshed by swiping down from the top of the page. New content appears continuously as this also includes suggestions. The same applies to the pages under the menu item “videos”.

Time fog (attention capturing damaging pattern)

Videos do not display any time notation (minutes and seconds) to show how long users have been watching and how long the video is. Occasionally they show a progress bar that fills up as the video plays.

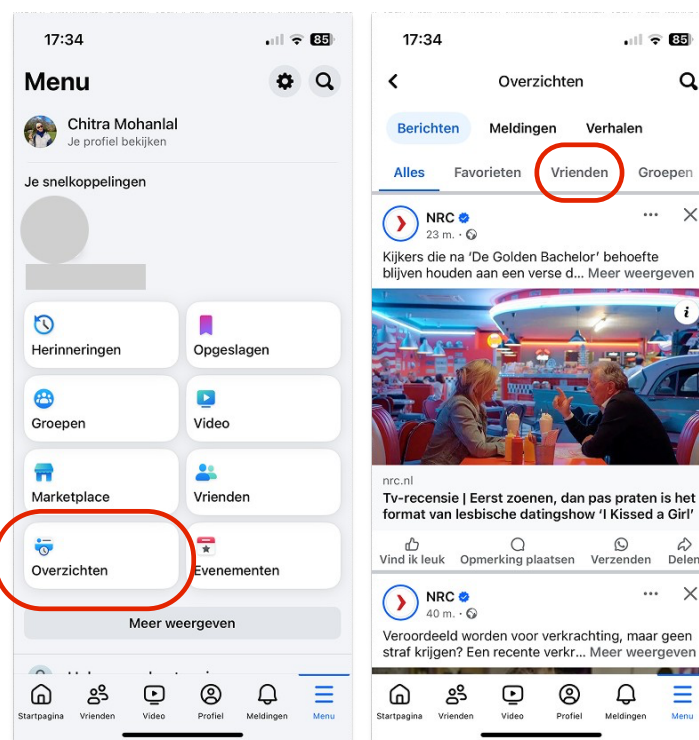


Guilty pleasure recommendations (attention capturing damaging pattern)

The start page is a feed that uses a profiling recommendation system. Based on the interactions between users and content, like posting comments or likes, or watching videos, the system shows content that users might be interested in.¹⁴

Platforms are required to offer a non-profiling alternative option (Article 38, DSA) that is directly and easily accessible from the specific section of the platform's online interface where the information is being prioritized (Article 27, DSA).

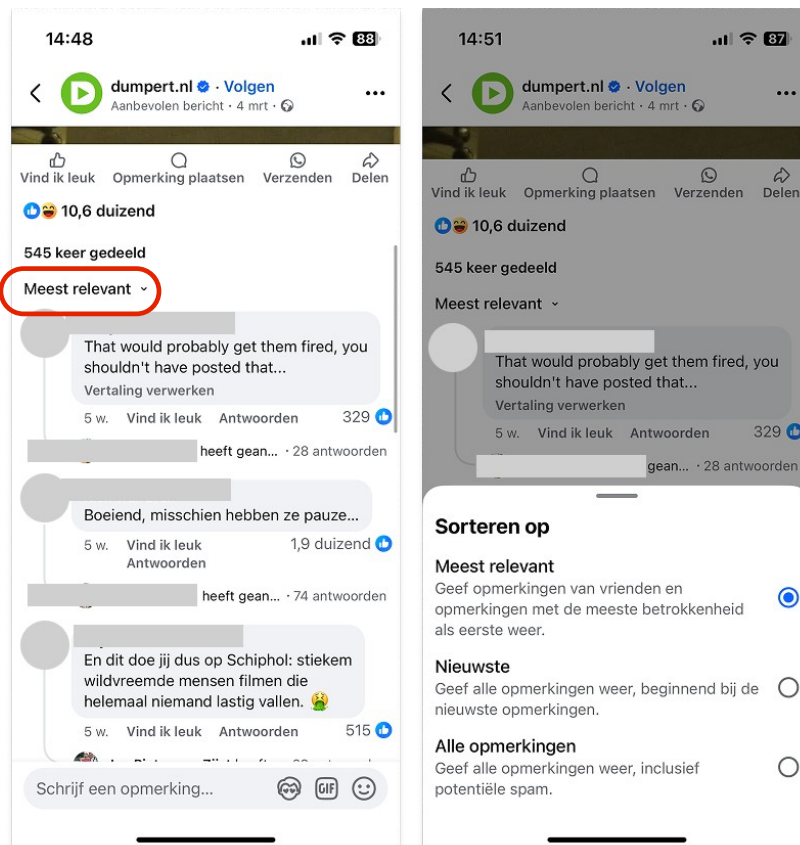
On Facebook the alternative *feeds* can be found in settings under “Feeds”. This means they are not directly accessible from the default feed (*hidden information*), nor can alternatives be set as default, which could constitute a breach of the DSA.¹⁵



¹⁴Visit: <https://transparency.meta.com/features/explaining-ranking/fb-feed-recommendations/>

¹⁵In April 2025 Bits of Freedom, together with EDRI, Gesellschaft für Freiheitsrechte and Convocation Design + Research filed a complaint with the Irish regulator.

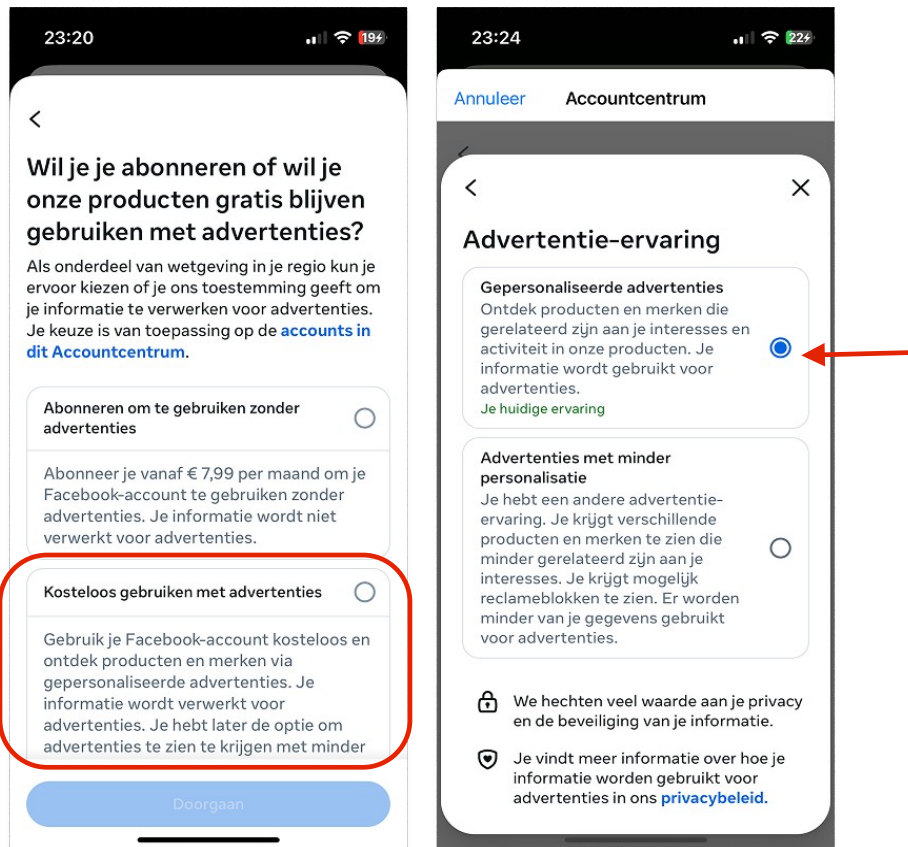
The same applies to comments sections, which are automatically sorted by “most relevant”. This ranking comes about by the AI system predicting in which comments users are likely to be most interested.¹⁶ Users have the option to rank by “newest” (chronological and non-profiling). With every new post, however, the ranking will be defaulted to “most relevant” again. Users would have to choose “Newest” every time if they wish to avoid personalization (*repeated choice*).



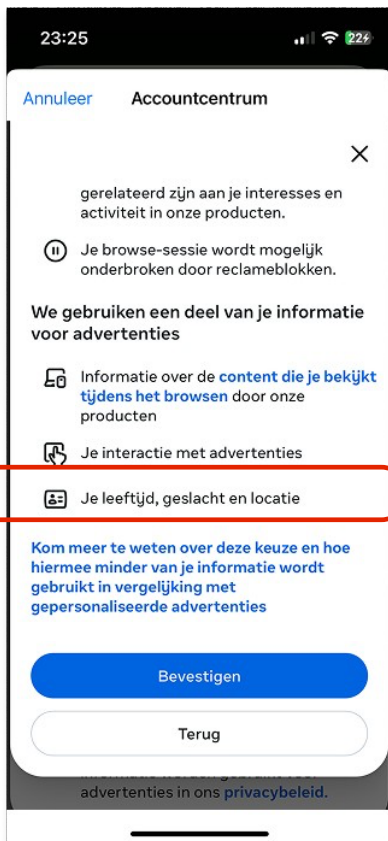
¹⁶Bezoek: <https://transparency.meta.com/features/explaining-ranking/fb-feed-ranked-comments/>

Privacy zuckering (deceptive pattern)

Users who wish to manage their ad preferences get to choose between a paid subscription or using Facebook free of charge with ads. If they choose ads, they can choose either “personalized” or “less personalized” ads. “Personalized” is preselected (*pre-selection*).



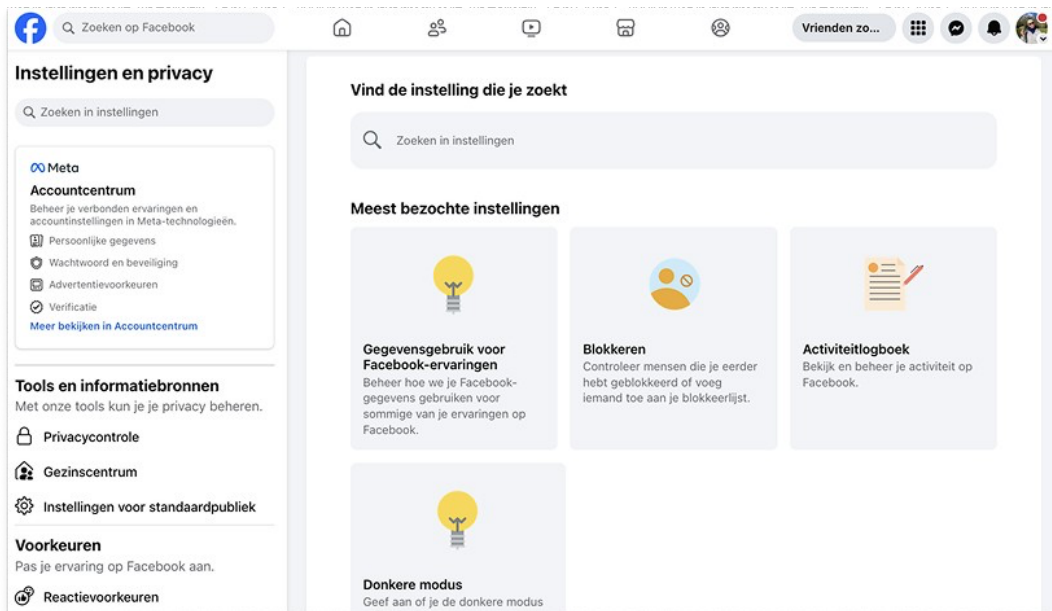
Users who choose “less personalized” still get to see ads based on their gender and location. In addition, they get to see “commercial breaks” while scrolling through the feed, which users have to view before they can move on (*forced action*). An annoying experience that may move users to select personalized ads after all.



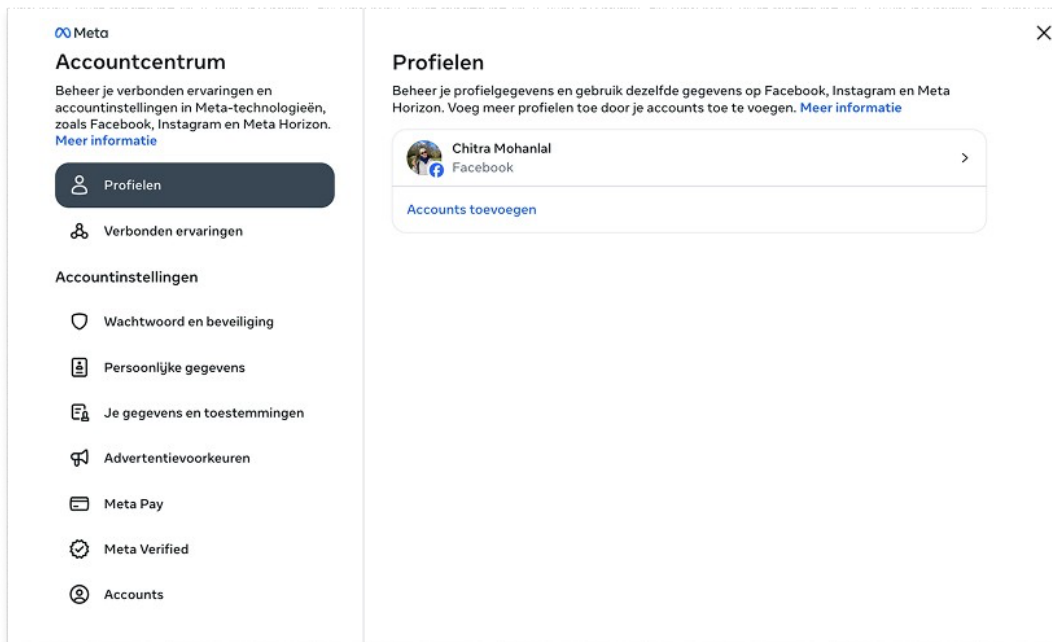
5.1.5 Deleting accounts

Roach motel (deceptive pattern)

It takes many *clicks* to delete an account. Users have to switch between at least two different environments: from the Facebook settings page (environment 1) they are directed to the Meta account center (environment 2).

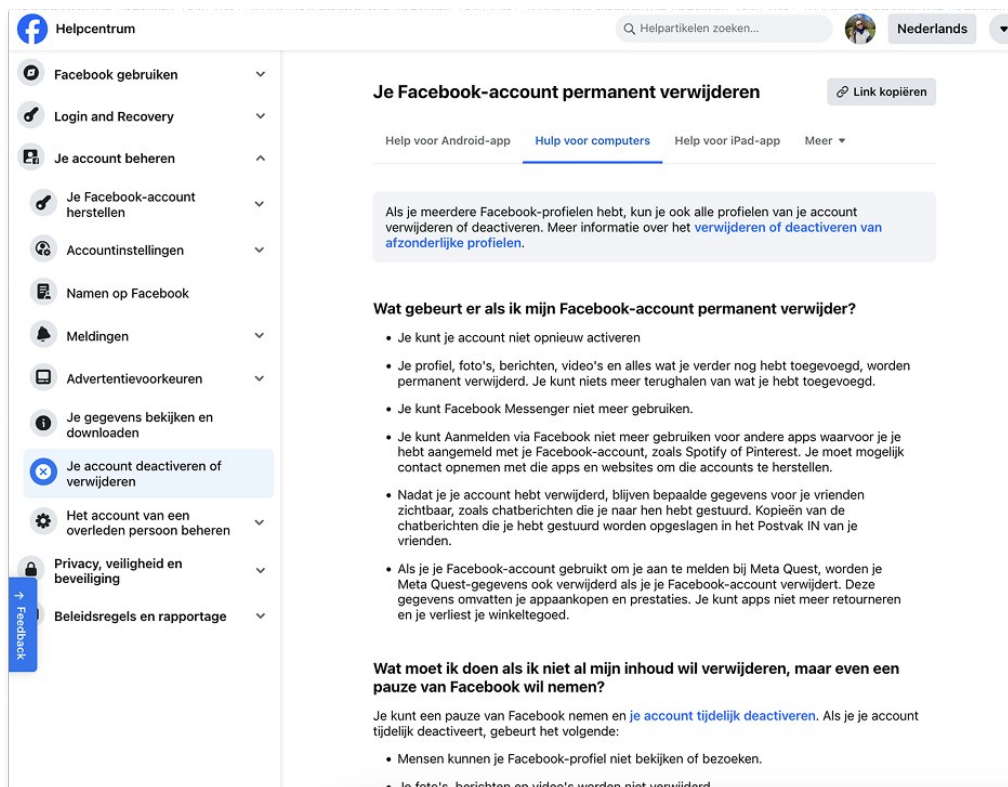


Facebook settings page



Meta account center

If users cannot find the function, they could well end up at the Facebook help center (environment 3) via a search engine.



Facebook help center

The Facebook help center does not allow for immediate action, for instance via a link. Instead users have to go through a step-by-step plan to delete their account. For that they have to go back to the previous two environments.

Je Facebook-account permanent verwijderen:

1. Klik in de rechterbovenhoek van Facebook op je profielfoto.
2. Selecteer **Instellingen en privacy** en klik op **Instellingen**.
3. Als **Accountcentrum** linksboven in je menu **Instellingen** staat, kun je je account verwijderen via het Accountcentrum. Als **Accountcentrum** linksonder in je menu **Instellingen** staat, kun je je account verwijderen via je Facebook-instellingen.

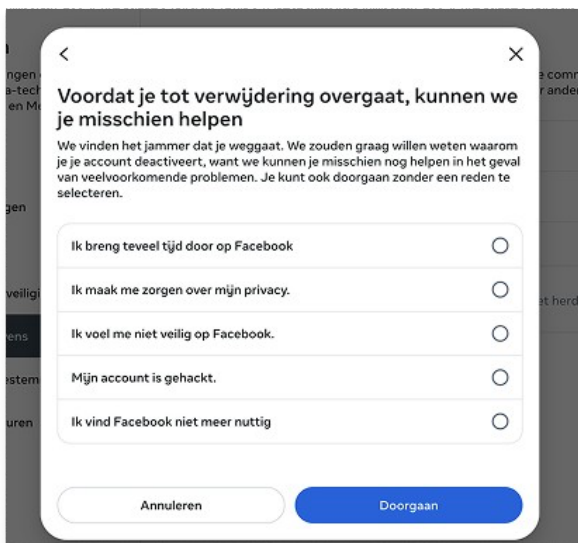
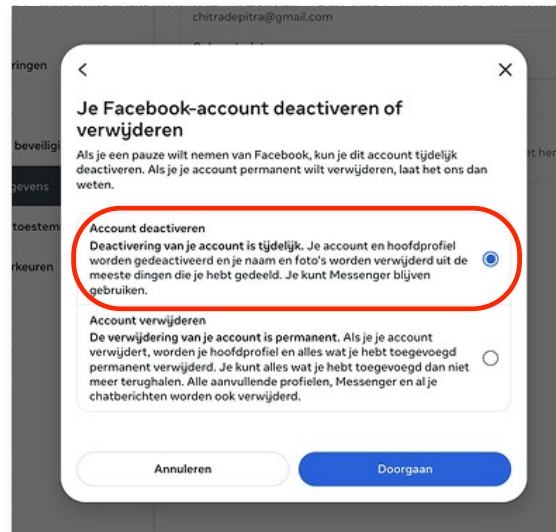
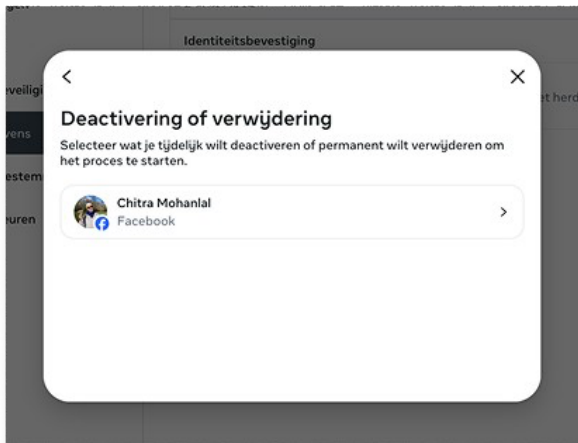
Je Facebook-account verwijderen via het Accountcentrum

Je kunt je account verwijderen door in het **Accountcentrum** rechtstreeks naar de **instellingen Eigendom en beheer van accounts** te gaan. Of je kunt deze instructies volgen:

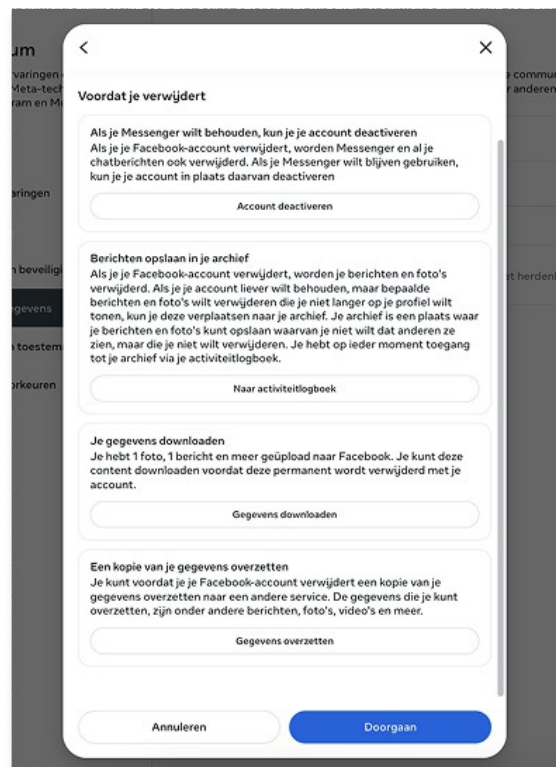
1. Klik in de rechterbovenhoek van Facebook op je profielfoto.
2. Selecteer **Instellingen en privacy** en klik op **Instellingen**.
3. Klik linksboven op je scherm op **Accountcentrum**.
4. Klik onder **Accountinstellingen** op **Persoonlijke gegevens**.
5. Klik op **Eigendom en beheer van account**.
6. Klik op **Deactiveren of verwijderen**.
7. Kies het account of profiel dat je wilt verwijderen.
8. Selecteer **Account verwijderen**.
9. Klik op **Doorgaan** en volg dan de instructies om te bevestigen.

Step-by-step instructions that refer to account center

The account-deleting process comprises many steps: Users are asked to select the account in question, whether they want to deactivate or delete their account, they have to state a reason, take action like backing up messages in the archive or downloading data, and re-entering their password. Under “deactivation or deletion”, “deactivation” is preselected, directing users to that option (*pre-selection*).

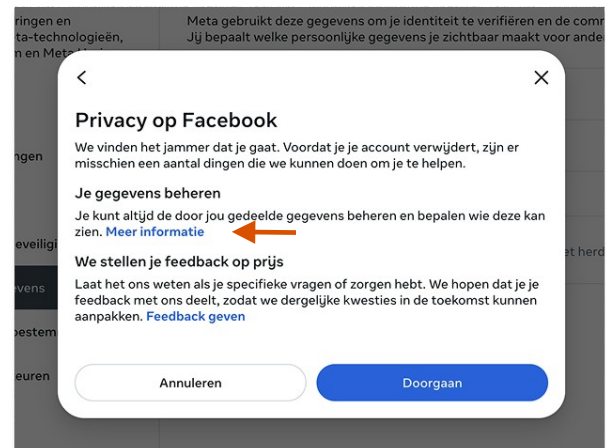
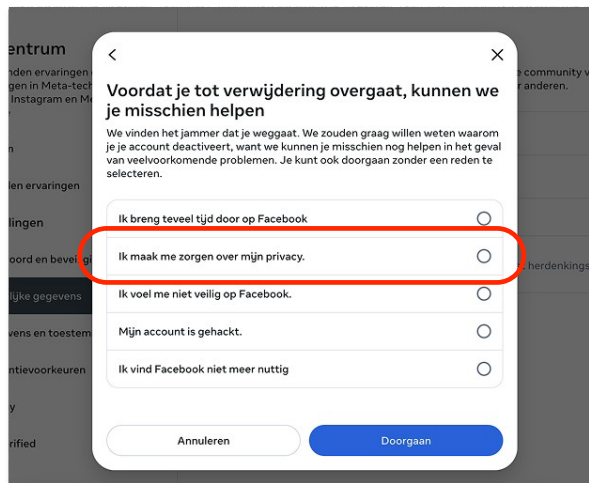


Stating a reason



Actions before deleting

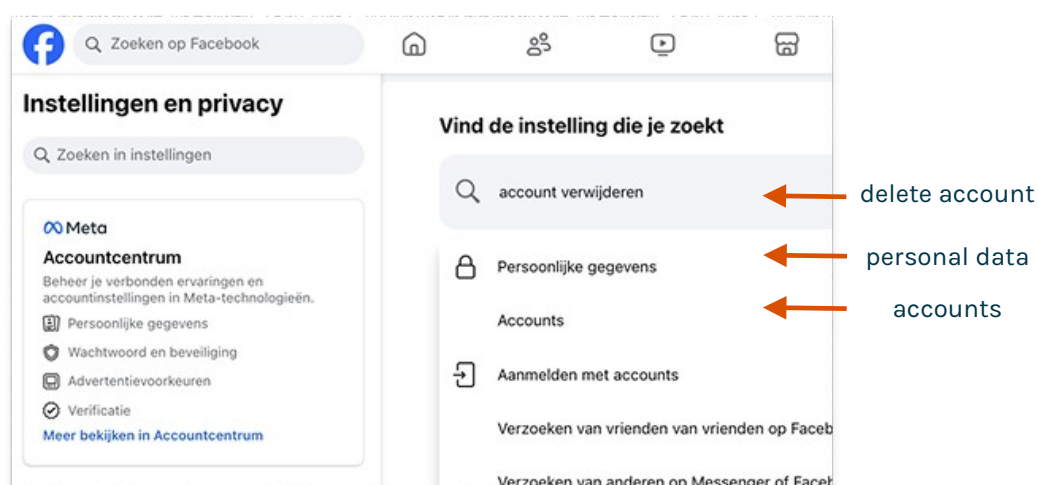
Users do not know how many steps or interruptions will follow. If, for instance, they select “privacy concern”, the next step will contain a link to the help center with relevant articles on privacy.

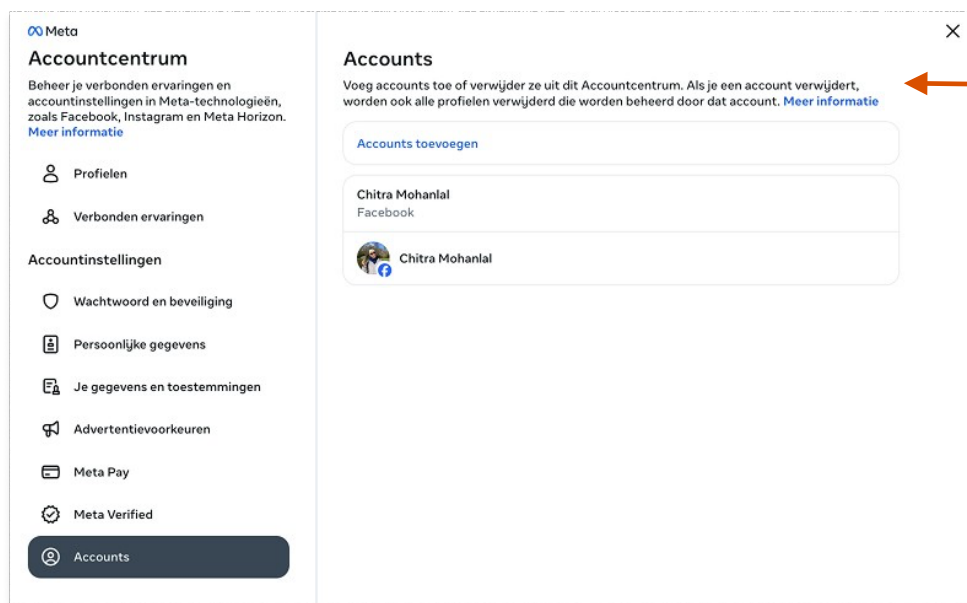


More information about privacy

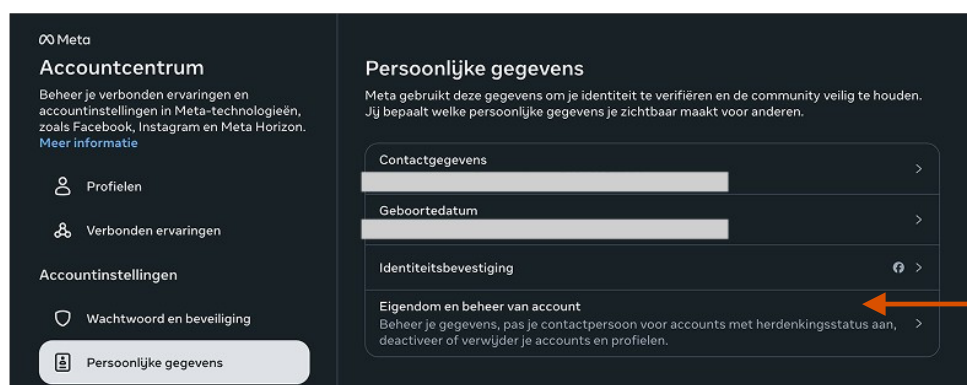
Hidden information (deceptive pattern)

The location of the function to delete an account is hard to find. Entering the search terms “delete account” on the settings page of Facebook does not yield any clear answers but leads to “personal data” and “accounts”. “Accounts” seems to make most sense, as other apps, too, use that category to delete accounts. But in fact the actual function can be found under “personal data”.





Deleting accounts from account center



Actual function of deleting account under personal data

Under 'Accounts' users see the text: "Add accounts or remove accounts from the Account Center". But there is no button to remove the account. It turns out that this text does not refer to the actual removing of the account, but to the removing of linked accounts like Instagram and WhatsApp from the Meta Account Center (Meta is the parent company of Facebook, Instagram and WhatsApp). This can be confusing.

5.2 Snapchat

Manipulative design was found during:

- Onboarding
- Settings and receiving of notifications
- Browsing content
- Interactions
- Subscribing and cancelling subscription

5.2.1 Onboarding

Forced action (deceptive pattern)

In step 1 of creating an account users are asked for their first name and last name (optional). They are also informed that Snapchat is a service sponsored by ads and that user data will be shared with advertisers and partners. At that point users can only choose “accept and continue” and not enter preferences. This, too, is a form of *privacy zuckering*, because these are personal data.

< Account maken
Stap 1 van 5

Voornaam

Ismail

Achternaam

Achternaam (optioneel)

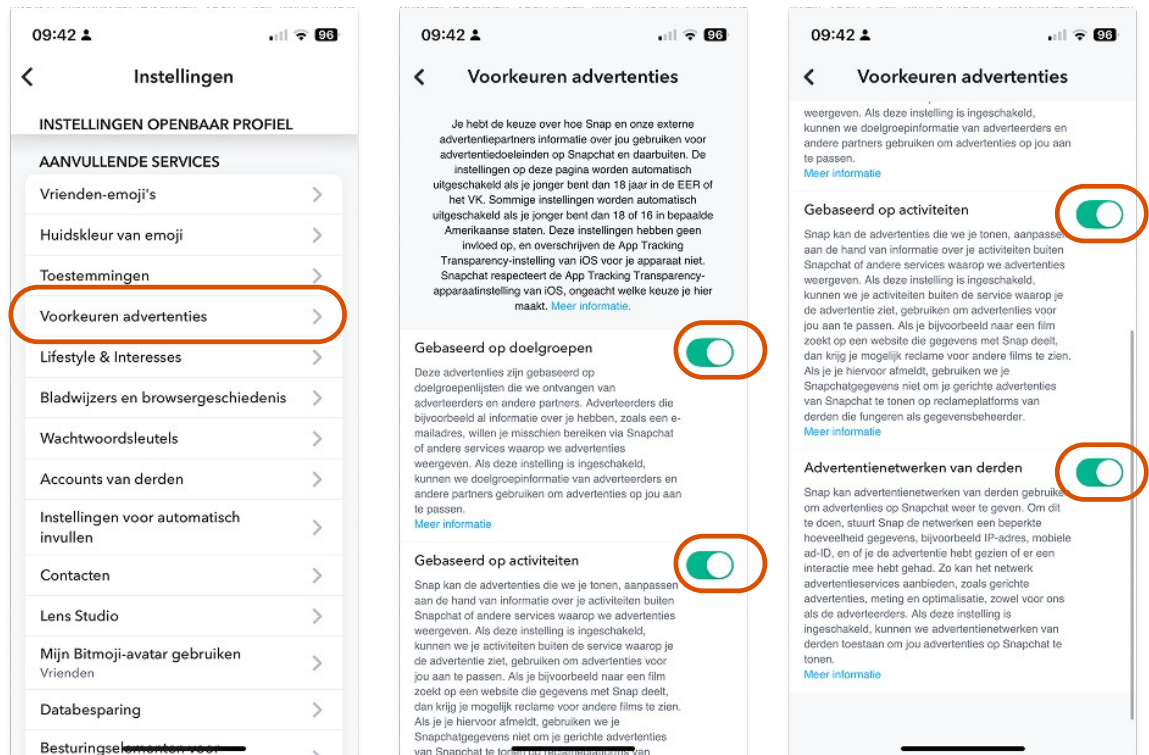
Door op Akkoord en doorgaan te tikken, bevestig je dat je akkoord gaat met ons [Servicevoorwaarden](#) en dat je onze [Privacybeleid](#) hebt gelezen.

Snapchat is een [gepersonaliseerde, door advertenties gesponsorde service](#). Dit houdt in dat we gebruikmaken van gegevens over jou, je vrienden, onze community en informatie die wordt verstrekt door adverteerders en partners, waaronder je activiteiten op hun websites en apps. Zo kunnen we je content en advertenties laten zien op Snapchat die voor jou interessant zijn, en daarnaast de prestaties meten van deze advertenties.

Akkoord en doorgaan

Hidden information (deceptive pattern)

Once they have signed up for an account, users can state preferences for ads under settings. They have to really look for it though. Here users can reject certain ads namely: based on target groups, based on activities and advertising networks of third parties. This option should be offered proactively during onboarding but instead users are forced to provide personal data for all applications.



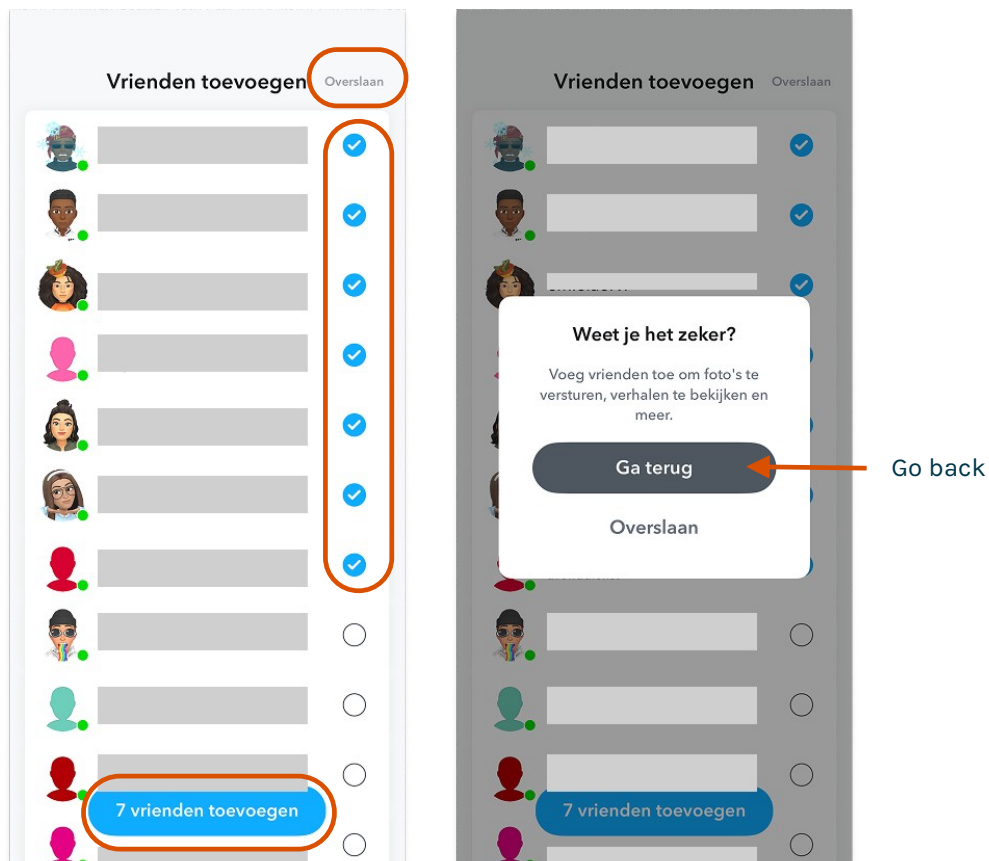
Misdirection by visual interference (deceptive pattern)

On the screen shown here, Snapchat prepares users that they will be asked to share their contacts. The pointing hand emoji directs users to grant full access. That is how Snapchat evades the visual equivalence applied later in the popup.



Pre-selection (deceptive pattern)

Snapchat makes and even preselects friend suggestions based on the user's contacts. If users do not give access to their contacts random users are suggested, some of whom have been preselected. This might tempt users into adding users who Snapchat presumes to be friends, or adding users without them wanting to be added.

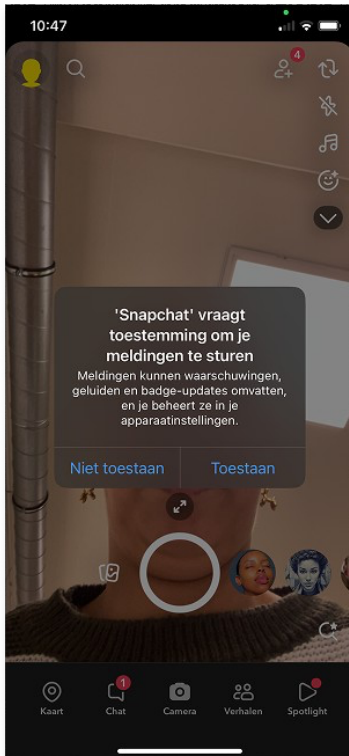


Misdirection by visual interference (deceptive pattern)

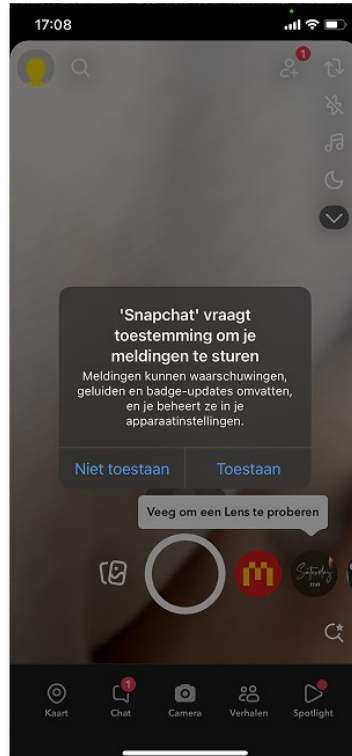
“add 7 friends” is marked by a big blue button, while “skip” is stated in small gray print at the top right. If users select “skip”, they get to see another popup “are you sure”? Again users are directed to “go back”.

Repeated choice pop-up (deceptive pattern)

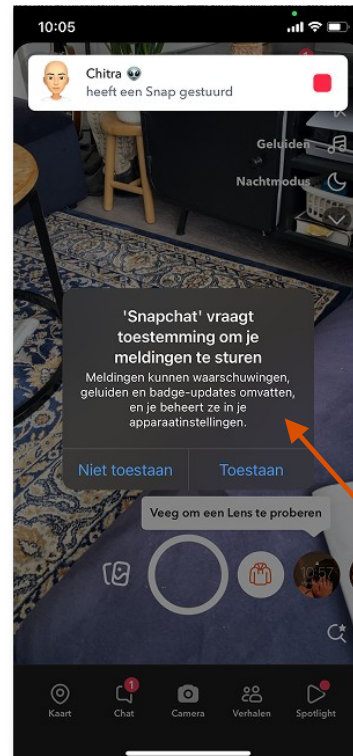
Users are asked to allow notifications of Snapchat. Users who refuse and open the app again after a few days, see the same popup. Moreover, the notification stays on the screen in a yellow bar.



3 april



6 april



Snapchat asks for permission to send notifications

13 april

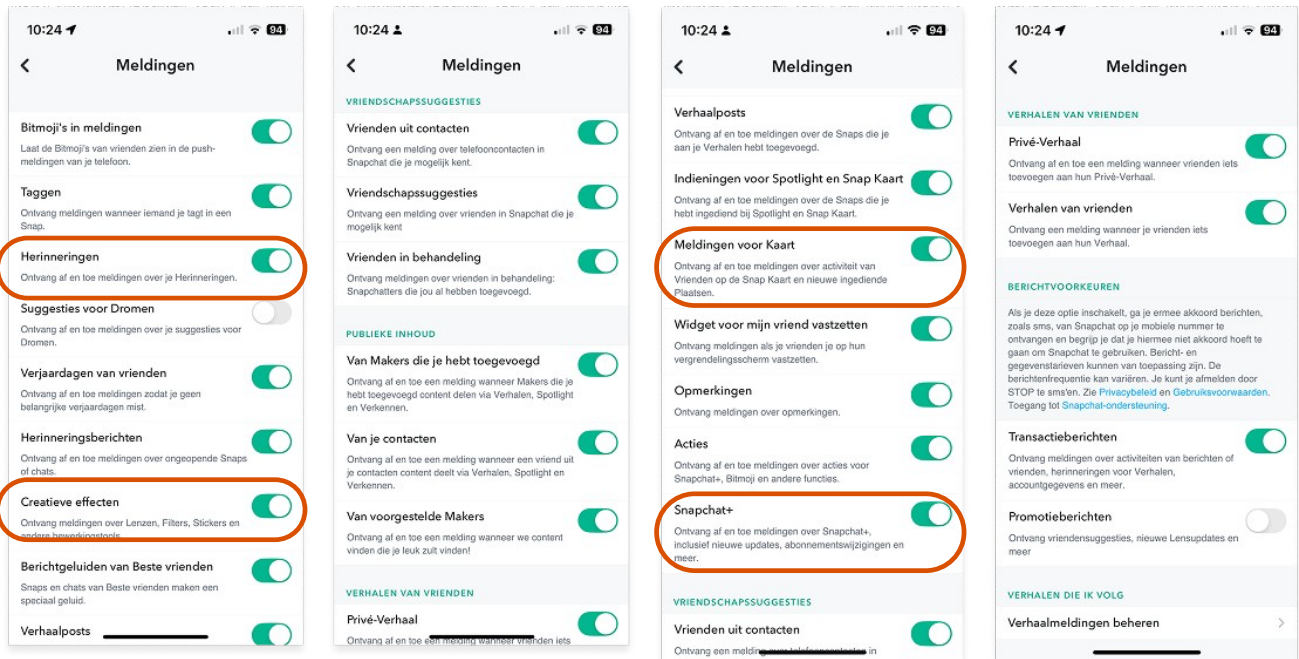


Turn on notifications to not miss any Snap

5.2.2 Settings and receiving of notifications

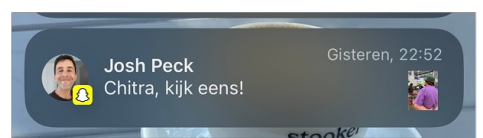
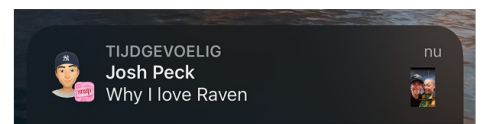
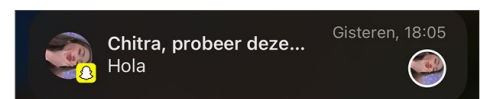
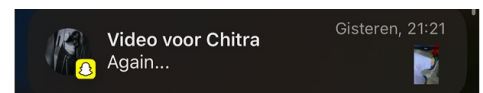
Recapture notifications (attention capturing damaging pattern)

Notifications that are enabled by default include (see photo): reminders, creative effects, map notifications about friends' locations and actions for Snapchat+. These are all notifications not triggered by interactions with users, but generated by the platform.



Fake friend notifications (attention capturing damaging pattern)

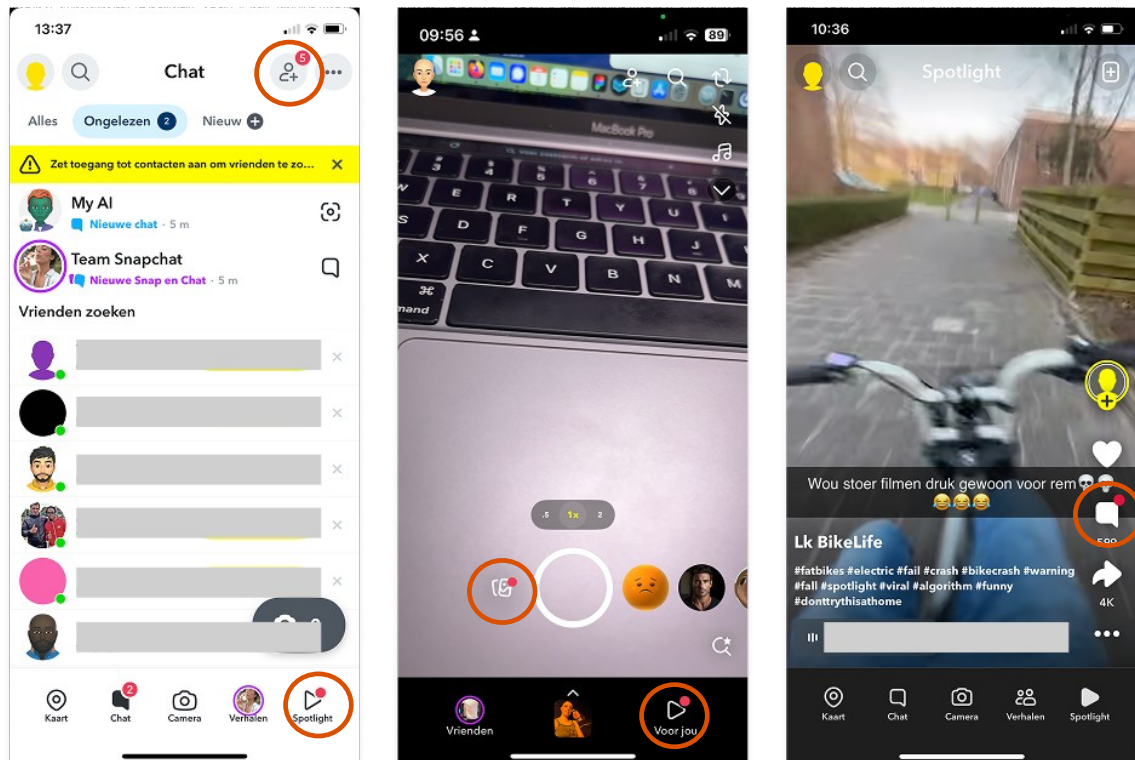
Notifications seem to come from users and to be specifically directed at users, but in reality these are notifications about lenses or recommended videos (generated by the platform) and notifications about new content of people users follow.



5.2.3 Browsing content

Recapture notifications (attention capturing damaging pattern)

Just like Facebook Snapchat frequently uses red *badges*. Not only in interactions with users or for actions users should take but also for new comments on videos (not related to the user), reminders and friend suggestions. As there is always new content in those categories, the red *badge* appears constantly.



Infinite scroll (attention capturing damaging pattern)

On the “Spotlight” video page users can scroll through content endlessly. There will always be new content as they follow suggestions.

Time fog (attention capturing damaging pattern)

The videos do not display any indication of how long they are or how long users have been watching (no time notation, no progress bar). Fast forwarding is not an option.

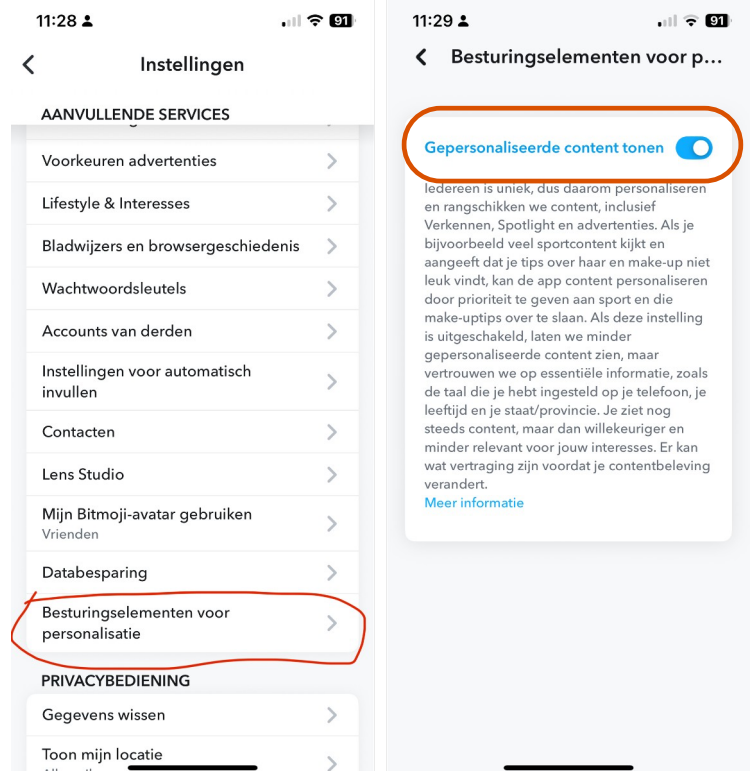
Guilty pleasure recommendations (attention capturing damaging pattern)

The video pages (“Spotlight” and “Discover”) use profiling recommendation systems¹⁷ by default. Based on personal preferences, country, age, language and interactions users have with content, like posting comments, likes, clicking on ads or viewing videos, the system shows content in which users might be interested.

Platforms are required to offer a non-profiling alternative option (Article 38, DSA) that is directly and easily accessible from the specific section of the online platform’s online interface where the information is being prioritized (Article 27 DSA).

At first sight it seems like users cannot select a non-profiling recommendation system. In the comments section there is no direct function/button either to change rankings.

But on the settings page of the app, under “operating elements for personalization” users can disable the setting “show personalized content”, to rank content by age, country and language only. When users open the app the next time, their choice is remembered.



¹⁷ Go to: <https://help.snapchat.com/hc/nl/articles/17338132910484-Personalisatie-op-Snapchat> en <https://help.snapchat.com/hc/nl/articles/8961653169940-Hoe-we-inhoud-rangschikken-op-Spotlight>

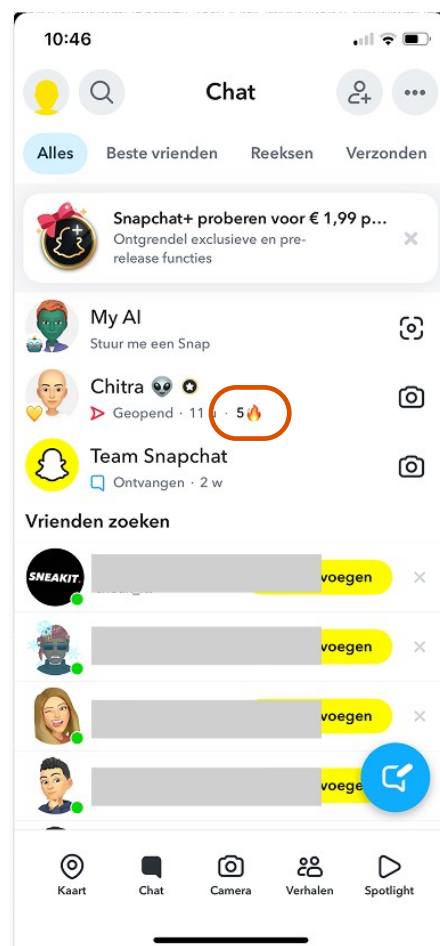
This setting is in another location than the feeds, which makes it hard to find. This could be in breach of the DSA.

It is not clear whether disabling personalization also affects the ranking of comments in comments sections. There is no direct function/button to change rankings. This calls for further investigation.

5.2.4 Interactions

Playing by appointment (attention capturing damaging pattern)

The *snapstreak* keeps track of the number of consecutive days that two users send each other at least one *snap* (photo/video) per day. The number next to the fire emoji indicates the *snapstreak* per chat. If users miss a day, the streak ends. However, users can restore their *streak* against payment (*restore*). Because high *streaks* give users the feeling they have invested a great deal of effort, they find it hard to give up (*sunk-cost fallacy*). By keeping the streak alive, users tell themselves that it is important to them (*effort justification bias*). And then there is the social pressure: some users say that breaking the streak feels like social rejection.¹⁸



¹⁸[Essen & Van Ouytsel, 2023](#)

Grinding (attention capturing damaging pattern)

Based on interactions with other users friendship milestones are awarded (like BF, Bestie, BFF, Super BFF). Users can maintain those milestones only by continually having the most interactions with each other, otherwise they lose their “status”. This, again, is a form of social pressure¹⁹: Users want to keep their status to avoid disappointing others, or they do not want to feel rejected or envious. Then there is the *snapscore*: the total number of snaps sent and received, which signifies a specific social status, and has a competitive effect. Users are encouraged to Snap not just once a day, but much more often.

Friend Emoji Guide 🧡

💖 Super BFF

You have been each other's #1 [Best Friend](#) for two months in a row. This is getting serious!

❤️ BFF

You have been each other's #1 Best Friend for two weeks in a row. Aww!

🧡 Besties

You are each other's #1 Best Friend. You sent the most Snaps to this Snapchatter, and they sent the most Snaps to you, too.

😊 BFs

They're one of your Best Friends! You send a lot of Snaps to this Snapchatter, but they're not your #1 Best Friend.

🤝 Mutual Besties

Your #1 Best Friend is also their #1 Best Friend.

😎 Mutual BFs

One of your Best Friends is also one of this Snapchatter's Best Friends!

🔥 Snapstreak!

You're on a [Snapstreak](#)! This appears next to the number of days that you and a friend have continually Snapped each other.

🕒 Snapstreak is ending

Your Snapstreak is going to end soon! Both you and your friend need to send a Snap to each other within 24 hours, or you'll lose your Snapstreak. Chats and Snaps sent in Groups don't count!

🎂 Birthday

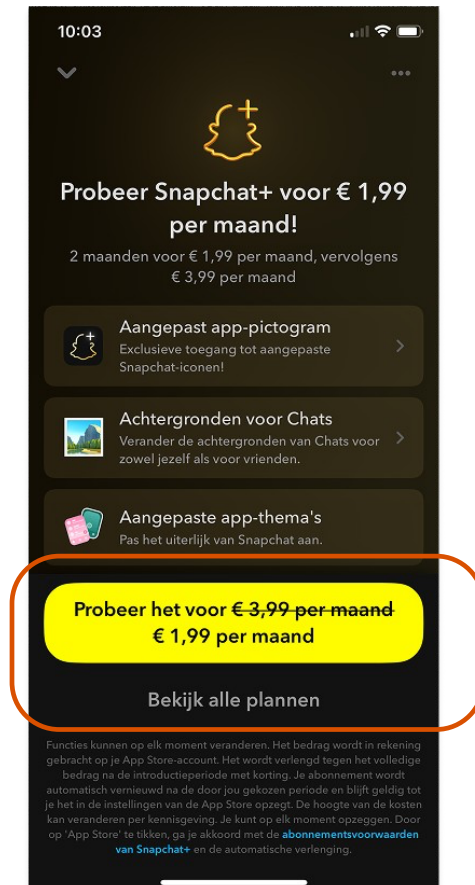
It's your friend's [birthday](#)! This appears next to your friend's name on the date they entered as their birthday on Snapchat.

¹⁹[Essen & Van Ouytsel, 2023](#)

5.2.5 Subscribing and cancelling subscription

Misdirection by visual interference (deceptive pattern)

“Try Snapchat+ for EUR 1.99 a month” says a big yellow button, while “check out all plans” is in gray small print. Users are thus visually directed to the monthly plan first displayed. All subscription plans should be displayed in the same way.

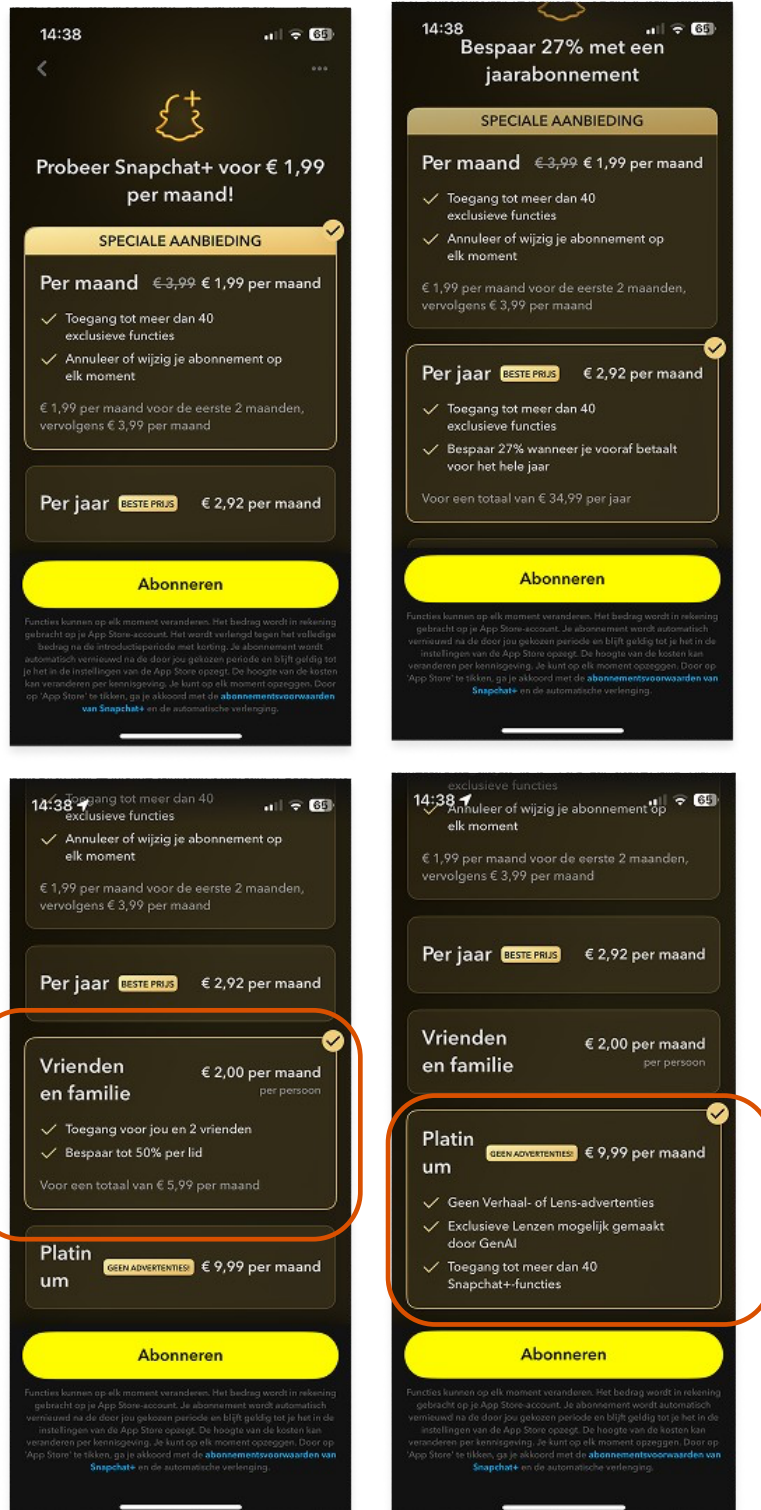


Price comparison prevention (deceptive pattern)

Users can compare subscription plans if they click on “check out all plans” but the different plans are not really clear on what they entail. Users have to click on each plan to view the details, which makes it harder to compare. Although it is clear that the monthly plan comes with exclusive functions, that does not apply to the Friends & Family Plan.

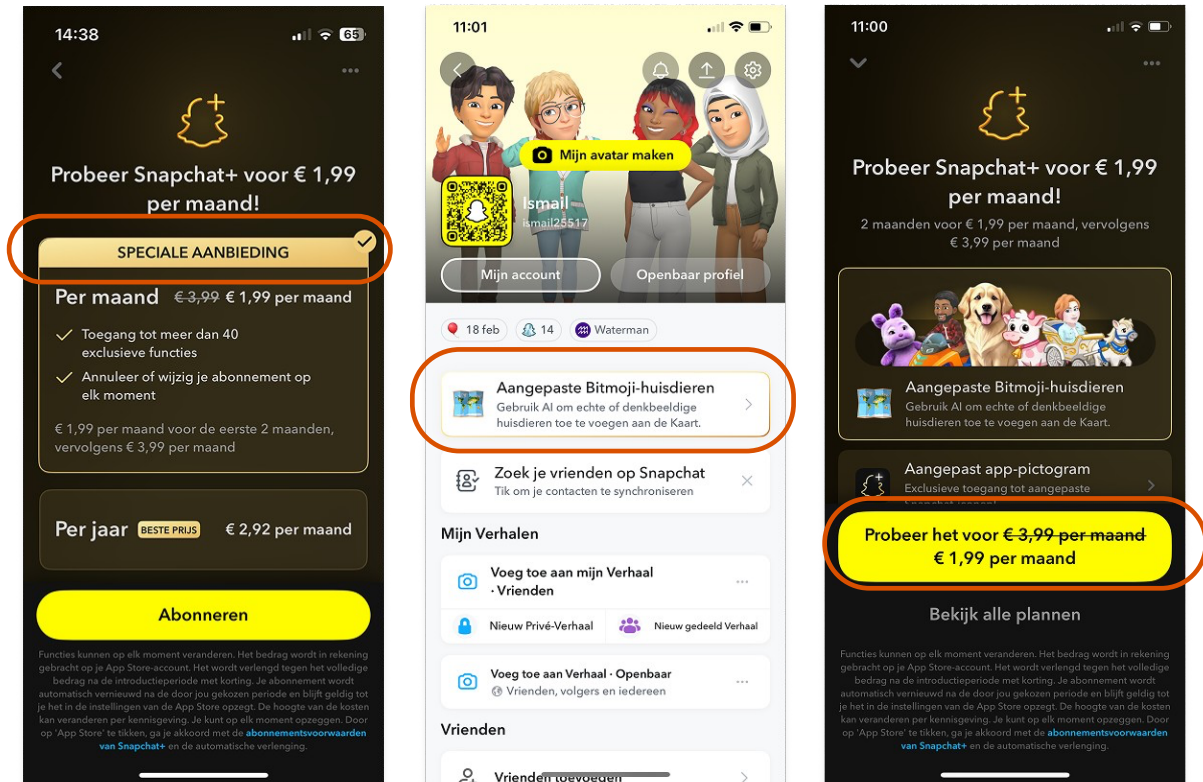
False hierarchy (deceptive pattern)

It is not clear for users that from the starting position of the page they can scroll down, where the other subscription plans appear: “Friends & family” and “Platinum”.



Fake discount (deceptive pattern)

The monthly plan costs EUR 1.99 per month for the first two months, after which it goes up to EUR 3.99. Although Snapchat calls it a special offer, it is on offer all the time.

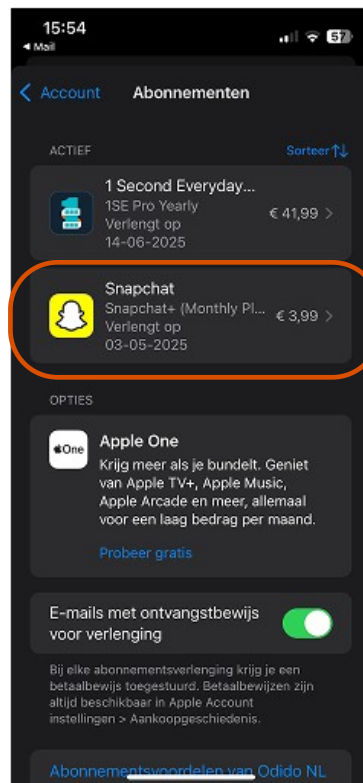
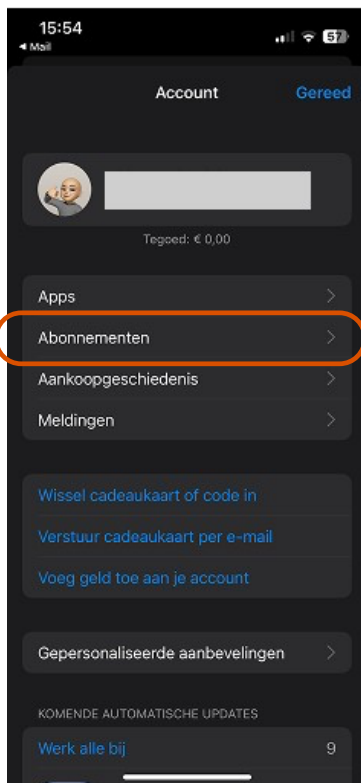


Forced action (deceptive pattern)

Users are presented with an exclusive function (like a customizable “Bitmoji” for their pets) but then it turns out they first have to get Snapchat+. Other examples of functions presented that way: “Priority Story Replies” and “Disable ads”

Roach motel (deceptive pattern)

Users cannot cancel their subscription in the app but have to go to “Subscriptions” in the App store. It takes some detective work and reading the fine print in the email confirming the subscription, but then it is easy to delete the account.



5.3 TikTok

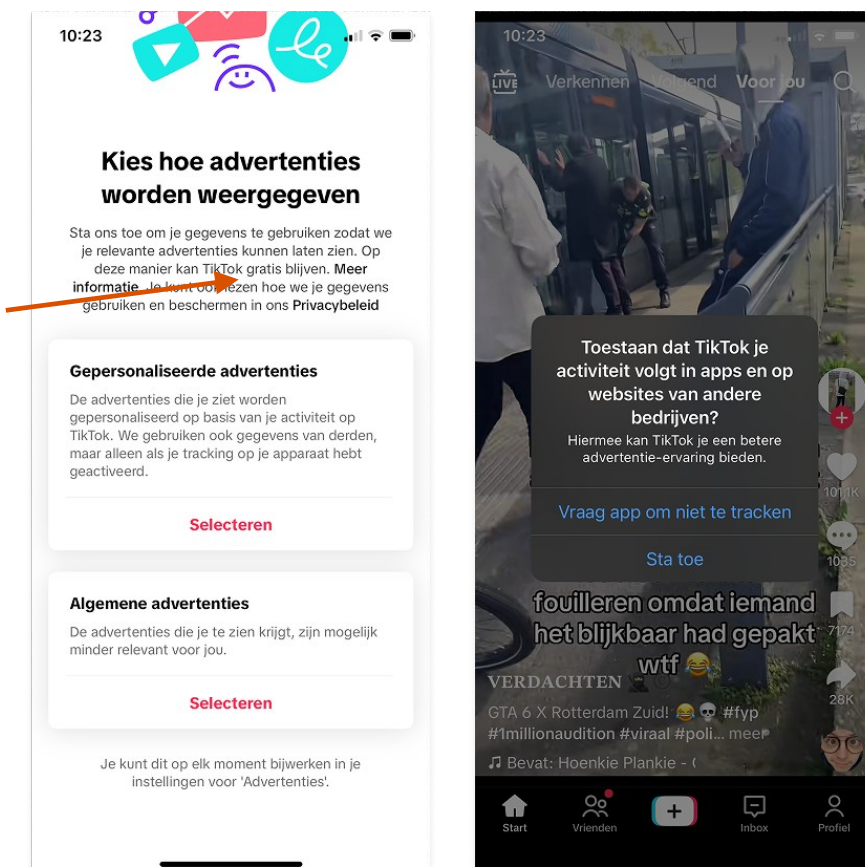
Manipulative design was found during:

- Onboarding
- Settings and receiving of notifications
- Browsing content
- Deleting account

5.3.1 Onboarding

Confirm shaming (deceptive pattern)

“Allow us to use your data so we can show you relevant ads to help TikTok stay free.” This suggests to users that they have to allow personalized ads if they want to continue to use the service free of charge.

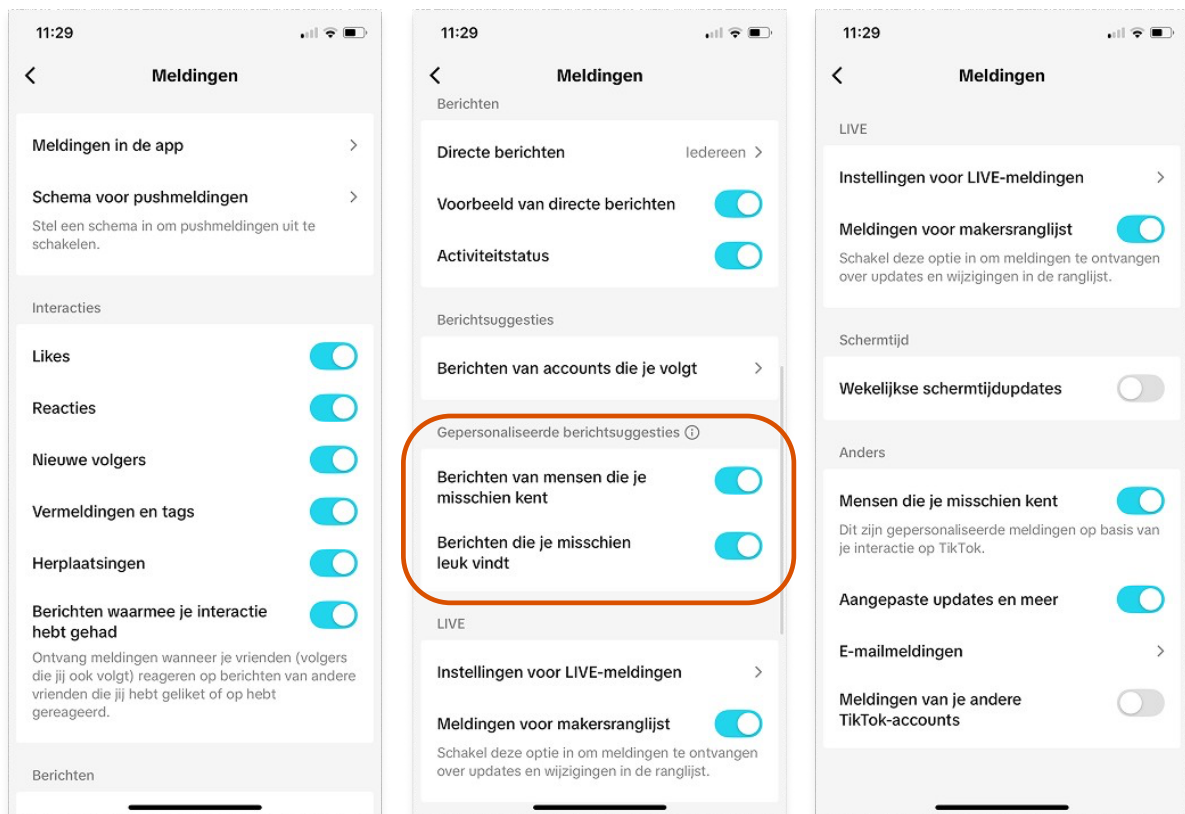
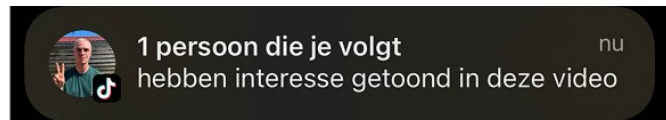


5.3.2 Settings and receiving of notifications

Recapture notifications (attention capturing damaging pattern)

All types of notifications are enabled by default, with the exception of “weekly screen time updates”. “customized updates and more” refer to posts from people users may know or like. Those notifications are generated by the platform and are not triggered by interactions. However, it is comparably easy to disable these notifications.

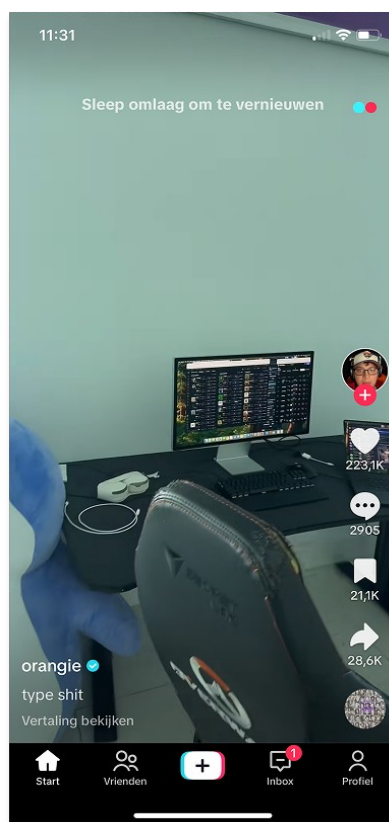
1 person you follow has displayed interest in this video



5.3.3 Browsing content

Infinite scroll (attention capturing damaging pattern) & casino pull-to-refresh (attention capturing damaging pattern)

On the start page (the “for you” feed) users can scroll through content endlessly, and refresh by swiping down. New content will always appear as these are mainly suggestions. “Following” feed can end once users have viewed all videos of the people they follow. In practice, however, users, will not reach the end easily because older videos will come up as well.



Time fog (attention capturing damaging pattern)

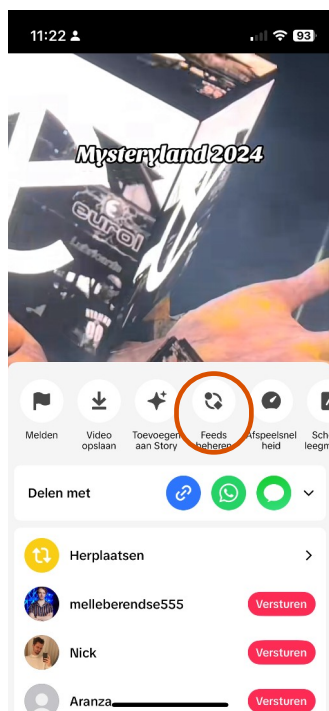
The video's do not display any time notation (minutes and seconds) to show how long users have been watching and how long the video is. Occasionally they show a progress bar that fills up as the video plays.

Guilty pleasure recommendations (attention capturing damaging pattern)

The “for you”, “Following” & “explore” *feeds* use profiling recommendation systems²⁰ by default. Based on location, language and interaction with content, like posting comments, likes, or viewing videos, the system shows content that users might be interested in.

Users can disable this so-called “personalization” by holding on the screen to pause it and tap on “manage *feeds*”. This is how they can make sure that *feeds* and comments sections no longer use personalization. The “for you” feed, for instance, will change into the “popular” *feed*. The content shown to users will still consider the country where they are registered as well as minority, if applicable.

This setting is hard to find. You have to know that you have to hold on the screen. The comments section does not show a direct function/button to change the ranking. The app, however, remembers the personalization setting when opened again.

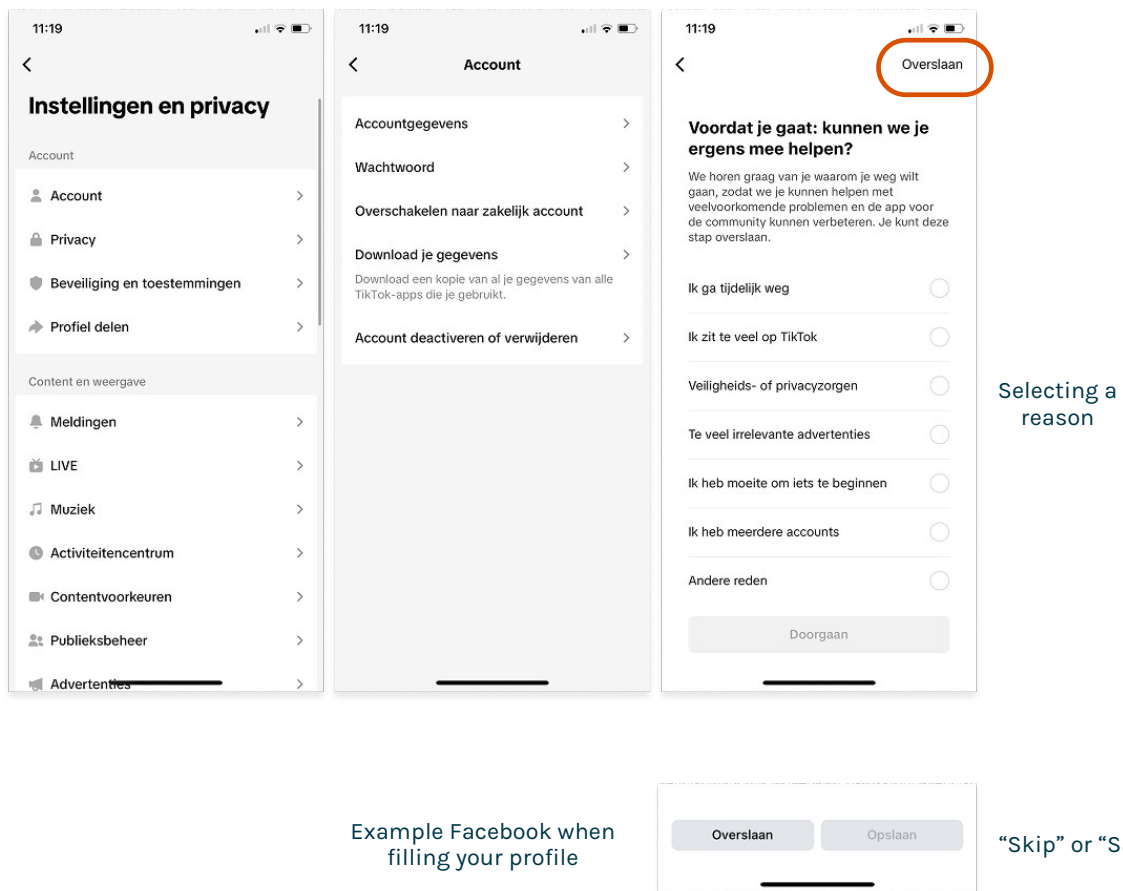


²⁰ Go to <https://support.tiktok.com/nl/using-tiktok/exploring-videos/how-tiktok-recommends-content> en <https://support.tiktok.com/nl/using-tiktok/exploring-videos/how-tiktok-recommends-content>

5.3.4 Deleting account

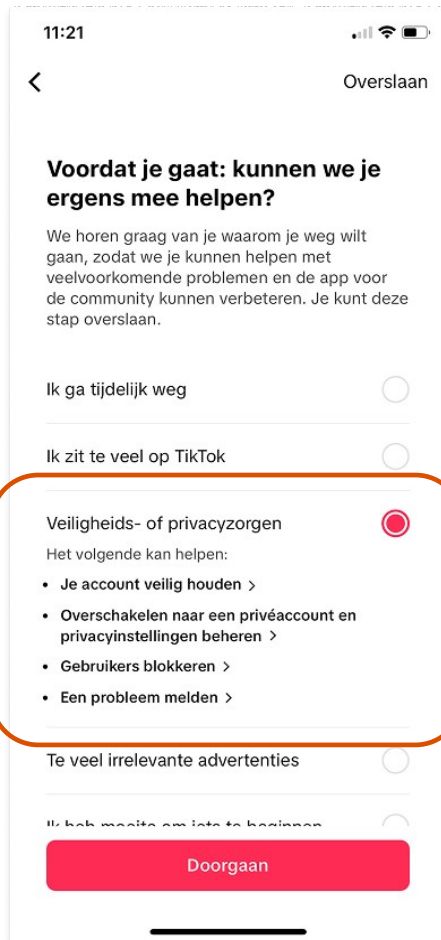
Misdirection by visual interference (deceptive pattern)

Deleting or deactivating the account is easy to find, but like Facebook, users are asked for a reason. It looks like they have to fill in a reason because the “continue” button is gray/inactive. However, at the top right a small button says “skip”. This is how users are directed to filling out a reason. “skip” should be an option equivalent to “continue”, see Facebook for instance.



Roach motel (deceptive pattern)

Depending on the reason selected, suggestions are made for articles on the help page. Users are recommended also to request a copy of their data. These are all extra steps before users can delete their account definitively.



5.4 Shein

Manipulative design was found during:

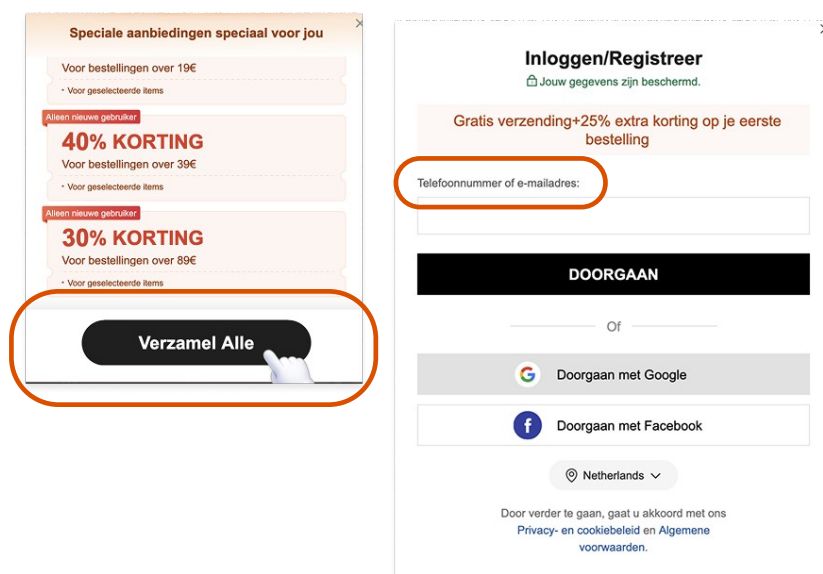
- Onboarding
- Browsing content
- Conducting transactions

The app, notifications and how to delete the account have not been investigated.

5.4.1 Onboarding

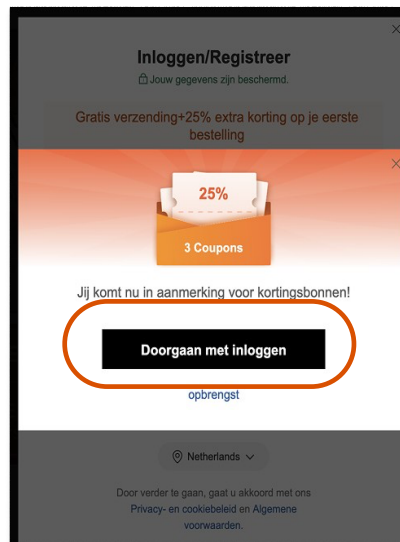
Forced action (deceptive pattern)

Users going to the homepage immediately get to see a popup with discount codes and the text “collect all”. When they click the button, users find out they only get those discount codes when they register as new customers. As they also have to provide personal data, this, too, is a form of *privacy zuckering*.



Bait and switch (deceptive pattern)

Users who click on the X of the popup to log in or register, get a new popup that again directs them to log in and get codes.

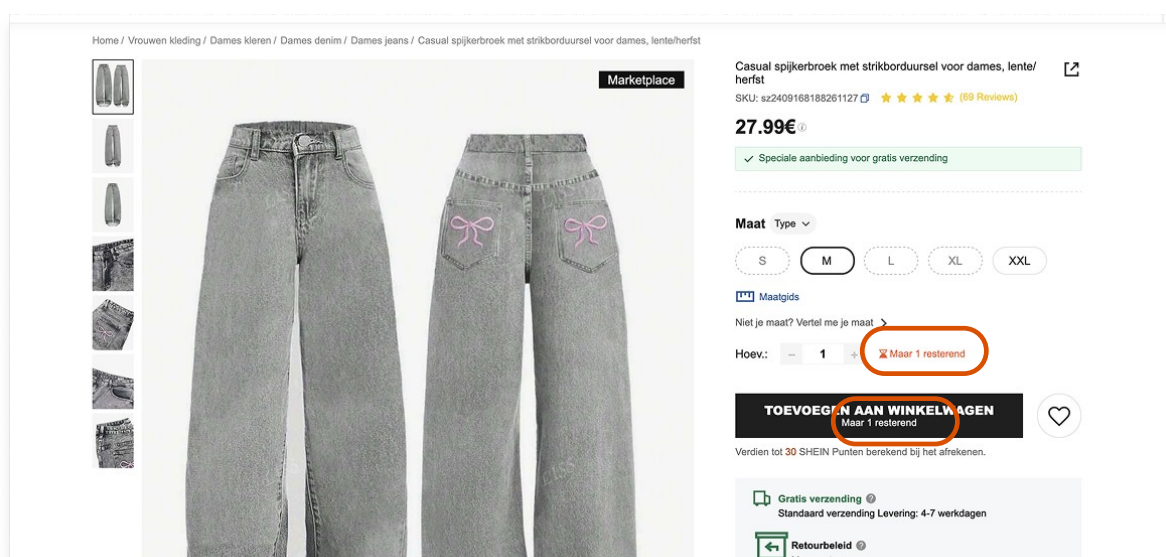


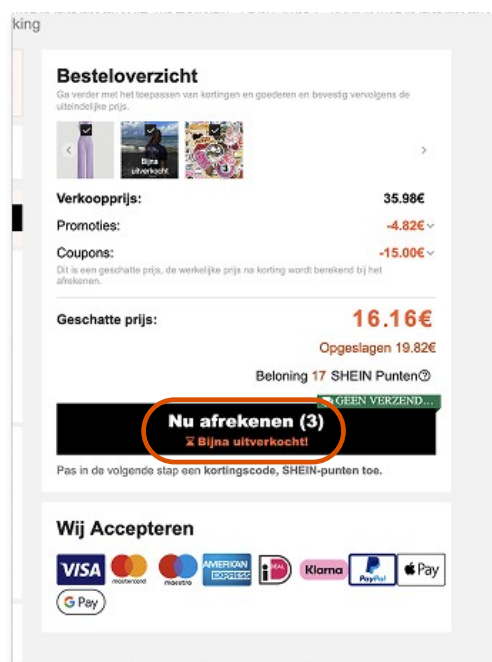
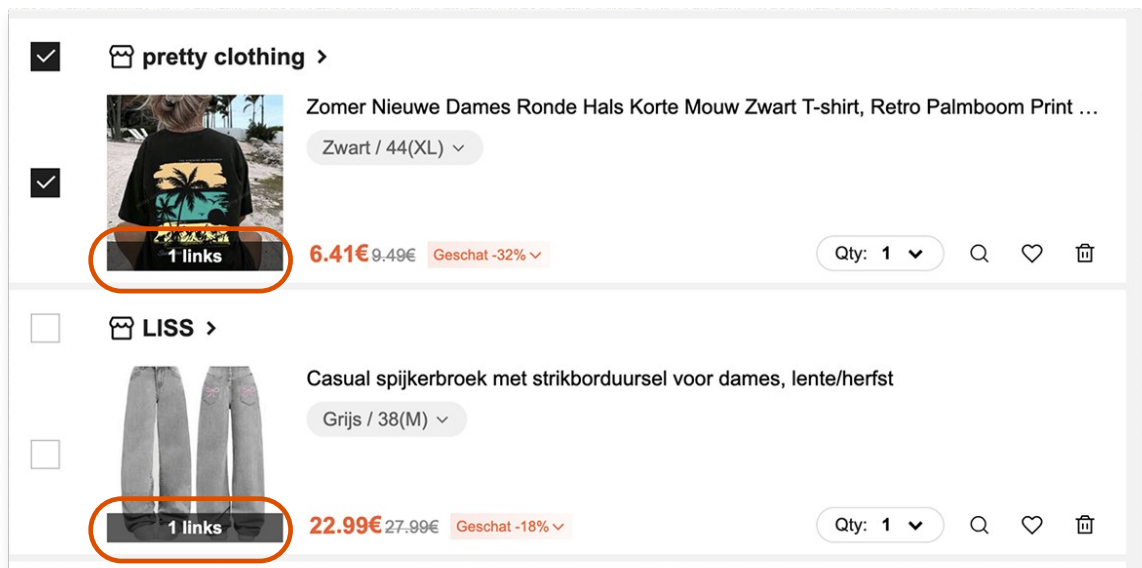
5.4.2 Browsing content

Fake scarcity (deceptive pattern)

Users browsing items see phrases like “pay now, almost sold out” or “only 1 left”. It appears that sometimes those phrases are false:

- On March 12, we added an item labelled “almost sold out” to our basket. On April 25, it is still in the basket.
- On April 4, we added an item labelled “only 1 left” to the basket. On April 17 it is still in the basket.



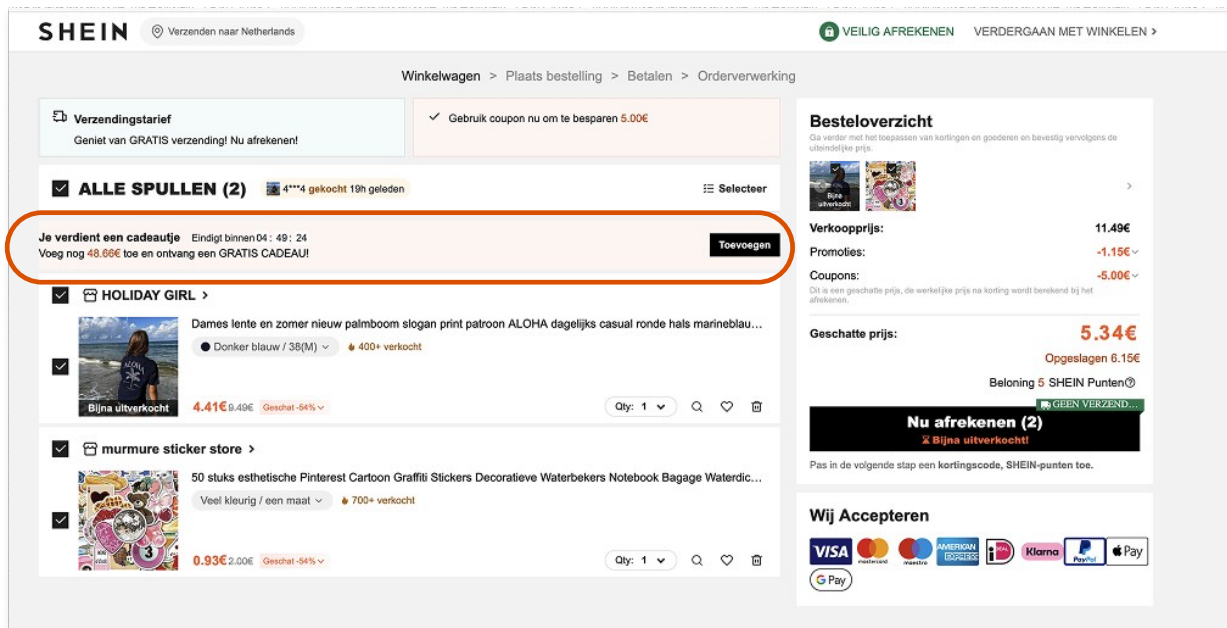


5.4.3 Conducting transactions

Pressured selling (deceptive pattern)

When adding items to their basket, users are informed they can get a gift if they reach a specific threshold:

- “Add another EUR 48 and get a FREE GIFT”
- “Add another EUR 19 to get a EUR 50 discount”



Limited time (deceptive pattern)

Users who have added items to their basket get the option to add a gift. They can only do so within a specific time period. Countdown timers are displayed to manipulate users into acting fast and impulsively.

Mails saying “you don’t want to miss out”, “don’t waste your discount codes” or “use your promo codes before they expire”, also give a sense of time pressure. As do phrases on the website like “pay now, almost sold out” (*fake scarcity*).



<input type="checkbox"/>	☆ SHEIN	Coupon Binnenin: dit wil je niet missen! - Open om uw exclusieve code te krijgen	Mar 14
<input type="checkbox"/>	☆ SHEIN	Verspil je Coupon niet. Gebruik ze zo snel mogelijk voordat ze verlopen! - Verspil je Coupon niet. Gebruik ze zo snel mogelijk voorda...	Mar 13
<input type="checkbox"/>	☆ SHEIN	Coupon Binnenin: dit wil je niet missen! - Open om uw exclusieve code te krijgen	Mar 13
<input type="checkbox"/>	☆ SHEIN	Laat ze niet in jouw winkelwagen liggen! Tijd om ze mee naar huis te nemen. - Verlaagd met 15%!	... Mar 13


Hidden costs (deceptive pattern)

“This is the estimated price, the actual price is calculated at checkout” suggests that the amount can still change. It appears this does not happen or not often.

king

Besteloverzicht

Ga verder met het toepassen van kortingen en goederen en bevestig vervolgens de uiteindelijke prijs.



Verkoopprijs: 35.98€

Promoties: -4.82€ ✓

Coupons: -15.00€ ✓

Dit is een geschatte prijs, de werkelijke prijs na korting wordt berekend bij het afrekenen.

Geschatte prijs: 16.16€

Opgeslagen 19.82€


Beloning 17 SHEIN Punten®

Nu afrekenen (3)

Bijna uitverkocht!

Pas in de volgende stap een kortingscode, SHEIN-punten toe.

Wij Accepteren



GEEN VERZEND...

5.5 Zalando

Manipulative design was found during:

- Tracking
- Onboarding
- Browsing content

We did not investigate the deleting of accounts.

5.5.1 Tracking

Misdirection by visual interference (deceptive pattern)

Users are visually directed to the button “OK” because it is black (Zalando’s primary color) while the other buttons are white. The buttons should be equivalent, identical in design, so as not to influence the users’ choice.

Confirm shaming (deceptive pattern)

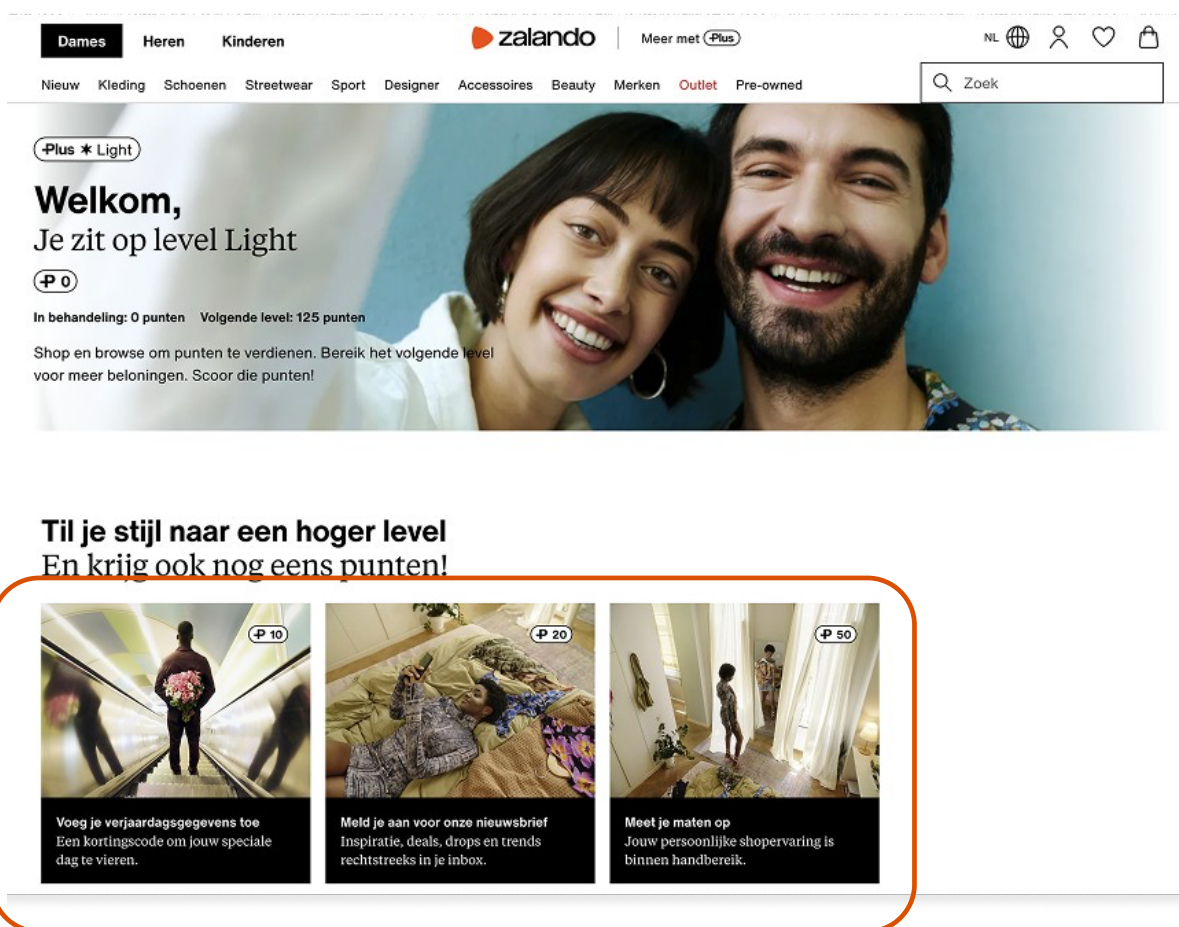
“Would you like a more personal experience” is written in big bold print, while small print informs users that they have to share data and allow *tracking* to get that experience. “OK” yields little information (*hidden information*), ‘Allow all cookies’, for instance, would be clearer.



5.5.2 Onboarding

Privacy zuckering (deceptive pattern)

Members of the loyalty program get points by providing personal information like measurements, and date of birth. The more points they earn, the higher their level within the loyalty program. Based on their level, users get advantages like free delivery, premium customer service, first access to restocks, or invitations to events.



Hidden information (deceptive pattern)

Users can earn points by providing their date of birth. In return they will receive a discount code on their birthday. It then turns out that the discount code can be used only if users have collected enough points for the next level. Points are earned, inter alia, by making purchases (*grinding*).

Zalando Plus

Tijd om jouw verjaardag te vieren!

Vier je verjaardag met een cadeautje! Voeg je gegevens toe en ontvang een kortingscode op je speciale dag.

P 10 Plus-punten

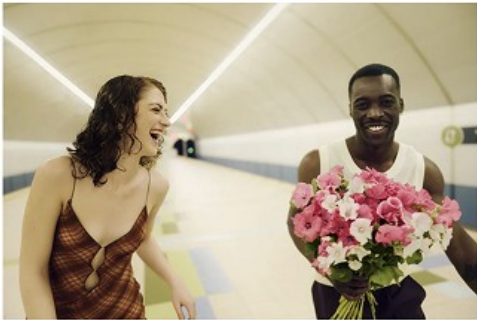
Geboortedatum

dd - mm - jjjj

Bekijk onze [Privacyverklaring](#) voor meer informatie over hoe wij jouw gegevens verwerken.

Opslaan

Zalando Plus



Yes!

We kunnen niet wachten om het samen te vieren

Je krijgt een kortingscode op je verjaardag zodra je Plus Shine hebt bereikt. Hier zijn wat extra punten om je daar een handje bij te helpen.

P +10 Plus-punten gespaard

Laat je inspireren

Ga naar Plus

Forced action (deceptive pattern)

Users can also earn points by adding their measurements. Users who want to add their measurements, find out they can only do so by downloading the app and having their body scanned by the camera.



Laat je maten opmeten in de Zalando-app

Met onze nieuwe tech kun je in 5 minuten je maten opmeten in onze app. Scan de QR-code om deze nu te openen.

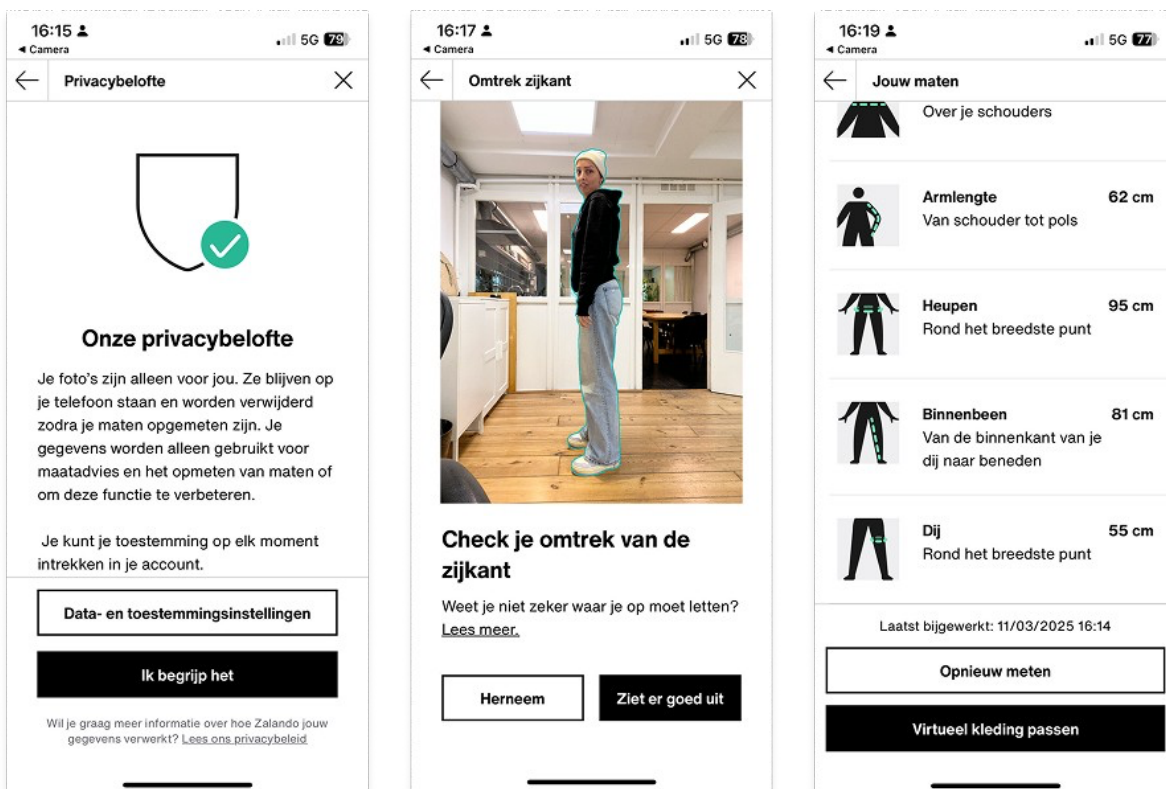
Weet je niet zeker of je onze app geïnstalleerd hebt?

1. Scan de QR-code een eerste keer om de app te installeren
2. Kom terug en scan dezelfde QR-code nogmaals om je mate op te meten!



ONTDEK HET OP Google Play

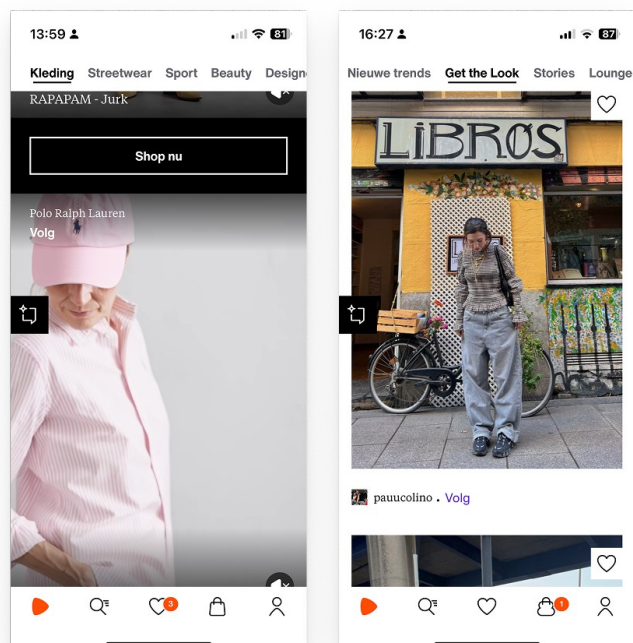
Download in de App Store



5.5.3 Browsing content

Infinite scroll (attention capturing damaging pattern)

The start page of the app contains several different *feeds*. Users can scroll endlessly through some of those feeds, like “get the look”. New content will appear constantly, as the app uses suggestions.



5.6 Booking.com

Manipulative design was found during:

- Browsing content

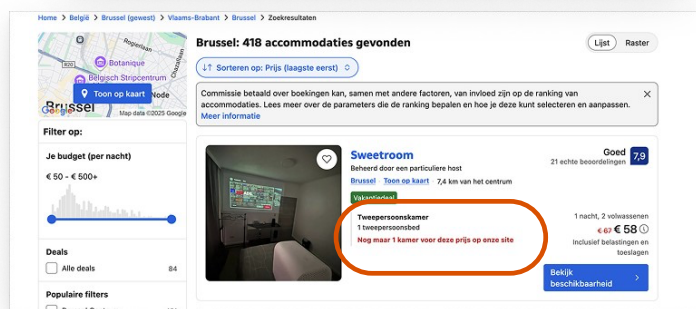
We did not investigate the app, notification or how to delete accounts.

5.6.1 Browsing content

Booking.com uses many phrases to convey a sense of urgency.

- “Not usually available, you’re in luck!”
- “Only 1 room left at this price on our site”
- “Limited supply in Brussels for your dates: 11 B&B’s like this are already unavailable on our site”
- “You’re booking the last available [room type] we have at [hotel] on our site” ‘

It is impossible to verify whether those statements are legitimate. Users can (wrongly) get the feeling that they have to decide quickly.



6. Follow-up

What will we do with our insights?

Out of the above-described user flows we made a top three of what we believed to be the most harmful patterns. These are the three on which we want to act.

1. Facebook, Snapchat and TikTok: notifications and red badges (recapture notifications, fake friend notifications, repeated choice pop-up);
2. Facebook, Snapchat and TikTok: profiling recommendation systems in content and comments (hidden information, false hierarchy, guilty pleasure recommendations)
3. Snapchat: finding and adding friends (misdirection by visual interference, pre-selection).

Based on our top three we will outline three research proposals that should contribute to our lobby or should result in enforcement action. In our research we will zoom in on the pattern in its specific context and adduce more evidence. We will demonstrate why a pattern is harmful by expanding on user behavior and experience. Finally, we will make recommendations for specific alternative options.

7. Annexes

i. Sources

1. Bartoli, N., & Benedetto, S. (2022). *Driven by notifications—exploring the effects of badge notifications on user experience*. Plos one, 17(6), e0270888.
<https://doi.org/10.1371/journal.pone.0270888>
2. Brignull, H., Miquel, M., Rosenberg, J., & Offer, J. (2015) *Dark Patterns - User Interfaces Designed to Trick People*.
<http://darkpatterns.org/>
3. Cara, C. (2020). *Dark patterns in the media: A systematic review*. Network Intelligence Studies, Volume VII, Issue 14.
https://www.researchgate.net/publication/341105338_DARK_PATTERNS_IN_THE_MEDIA_A_SYSTEMATIC_REVIEW
4. European Commission, Directorate-General for Justice and Consumers, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Lica, G., Lechardoy, L., & Rodríguez de las Heras Ballell, T. and others. (2022). *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation: Final Report*. Publications Office of the European Union 2022.
<https://data.europa.eu/doi/10.2838/859030>
5. Essen, C. M., & Van Ouytsel, J. (2023). *Snapchat streaks—How are these forms of gamified interactions associated with problematic smartphone use and fear of missing out among early adolescents?*. Telematics and Informatics Reports, Volume 11, 2023, 100087, ISSN 2772-5030,
<https://doi.org/10.1016/j.teler.2023.100087>
6. Gray, C. M., Bielova N., Santos, C., & Mildner, T. (2024). *An Ontology of Dark Patterns: Foundations, Definitions, and a Structure for Transdisciplinary Action*. In Proceedings of the CHI Conference on Human Factors in Computing Systems, 31 pages.
<https://doi.org/10.48550/arXiv.2309.09640>
7. Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). *The Dark (Patterns) Side of UX Design*. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, p 534. <https://doi.org/10.1145/3173574.3174108>

8. Gray, C. M., Mildner, T. & Gairola, R. (2025). *Getting Trapped in Amazon's "Iliad Flow": A Foundation for the Temporal Analysis of Dark Patterns*. In CHI Conference on Human Factors in Computing Systems (CHI'25), April 26–May 01, 2025, Yokohama, Japan. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3706598.3713828>

9. Leiser, M., & Santos, C. (2023). *Dark Patterns, Enforcement, and the emerging Digital Design Acquis: Manipulation beneath the Interface*. (pp. 1-31). SSRN. <https://research.vu.nl/en/publications/53ce5bf6-58a2-47c1-af82-a9e5e6233972>

10. Leiser, M., & Yang, W.-T. (2023). *Illuminating Manipulative Design: from 'Dark Patterns' to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive*. Loyola Consumer Law Review, 34(3), 484-528. Article 6. <https://lawecommons.luc.edu/lclr/vol34/iss3/6>

11. Monge Rofarello, A., Lukof, K., & De Russis, L. (2023). *Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces*. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, Hamburg, Germany. ACM, New York, NY, USA, 19 pages. <https://doi.org/10.1145/3544548.3580729/>

12. Ruohonen, J., Koskinen, J., Harnow Klausen, S., & Gerdes, A. (2025). *A Scenario Analysis of Ethical Issues in Dark Patterns and Their Research*. <https://doi.org/10.48550/arXiv.2503.01828>

13. Soysal, İ. (2025). *Attention Integrity: On How to Protect Society from Harmful Effects of Attention-Grabbing Technologies with Regulation* [Unpublished Master's thesis]. Tilburg Institute for Law, Technology, and Society. <https://arno.uvt.nl/show.cgi?fid=182379>

ii. VLOP's

VLOPs are large online platforms and search engines that in Europe have at least 45 million active users per month. On April 25, 2023 the European Commission published the first list of VLOP's. Every now and then new platforms are added to the list. Platforms frequently object to being included. Below the latest update of the list: <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>

- Alibaba
- AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- Shein
- TikTok
- Temu
- Twitter/X
- Wikipedia
- YouTube
- Zalando

Search engines

- Bing
- Google Search

Porn sites

- Pornhub
- Stripchat
- Xvideos
- Xnxx

iii. Digital Services Act (“DSA”)

Article 25

Online interface design and organization

1. Providers of online platforms shall not design, organize or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.

2. The prohibition in paragraph 1 shall not apply to practices covered by Directive 2005/29/EC or Regulation (EU) 2016/679.

3. The Commission may issue guidelines on how paragraph 1 applies to specific practices, notably:

- (a) giving more prominence to certain choices when asking the recipient of the service for a decision;
- (b) repeatedly requesting that the recipient of the service make a choice where that choice has already been made, especially by presenting pop-ups that interfere with the user experience;
- (c) making the procedure for terminating a service more difficult than subscribing to it.

iv. Unfair Commercial Practices Directive (“UCPD”)

a. Article 5

Prohibition of unfair commercial practices

1. Unfair commercial practices shall be prohibited.
2. A commercial practice shall be unfair if:
 - (a) it is contrary to the requirements of professional diligence, and
 - (b) it materially distorts or is likely to materially distort the economic behavior with regard to the product of the average consumer whom it reaches or to whom it is addressed, or of the average member of the group when a commercial practice is directed to a particular group of consumers.
3. Commercial practices which are likely to materially distort the economic behavior only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group. This is without prejudice to the common and legitimate advertising practice of making exaggerated statements or statements which are not meant to be taken literally.
4. In particular, commercial practices shall be unfair which:
 - (a) are misleading as set out in Articles 6 and 7, or
 - (b) are aggressive as set out in Articles 8 and 9.
5. Annex I contains the list of those commercial practices which shall in all circumstances be regarded as unfair. The same single list shall apply in all Member States and may only be modified by revision of this Directive.

b. Article 6

Misleading actions

1. A commercial practice shall be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise:
 - (a) the existence or nature of the product;
 - (b) the main characteristics of the product, such as its availability, benefits, risks, execution, composition,

accessories, after-sale customer assistance and complaint handling, method and date of manufacture or provision, delivery, fitness for purpose, usage, quantity, specification, geographical or commercial origin or the results to be expected from its use, or the results and material features of tests or checks carried out on the product;

- (c) the extent of the trader's commitments, the motives for the commercial practice and the nature of the sales process, any statement or symbol in relation to direct or indirect sponsorship or approval of the trader or the product;
 - (d) the price or the manner in which the price is calculated, or the existence of a specific price advantage;
 - (e) the need for a service, part, replacement or repair;
 - (f) the nature, attributes and rights of the trader or his agent, such as his identity and assets, his qualifications, status, approval, affiliation or connection and ownership of industrial, commercial or intellectual property rights or his awards and distinctions;
 - (g) the consumer's rights, including the right to replacement or reimbursement under Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees⁽¹⁾, or the risks he may face.
2. A commercial practice shall also be regarded as misleading if, in its factual context, taking account of all its features and circumstances, it causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise, and it involves:
- (a) any marketing of a product, including comparative advertising, which creates confusion with any products, trademarks, trade names or other distinguishing marks of a competitor;
 - (b) non-compliance by the trader with commitments contained in codes of conduct by which the trader has undertaken to be bound, where:
 - (i) the commitment is not aspirational but is firm and is capable of being verified,
 - and
 - (ii) the trader indicates in a commercial practice that he is bound by the code.

c. Article 7

Misleading omissions

1. A commercial practice shall be regarded as misleading if, in its factual context, taking account of all its features and circumstances and the limitations of the communication medium, it omits material information that the average consumer needs, according to the context, to take an informed transactional decision and thereby causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.
2. It shall also be regarded as a misleading omission when, taking account of the matters described in paragraph 1, a trader hides or provides in an unclear, unintelligible, ambiguous or untimely manner such material information as referred to in that paragraph or fails to identify the commercial intent of the commercial practice if not already apparent from the context, and where, in either case, this causes or is likely to cause the average consumer to take a transactional decision that he would not have taken otherwise.
3. Where the medium used to communicate the commercial practice imposes limitations of space or time, these limitations and any measures taken by the trader to make the information available to consumers by other means shall be taken into account in deciding whether information has been omitted.
4. In the case of an invitation to purchase, the following information shall be regarded as material, if not already apparent from the context:
 - (a) the main characteristics of the product, to an extent appropriate to the medium and the product;
 - (b) the geographical address and the identity of the trader, such as his trading name and, where applicable, the geographical address and the identity of the trader on whose behalf he is acting;
 - (c) the price inclusive of taxes, or where the nature of the product means that the price cannot reasonably be calculated in advance, the manner in which the price is calculated, as well as, where appropriate, all additional freight, delivery or postal charges or, where these charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable;
 - (d) the arrangements for payment, delivery, performance and the complaint handling policy, if they depart from the requirements of professional diligence;
 - (e) for products and transactions involving a right of withdrawal or cancellation, the existence of such a right.
5. Information requirements established by Community law in relation

to commercial communication including advertising or marketing, a non-exhaustive list of which is contained in Annex II, shall be regarded as material.

d. Annex I

COMMERCIAL PRACTICES WHICH ARE IN ALL CIRCUMSTANCES CONSIDERED UNFAIR

Misleading commercial practices

1. Claiming to be a signatory to a code of conduct when the trader is not.
2. Displaying a trust mark, quality mark or equivalent without having obtained the necessary authorization.
3. Claiming that a code of conduct has an endorsement from a public or other body which it does not have.
4. Claiming that a trader (including his commercial practices) or a product has been approved, endorsed or authorized by a public or private body when he/it has not or making such a claim without complying with the terms of the approval, endorsement or authorization.
5. Making an invitation to purchase products at a specified price without disclosing the existence of any reasonable grounds the trader may have for believing that he will not be able to offer for supply or to procure another trader to supply, those products or equivalent products at that price for a period that is, and in quantities that are, reasonable having regard to the product, the scale of advertising of the product and the price offered (bait advertising).
6. Making an invitation to purchase products at a specified price and then:
 - (a). refusing to show the advertised item to consumers; or
 - (b) refusing to take orders for it or deliver it within a reasonable time; or
 - (c) demonstrating a defective sample of it,With the intention of promoting a different product (bait and switch).
7. Falsely stating that a product will only be available for a very limited time, or that it will only be available on particular terms for a very limited time, in order to elicit an immediate decision and deprive consumers of sufficient opportunity or time to make an informed choice.
8. Undertaking to provide after-sales service to consumers with whom the trader has communicated prior to a transaction in a language which is not an official language of the Member State where the trader is located and then making such service available only in another language without clearly disclosing this to the consumer before the consumer is committed to the transaction.
9. Stating or otherwise creating the impression that a product can legally be sold when it cannot.
10. Presenting rights given to consumers in law as a distinctive feature

of the trader's offer.

11. Using editorial content in the media to promote a product where a trader has paid for the promotion without making that clear in the content or by images or sounds clearly identifiable by the consumer (advertorial). This is without prejudice to Council Directive 89/552/EEC⁽¹⁾.
12. Making a materially inaccurate claim concerning the nature and extent of the risk to the personal security of the consumer or his family if the consumer does not purchase the product.
13. Promoting a product similar to a product made by a particular manufacturer in such a manner as deliberately to mislead the consumer into believing that the product is made by that same manufacturer when it is not.
14. Establishing, operating or promoting a pyramid promotional scheme where a consumer gives consideration for the opportunity to receive compensation that is derived primarily from the introduction of other consumers into the scheme rather than from the sale or consumption of products.
15. Claiming that the trader is about to cease trading or move premises when he is not.
16. Claiming that products are able to facilitate winning in games of chance.
17. Falsely claiming that a product is able to cure illnesses, dysfunction or malformations.
18. Passing on materially inaccurate information on market conditions or on the possibility of finding the product with the intention of inducing the consumer to acquire the product at conditions less favorable than normal market conditions.
19. Claiming in a commercial practice to offer a competition or prize promotion without awarding the prizes described or a reasonable equivalent.
20. Describing a product as “gratis”, “free”, “without charge” or similar if the consumer has to pay anything other than the unavoidable cost of responding to the commercial practice and collecting or paying for delivery of the item.
21. Including in marketing material an invoice or similar document seeking payment which gives the consumer the impression that he has already ordered the marketed product when he has not.
22. Falsely claiming or creating the impression that the trader is not acting for purposes relating to his trade, business, craft or profession, or falsely representing oneself as a consumer.
23. Creating the false impression that after-sales service in relation to a product is available in a Member State other than the one in which the product is sold.

Bits of Freedom fights for your freedom and privacy on the internet.

These fundamental rights are essential for your development, for technological innovation and for the rule of law. But this freedom isn't self-evident. Your data is being stored and analysed. Your internet traffic is slowed down and blocked.

Bits of Freedom makes sure that your internet is your business.

Bits of Freedom
bitsoffreedom.nl
🐦 [@bitsoffreedom](https://twitter.com/bitsoffreedom)
Prinseneiland 97HS
1013 LN Amsterdam

Contact:
Chitra Mohanlal
+31 6 1261 7199
chitra@bitsoffreedom.nl

BITS OF FREEDOM