Trust, Transparency and Control Labs

Best Practices for People-Centric Consent Design

This report presents the key findings from an ongoing program of work and industry consultation undertaken by the Trust, Transparency and Control Labs team at Meta.

Meta

In collaboration with CraigWalker

What you'll find in this best practices guide

Introduction to best practices for people-centric consent design

As more and more people engage with digital products and services, there is a need to find new ways of empowering them over their personal data and privacy. Transparency, education, controls and consent moments have emerged as key UX tools in achieving this aim.

This best practice guide focuses on **consent moments**. How can we design consents that empower users, balancing their need for control with usability?

It has been informed by an ongoing program of work, co-design and industry consultation into consent design. Since 2017, Trust, Transparency & Control Labs have been running Design Jam workshops with companies throughout the world (including São Paulo, Berlin, Singapore, Dublin, Mexico City, New Delhi, Brussels and Washington DC).

In 2020, we published a report on "People-Centric Approaches to Notice, Consent, and Disclosure" and in 2023 we published a report on "Data Transparency and Control in XR and the Metaverse".

From all of these collaborative workshops and programs across the globe, we have synthesized some of the best practices and approaches towards designing user-centric consent experiences.

This guide is intended to be useful for product teams building solutions with privacy as default, and for policy experts looking for ways to translate high-level guidance into something more concrete.

What we mean by....

Consent moment
The moment in a product or service experience where a user is asked to give permission for their data to be collected or used. This may be a single notice or a series of questions, and may happen more than once.

Transparency
Transparency means designing product experiences that are open, encouraging people to understand their data collection and give informed consent.

Control
Control gives users the ability to have meaningful agency over their relationship with their data or a given processing activity.

Striking the right balance between control and consent fatigue

The promise of **consent** is to give users control over when and how their data is processed. If users are informed, they can make better decisions about their privacy and exert control over how and when their data is shared.

However, there is a central tension inherent in this promise: on the one hand, the need to give users enough information and granular control, and on the other the risk of causing **consent fatigue**.

When designed well, consent is a **moment to pause**, adding friction to slow the user down. This gives them time and space to make an informed choice. Best-practice consent moments prompt a "lean-in" experience where people are engaged in their privacy choice and, as a result, are more likely to make informed decisions.

However, using consent too frequently or indiscriminately risks adding too much friction. This can cause users to disengage, make arbitrary decisions and for product makers may force a trade-off between ease of use and meaningful engagement. In this way, paradoxically, more consent moments may lead to less control for users.

Around the world, policy and product makers have been trying to strike a balance between these tensions, so users make informed decisions about their data.

The **European Commission** recently noted in their Cookie Pledge, that "many people are tired of having to engage constantly with complex cookie banners generating the so-called cookies fatigue and as a result they may simply give up trying to express their real privacy preferences".

In **Australia**, the Australian Privacy Act Review Report has stated that "an over-reliance on notice and consent can place an unrealistic burden on individuals to understand the risks of complicated information handling practices and may not result in improved privacy outcomes".

The National Privacy Commission in the **Philippines** is actively advocating for companies to move away from an over-reliance on consent, stating that "organizations must avoid consent fatigue by properly identifying the lawful basis for processing prior to any data collection. If another lawful basis applies, then a request for consent is unnecessary and does not need to be made".

We present the design patterns in this report as a continuation of a long-running conversation about consent moments, and how design thinking can help us create consent that lives up to its promise – **empowering users with more control over their data**.

How to use this report

These best practices for consent patterns have been developed to guide product makers and policy makers in thinking around the design of consent moments.

They are not intended to be definitive standards, but are instead aspirational best practices or suggestions.

The report contains illustrative examples with annotations intended to help ground these practices in real-world contexts.

There are two types of examples: “Best practices” and “To be avoided”.

Best practices
Best practices or suggested approaches.

To be avoided
Practices that might undermine a good consent moment for users.

These examples are not intended to be comprehensive or absolute, and there may be contexts where a “To be avoided” practice is okay, or even desirable. Conversely, there may be contexts where the “Best practices” do not apply.

This guidance is not intended to be legal advice

One of the key challenges that emerged during our workshops was the **significant variation** in approaches and attitudes to consent throughout the world. From country to country and region to region, we encountered many different cultural, social and legal perspectives on consent.

This best practice guidance is based around user experience, rather than starting with laws and regulations. While a lot of this research has come from workshops with policy and legal experts, it has not been created to comply with any one jurisdiction. As such, it is not intended to be legal advice, and you should **always consult with legal counsel in your region**.

We hope it is a starting point when thinking through better consent design for users, no matter where they live.

FRAMEWORK

Consent archetypes: three patterns

This guide presents **three archetypes** for consent moments. From our workshops, these emerged as the three most common design patterns that can be used to obtain permission from a user to process their data.

The following consent archetypes are broad categories that designers can use as a starting point in designing a consent moment.

When considering what consent archetype might be best for a particular context, it is useful to consider the **purpose** and **context** of the consent.

Each archetype has a design pattern, a description and an overview of the user need and product context that it best serves.

Total

This design approach best used for necessary data processing. It's a "take it or leave it" moment that communicates to users that if they decline consent, they will not be able to use the service.

Tiered

This design approach gives the user high-level options, so they can choose a service level. Each service level has preset data processing activities.

Selective

This design approach gives users a clear affirmative / negative option, usually with two buttons. It allows them to opt into or out of optional data processing while still using the main service.

CONSENT ARCHETYPES

Total Consent

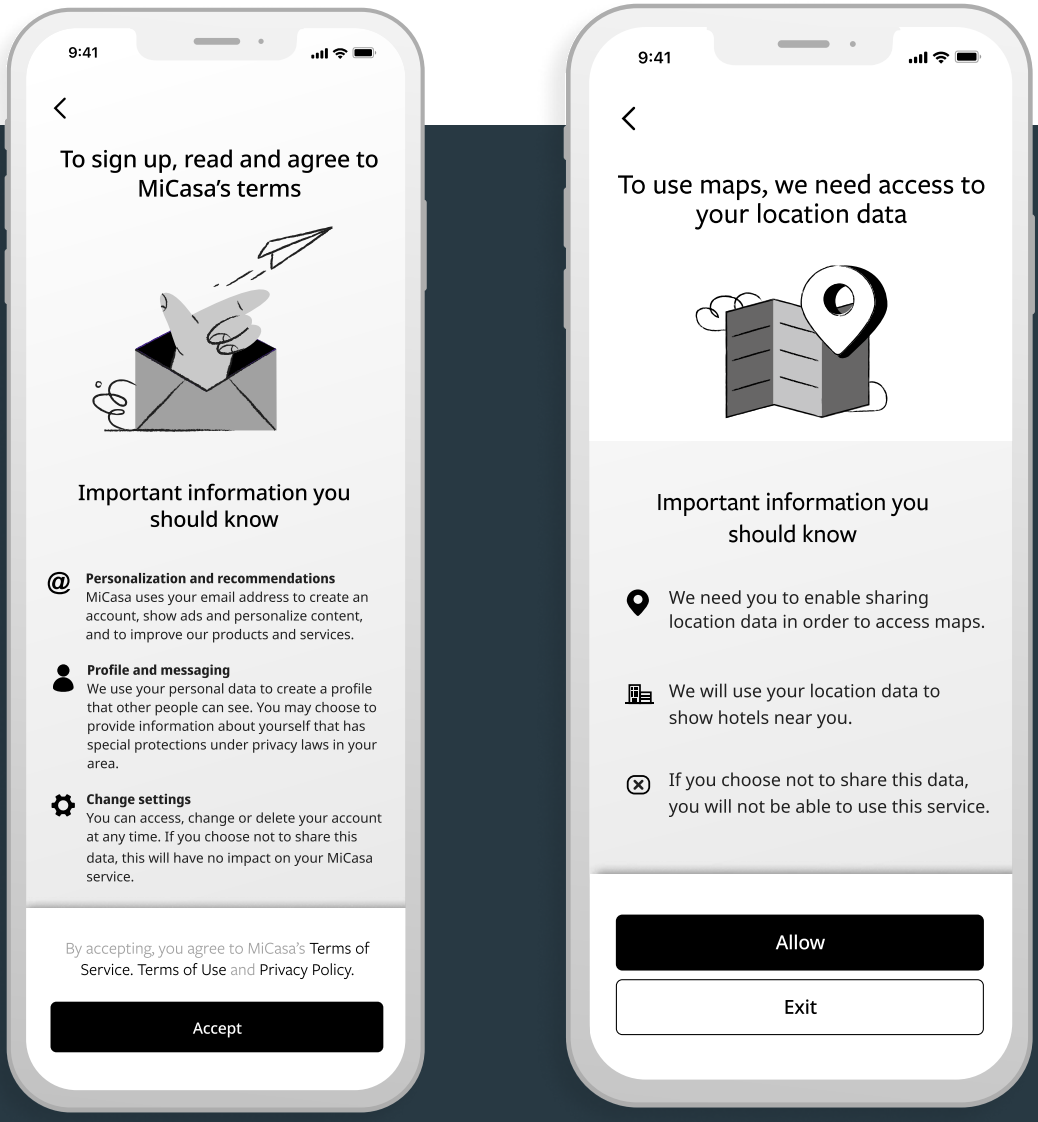
Total consent types are best used for **necessary data processing**. It's a "take it or leave it" moment that communicates to users that if they decline, they will not be able to use the service.

Product makers should:

→ Provide a clear notice about a data processing activity or group of activities.

→ Use a single button to capture consent: "agree / ok / accept / acknowledge" (or similar).

→ Consider using this during **onboarding** or after a **significant change**, and where data processing is necessary to provide the service.



CONSENT ARCHETYPES

Tiered Consent

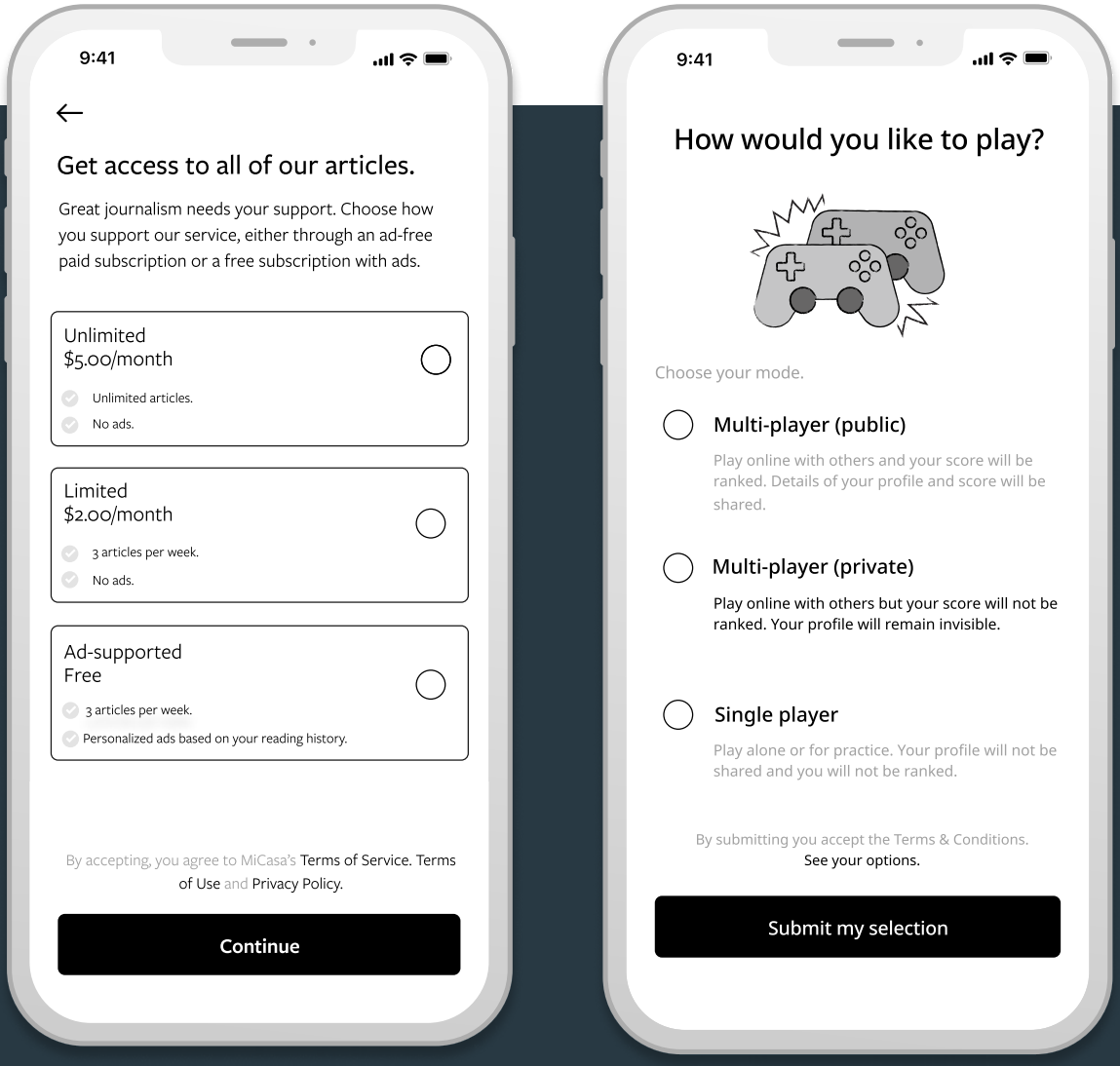
A tiered consent gives the user **high-level options**, so they can choose a service level. Each service level has preset data processing activities. For example, a user may have a choice between an ad-free and an ad-supported service.

Product makers should:

→ Describe processing activities based on the experience users get, for example “single player” or “ad-supported”.

→ Present all options in a tier equally, without indicating one is “preferred” or “recommended”.

→ Not pre-select one of the options, and allow users free choice.



CONSENT ARCHETYPES

Selective Consent

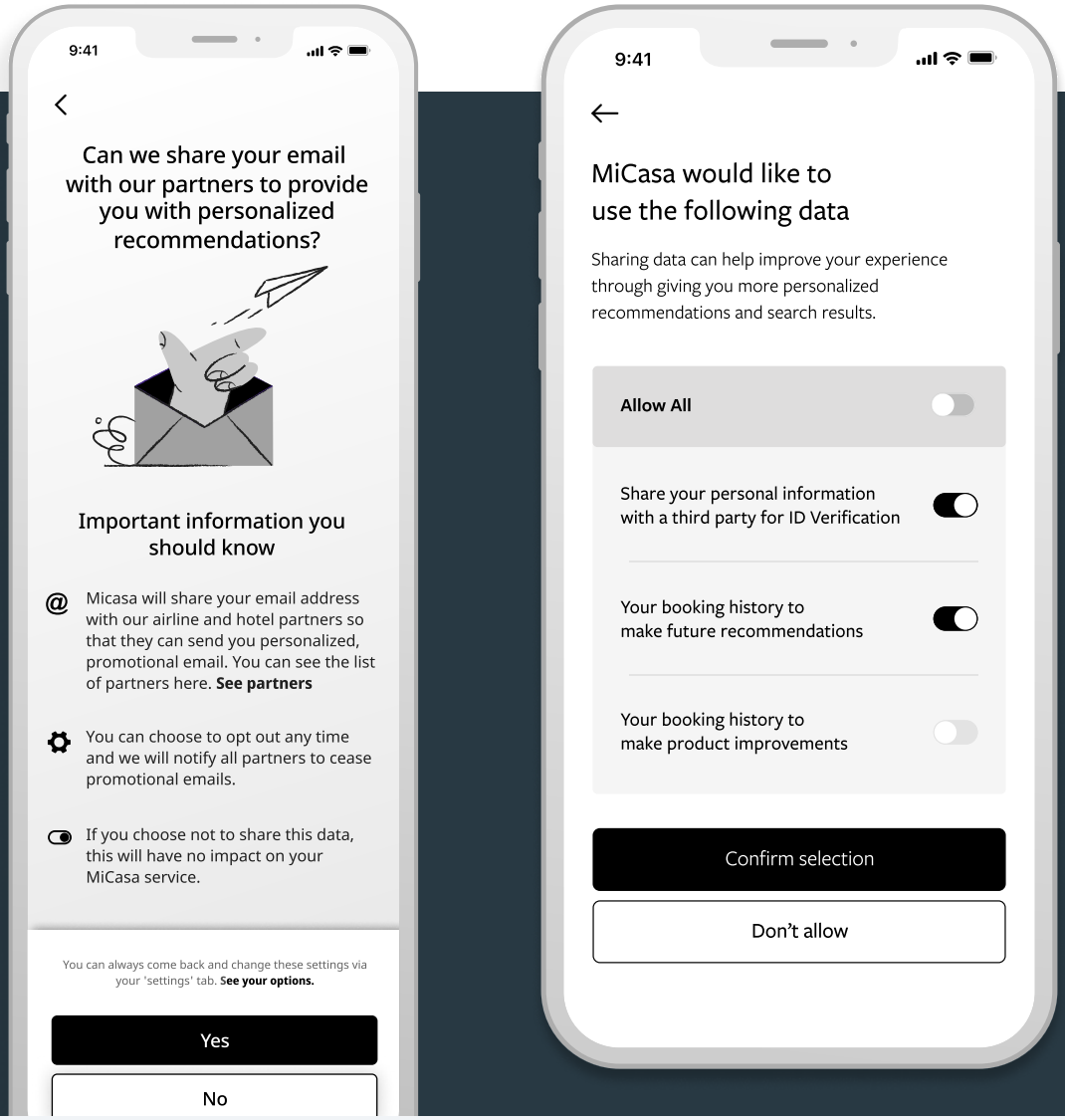
A selective consent captures consent through a pair of buttons with a **clear positive / negative option**. This consent gives users granular control, allowing them to opt out of certain data sharing while still using the service.

Product makers should:

→ Provide the ability to accept or decline individual processing purposes separately.

→ Make it clear how declining a consent will degrade a service or how accepting a consent will improve a service.

→ Use this to give granular choice for optional data processing activities which are not integral to the provision of the service.



Consent Design Best Practices

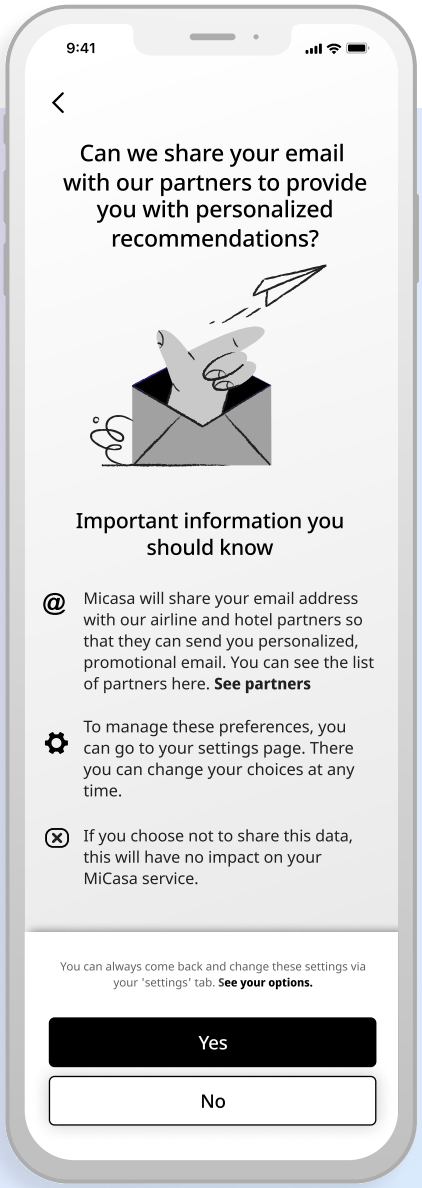
→ High-level guidance on consent moments with illustrative examples.

CONSENT BEST PRACTICE

Ensure accessibility

Best practice consent is **accessible** to the widest range of users. To achieve this, **product makers should**:

- → Account for different levels of literacy in both language and content design.
- → Limit complexity.
- → Express important information in a way that would be comprehensible to non-experts.
- → Design consent with people's context in mind.
- → Consider limits on people's time and screen space.
- → Ensure designs are aligned with widely established industry web and accessibility standards.



Clear headline
Directly states request and benefit for user.

Relevant image
Illustrates the data being shared.

Call to action (CTA)
Presents a simple choice.

Leverage design elements to support user understanding

GUIDANCE

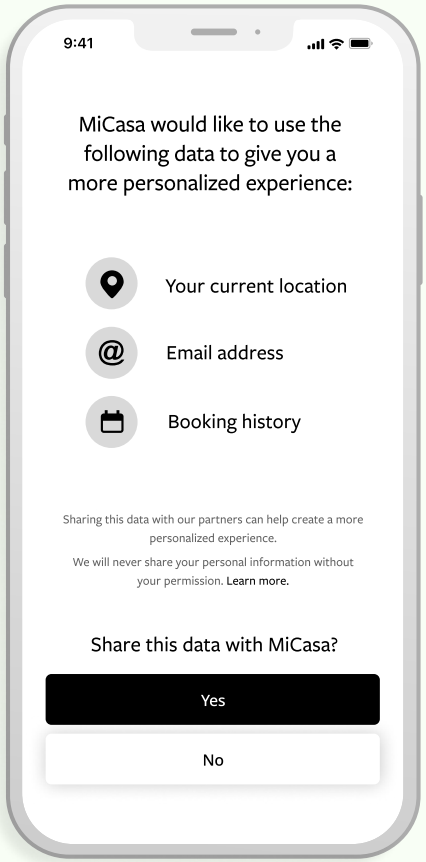
Product makers have a role in presenting dense information to users in **more accessible ways**. This may be through iconography, breaking text into digestible parts or reducing the amount of text wherever possible.

The example on the right demonstrates that more information is not always more transparent, and shows how visual elements can add more confusion when they are not used thoughtfully.

CONSIDERATIONS

- Clear questions reduce cognitive load and allow users to express their true preferences.
- They ensure product makers can be confident that users give informed consent.
- They can be formed either as an imperative statement (“Share your email to...”) or an interrogative question (“Can we use your email to...?”)

BEST PRACTICES



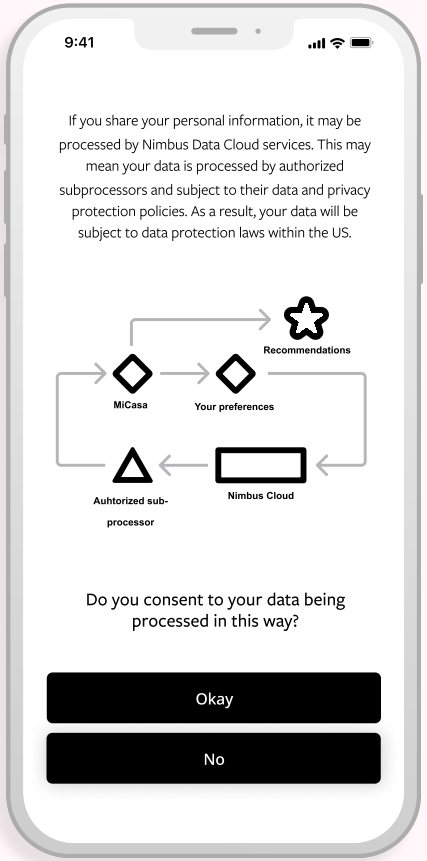
Clear headline
Headline is clear and easily scannable.

Easily recognisable icons
Icons support text to improve accessibility.

Detailed explanation available Option for interested users to get more detail.

Contrasting colors
Affirmative and negative in differentiated colors to help users navigate easily.

AVOID



Extreme detail
Unnecessary detail that increases cognitive load for users.

Confusing icons
Over-complicated explanation of processing activity.

Buttons same color
May make it harder to differentiate options.

Supporting commentary

How these principles have been applied around the world

Researchers in consumer psychology have identified that information overload is one of the main pitfalls when an individual is trying to make a decision. When faced with too much information, people are likely to adopt “simplifying rules” and discard or ignore a lot of the information available to them.[1] This is why providing more information can paradoxically undermine transparency.

Academics have argued that many privacy policies are “unreadable”, as they are written for those with a university level education and use industry-specific language.[2] Using simple sentences, plain language and design elements can lower the reading age of text.

Guidance from the UK’s ICO states that information in consent notices should be concise, easily accessible and use clear and plain language.[3]

1. Ram, N. (2008). “Tiered Consent And The Tyranny Of Choice.” University of Baltimore Law.

2. Kelley, P., Cesca, L., Bresee, J., Cranor, L. (2009). “Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach.” Carnegie Mellon University.

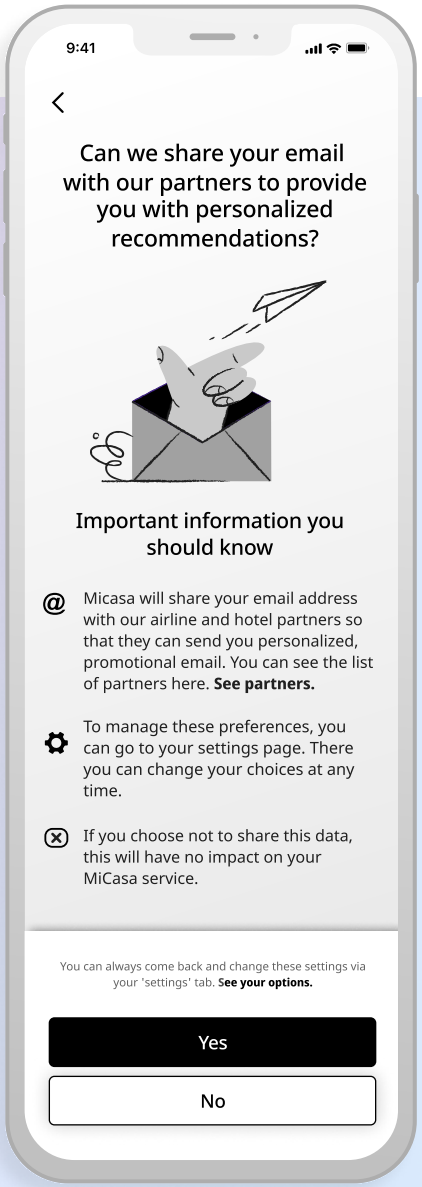
3. ICO. (2023). “Collecting Personal Data.” https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/collecting-personal-data/

CONSENT BEST PRACTICE

Make consent requests with clarity

Best practice consents are **clear and unambiguous**. When making a request, **product makers should:**

- → Ask for consent explicitly and prominently.
- → Use a question or statement to which a user can either agree or disagree.
- → State the relevant uses of data.
- → Communicate the potential upsides and downsides of giving consent.
- → Surface the most important information first and most prominently, ensuring that people who have little time have the best opportunity to engage.
- → Ensure the buttons or options on the page are a clear answer to the consent question asked on the screen.



Clear consent question
Explicit and prominent consent question.

Clear options
Users give a definitive answer.

Get a definitive consent answer from the user by presenting a clear consent question

GUIDANCE

Clear consent questions are **simple**, **short** and can be answered in a simple **affirmative or negative**.

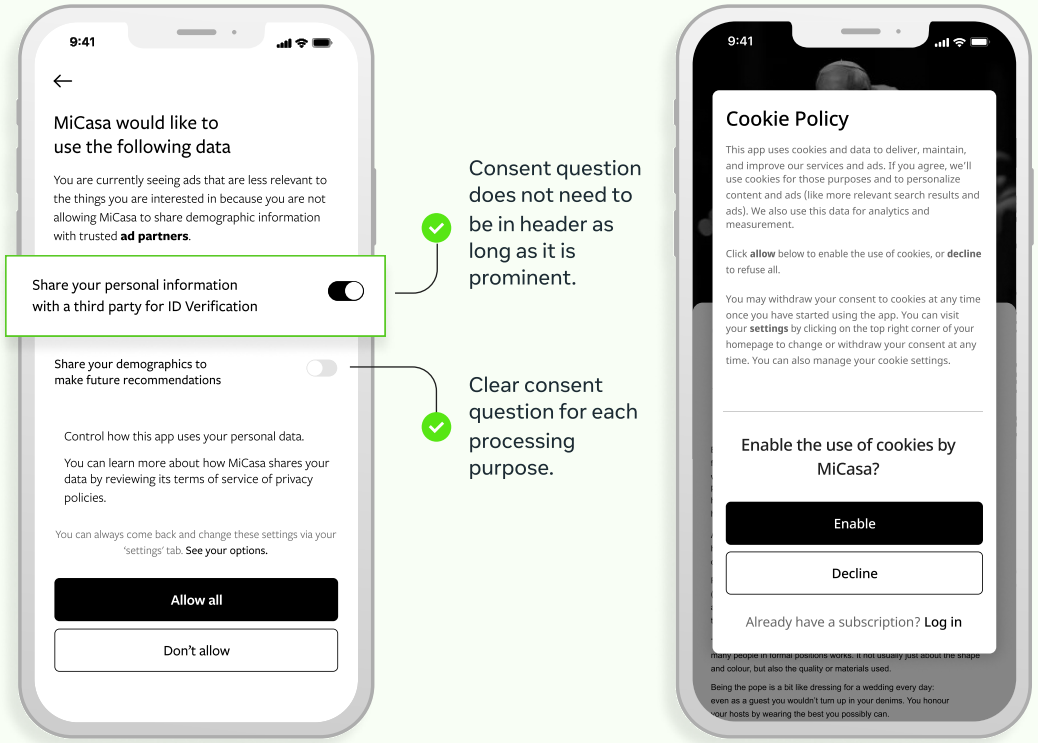
The placement of the question is not important, as long as it is **prominent**. The first two examples show relevant questions in different places, and either would be best practice.

Designers should avoid ambiguous questions, as in the example on the right. Here, the question does not specify the data processing activity or what a user gets from sharing data, and the buttons do not **directly answer the question**.

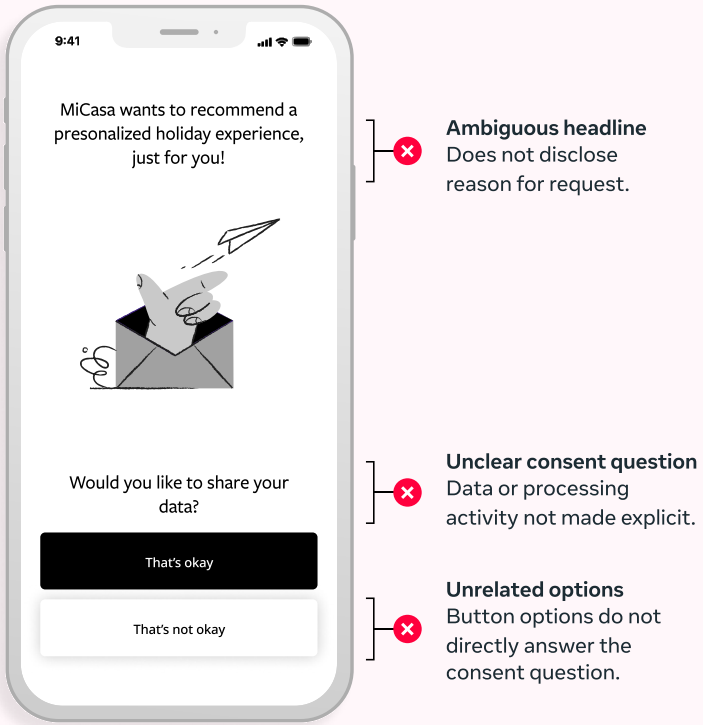
CONSIDERATIONS

- Clear questions reduce cognitive load and mean users are more likely to express their true preferences.
- Companies can get definitive positive consent from users.
- Clear consent questions can be formed either as an imperative statement or an interrogative question.

BEST PRACTICES



AVOID



Supporting commentary

How these principles have been applied around the world

In 2008, researchers analyzed common privacy policies and estimated the time it would take an average user to read them. They estimated that this time came at a cost of US $781 billion in lost hours.[1]

To reduce this load, researchers have stated that designers should use clear, short and relevant messages.[2]

1. McDonald, A. and Cranor, L. (2008). “The Cost of Reading Privacy Policies.” I/S: A Journal of Law and Policy for the Information Society.

2. Acquisti, A., et al., (2017). “Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online.” ACM Computing Surveys.

CONSENT BEST PRACTICE

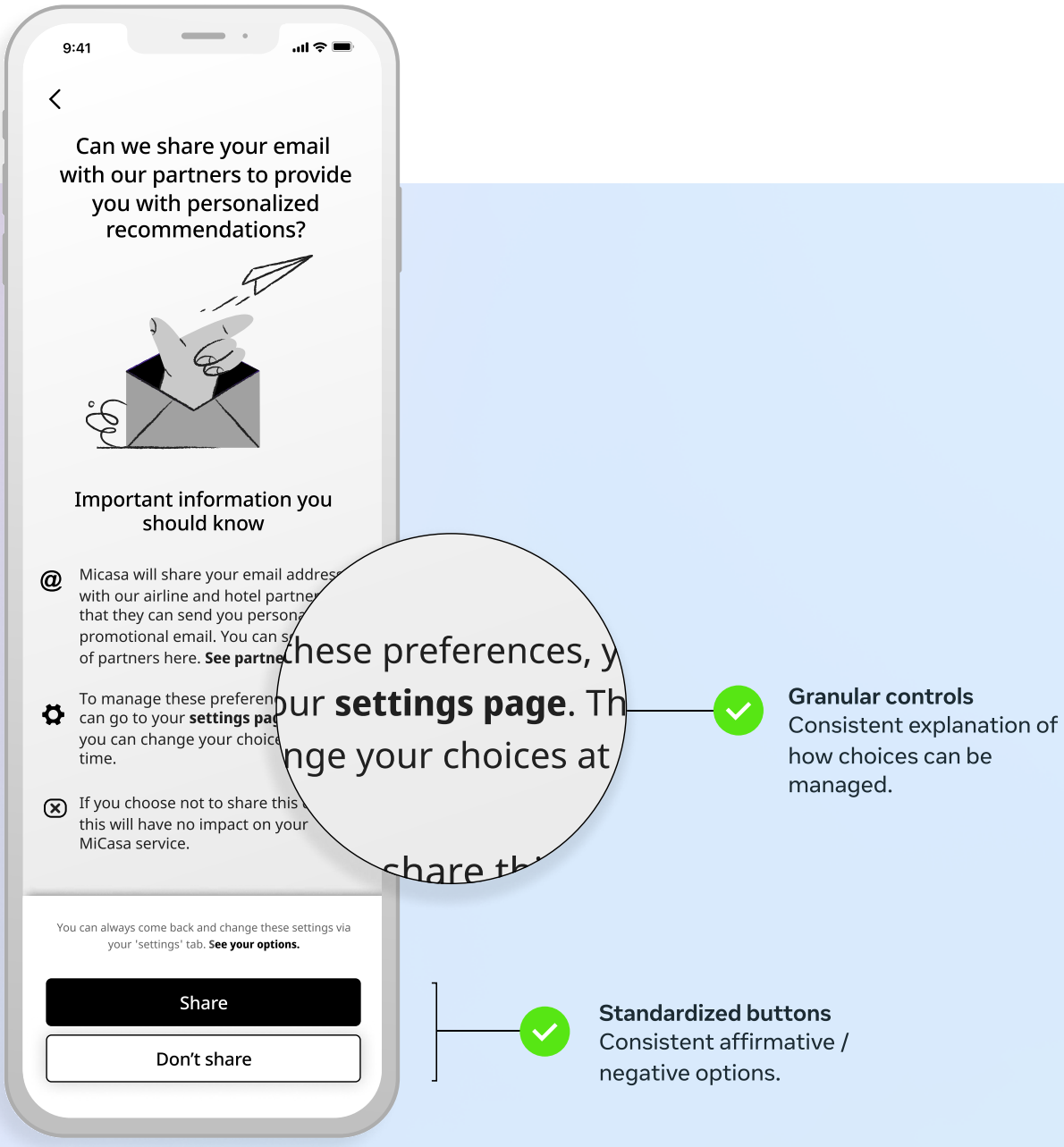
Be consistent

Best practice UX uses **consistent design language** and **standardized elements** to support better product experiences. This extends to consent moments, which should be consistent as much as possible.

Product makers should:

→ Use a consistent tone, language and visuals across consent moments.

→ Use consistent language to explain how privacy choices can be managed or revisited later.



Consistency throughout a user's relationship with a product creates more positive experiences

GUIDANCE

Research supports the idea that users will take cognitive short-cuts to simplify and essentialize complex information in consent moments. Designers should aim to support this process through consistency.

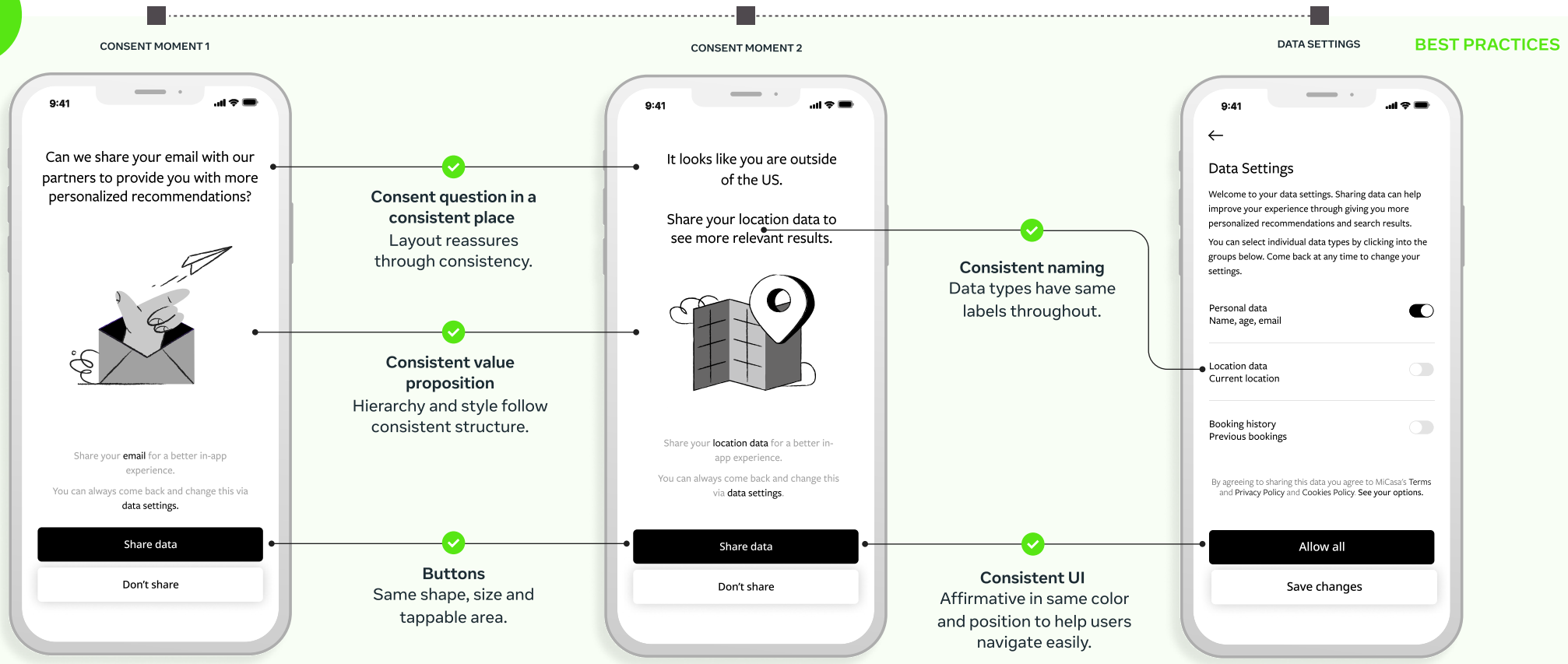
Avoid surprising users by keeping consent questions and buttons in **consistent placements**, keeping affirmative and negative options in the **same order and color**, and using **consistent iconography**.

These best practice examples show some of the main elements designers should consider in creating consistent experiences.

CONSIDERATIONS

- There is no single definitive UX that creates a universal positive experience
- Product makers should be empowered over the design of their products, aiming for internal consistency.

BEST PRACTICES



Inconsistency throughout an experience can be confusing and lead to misunderstanings

GUIDANCE

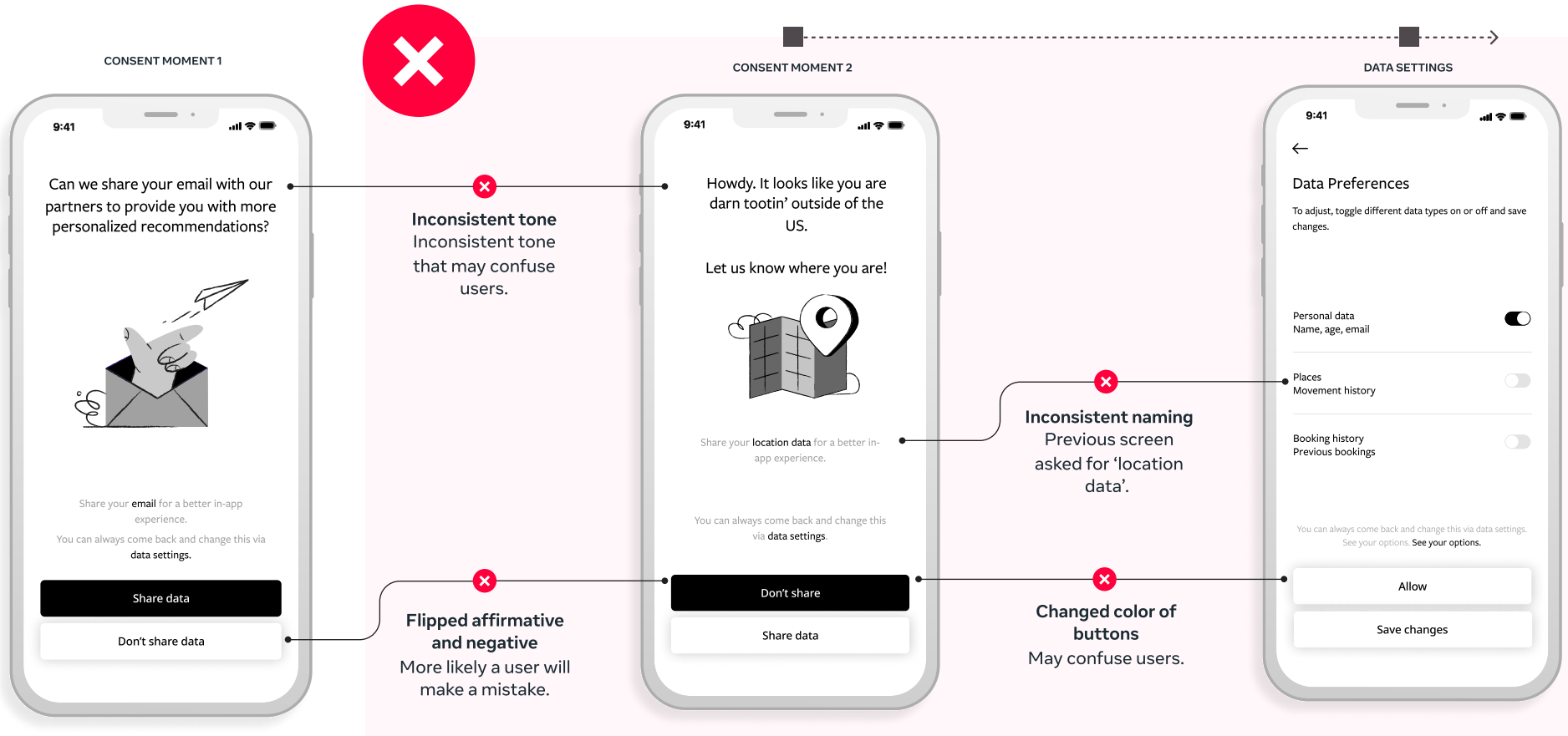
This flow shows an example of an inconsistent experience. These inconsistencies may not be a problem in isolation, but when part of a larger flow or experience may increase both **the cognitive load** and the **likelihood of users making mistakes**.

For example, in the second screen the **colors** for affirmative and negative have flipped. For a user trying to move quickly through the flow, this might cause them to mistakenly "accept" when they intended to decline consent.

Inconsistent language between screens makes it harder for users to understand what data processing activity they are consenting to.

CONSIDERATIONS

- Inconsistent design elements that can confuse users and lead them to make mistakes when trying to express their choice
- CTAs should be the same visual size, the same tappable area, and should be in close proximity.



Supporting commentary

How these principles have been applied around the world

The Australian Government's "Privacy Act Review: Report" noted that consistent wording, layouts and icons are an important way to reduce information overload. The Office of the Australian Information Commissioner (OAIC) is even considering creating guidance on standardized consents. In their submission to this report, the Castan Centre for Human Rights Law (Monash University) said standardization was a "promising mechanism" when trying to combat consent complexity.[1]

1. Attorney-General's Department, Australian Government (2022). "Privacy Act Review: Report 2022", at 106.

CONSENT BEST PRACTICE

Be fair

Best practice consent presents the request and relevant information **fairly**.

This does not mean **perfect neutrality**. In fact, when product makers explain their intent and what value users can expect to get from data processing, it helps people make informed decisions.

Best practices

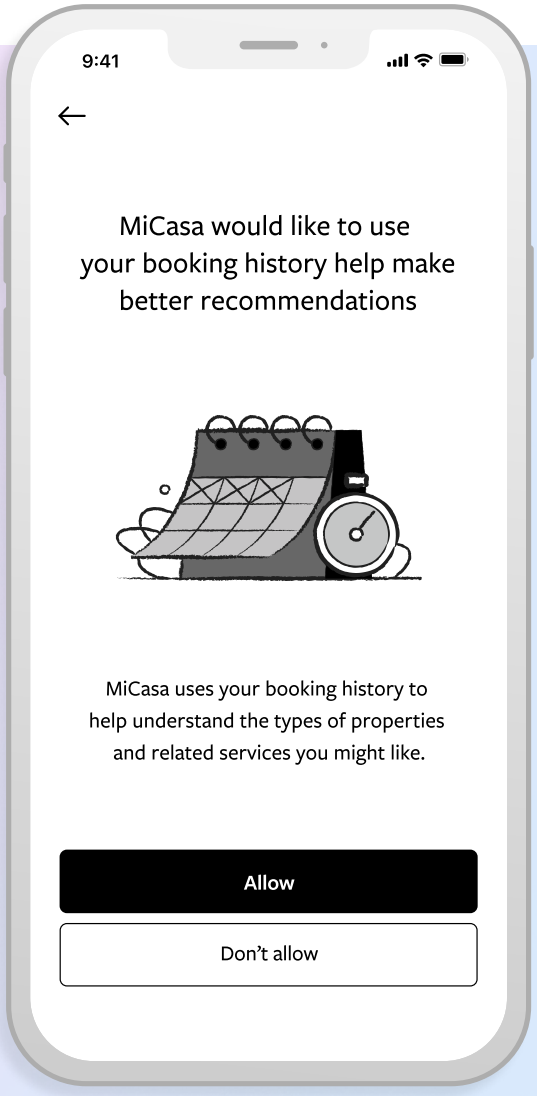
→ Describe benefits and outcomes fairly.

→ Present balanced options.

To be avoided

→ Use intentionally misleading or coercive language.

→ Deploy unnecessary confirmations or other types of friction that favor consenting over declining or dismissing.



Prominent consent question
Explicit and prominent consent question.

Description of benefits
Body copy clearly describing the intent of data processing and the value for users

Use consent moments to communicate the value being created

GUIDANCE

Letting a user know what **value they get** from their data being processed can lead to better product experiences. Communicating value ensures users know why they are sharing data in terms they can easily understand, through the lens of the benefit or service they get.

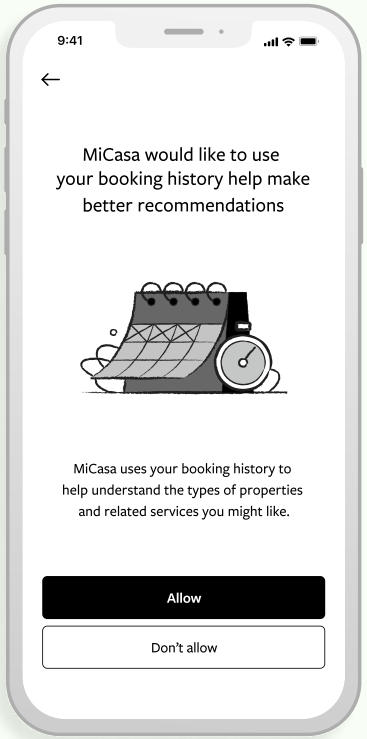
Product makers should aim to **express value clearly and simply**, stating how the data will be used and what **benefit** there may be for the user.

As the second example shows, over-promising, ambiguity and falsely instilling panic take this too far and would be considered **unfair** or **deceptive** design practices.

CONSIDERATIONS

- Neutrality doesn't lead to better privacy outcomes.
- Conveying value does not necessarily mean something is a deceptive design.
- Being fair and clear avoids overpromising or potentially misleading people.

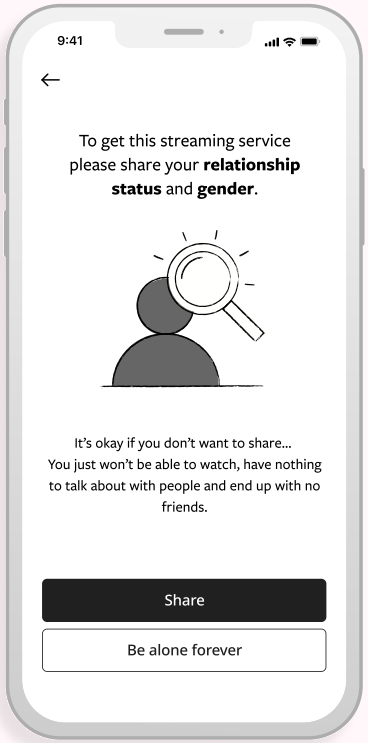
BEST PRACTICES



Value explained clearly
Explains the value a user might get from sharing data.

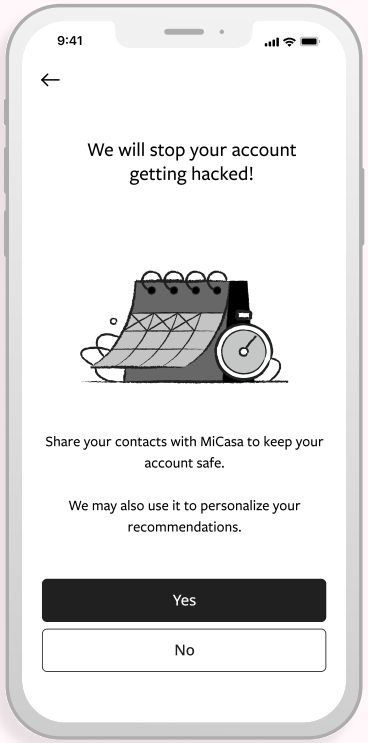
Clear body copy
Clearly and simply outlines how the data will be used.

AVOID



Unclear value proposition
Data request does not have a clear connection to the service.

Emotional steering
Phrase creates a sense of shame or fear.



Overpromising headline
Falsely implies sharing data can protect account.

Misleading copy
Falsely implies data is needed for security.

Supporting commentary

How these principles have been applied around the world

In the UK, the ICO has taken the view that it is possible to incentivize consent to some extent. It's okay for there to be a benefit to consenting to processing. For example, discounts for joining a loyalty program would not necessarily be deceptive. However, product makers must be careful not to cross the line or unfairly penalize those who refuse consent.[1]

In many jurisdictions, such as the EU and Australia, laws state that data processing practices should be "fair".[2]

Under Canadian privacy law, there is also scope for the Canadian Privacy Commissioner to publish more detailed guidance on what they consider to be inappropriate data practices.[3] They create this guidance through consultation with industry and policy stakeholders, helping ensure the legislation meaningfully reflects community standards and expectations.[4]

1. ICO (UK), (2022). "Lawful, fair and transparent processing". Online. Accessed 18 December 2023.
2. Privacy Act 1988 (Cth), APP 3.5: "an APP entity must solicit and collect personal information only by lawful and fair means."
3. Office of the Privacy Commissioner of Canada, "Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)", Online. Accessed 18 December 2023. See also: PIPEDA subsection 5(3): "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."
4. See, for e.g., Office of the Privacy Commissioner of Canada, "A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act", Online. Accessed 18 December 2023.

CONSENT BEST PRACTICE

Group thoughtfully

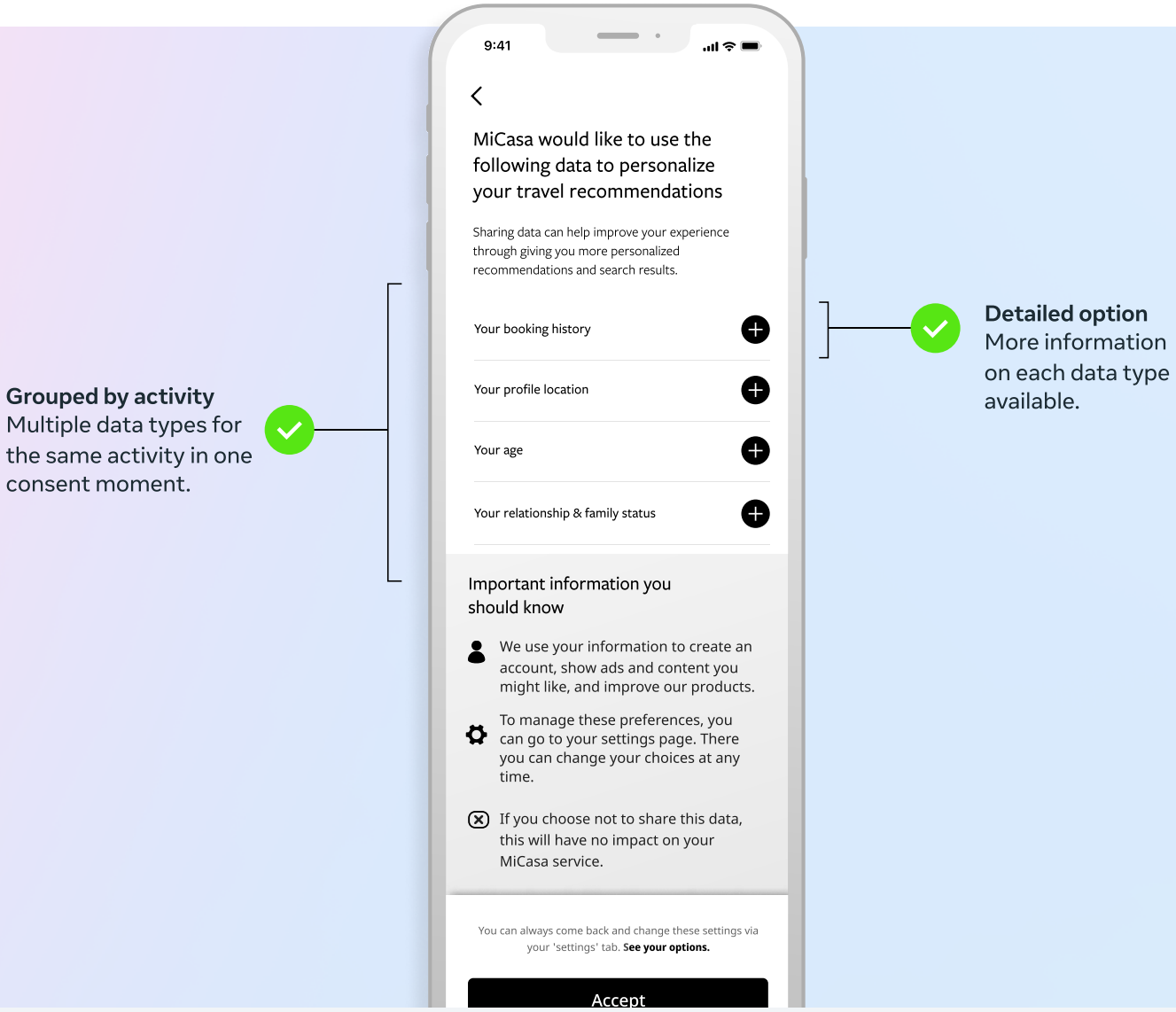
Best practice consent involves **grouping consents** to reduce friction, avoid consent fatigue and provide better user experiences. Too many separate consent moments may **undermine user control**.

Product makers should:

→ Group consents in ways that make sense to people and are aligned with their natural mental models, e.g. when multiple data types are required for the same data processing activity.

→ Group only when user control will be increased, not to obfuscate important information. Be especially mindful to be explicit on requests for sensitive data.

→ Keep consents separate when the purposes are sufficiently distinct requests.



Group necessary activities under one Total Consent

GUIDANCE

For **necessary** data processing activites - that is, processing that needs to happen to provide the service - best practice is grouping them together.

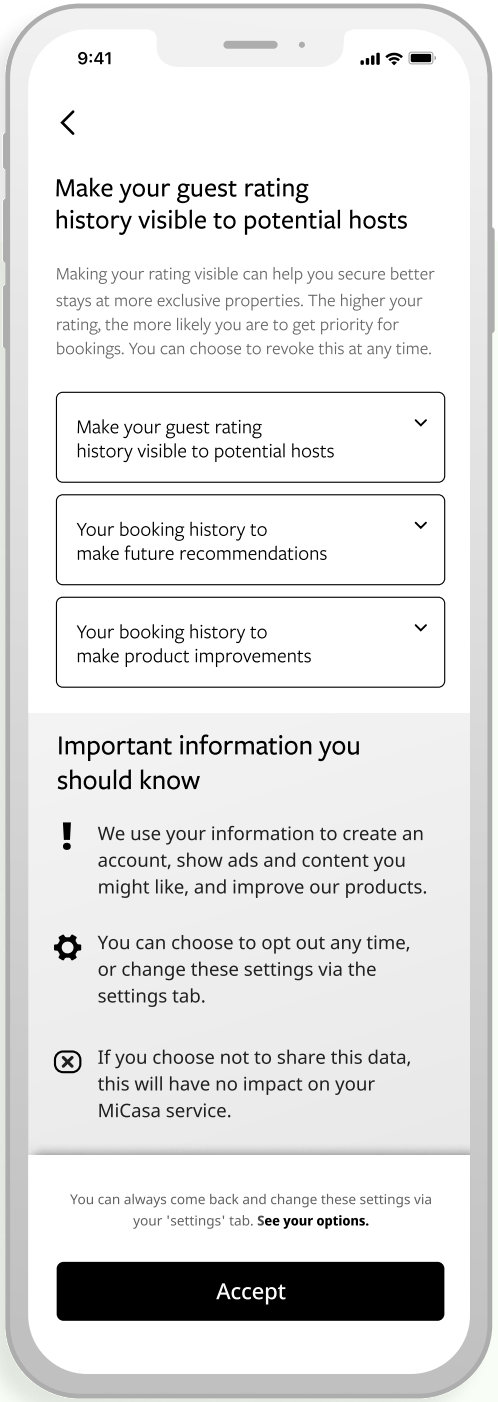
This means a user only needs to consent to **one screen** in order to access the service, while giving them an option to learn more if they want.

CONSIDERATIONS

- Removing unnecessary friction reduces confusion and consent fatigue, promoting more informed decision-making.
- This approach improves people's experience without obfuscating important information.
- Grouping necessary data types and processing activities supports better privacy outcomes.

BEST PRACTICES

Grouped by activity
Multiple data types for the same activity in one consent moment.



TOTAL CONSENT

Mandatory consent
Data is needed to provide access to the service.

Group multiple data types for the same activity

GUIDANCE

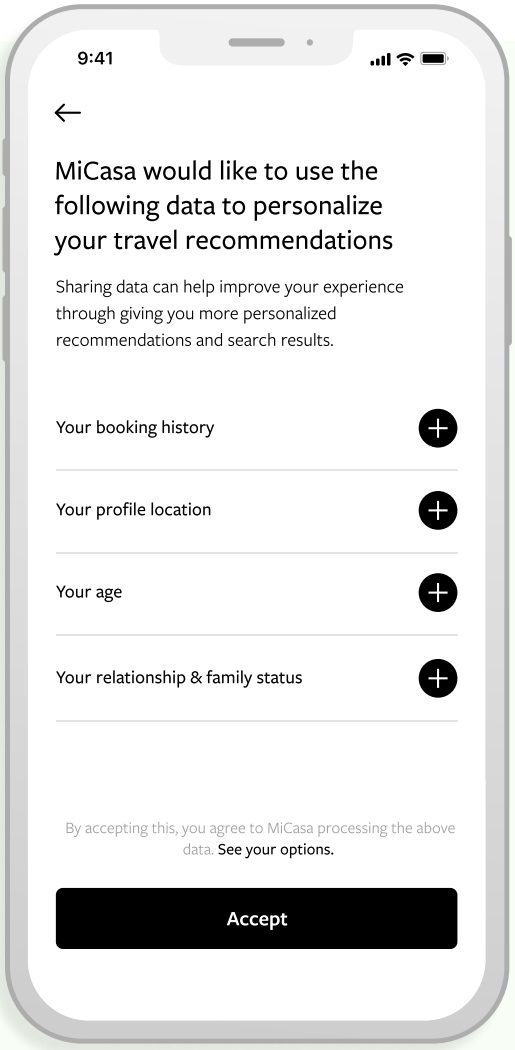
Grouping **multiple data types** can help support user understanding, and prevent information overload.

Considering how to best group consents in ways that make sense to people reduces overload, and can lead to more informed privacy decisions.

CONSIDERATIONS

- Reducing friction increases engagement and prevents consent fatigue.
- Access to further information on each request meets people's privacy expectations.
- Unexpected or random groupings that bury a data request erode user trust.

BEST PRACTICES



Grouped by activity
Multiple data types for the same activity in one consent moment.

Option for more detail
More information on each data type available.

TOTAL CONSENT

Group optional activities with “allow all” to improve user experience

GUIDANCE

Where data processing activities are **optional** - that is, the user can access the service even if they don’t share the data - best practice is giving an **allow all** option.

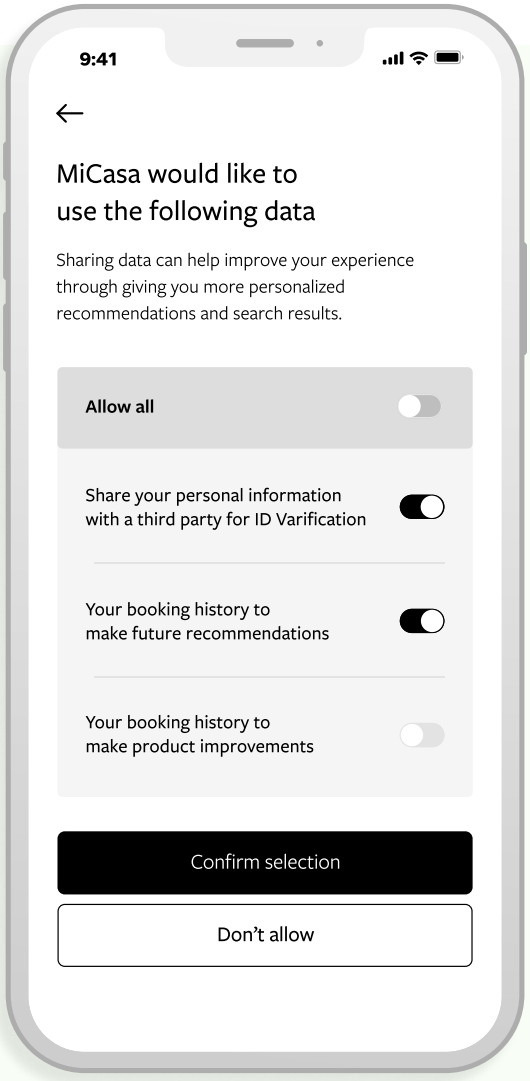
This means users can easily accept or decline different data processing activities if they choose.

CONSIDERATIONS

- Allow all can sit alongside more granular controls.
- Providing granular choices ensures people retain control of the data they share.
- Providing an allow all option can reduce consent fatigue.

BEST PRACTICES

Allow all
Option to confirm multiple consent requests at once.



Granular data controls
Individual toggles for each request for users who want more granularity.

SELECTIVE CONSENT

Separate consents can overwhelm and confuse people

GUIDANCE

When faced with **information overload**, users are more likely to disengage, not make a choice, or make a choice just to move through things more quickly. This undermines the goal of consent moments.

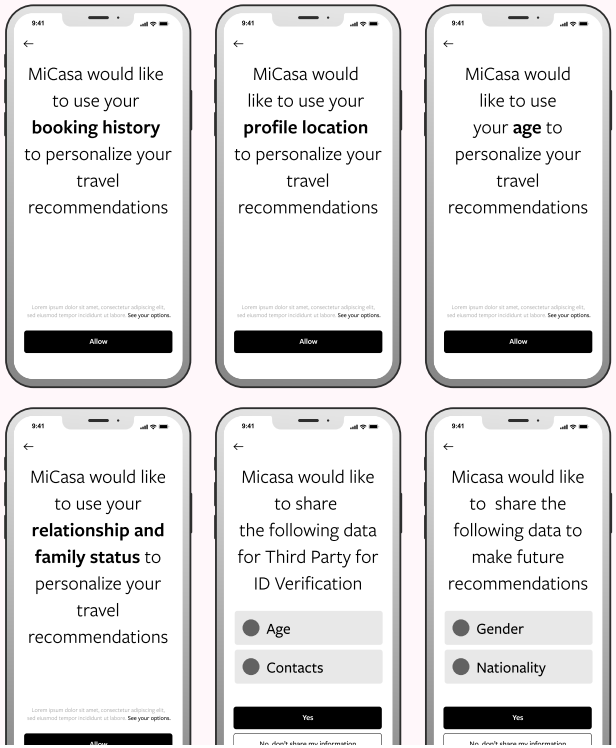
On the left is a sample user experience where every consent is requested separately and individually, resulting in disengagement, fatigue and attrition.

On the right is a **thoughtful grouping** of consents. Multiple data types are grouped for a single purpose in a Total Consent design. Multiple optional consents are grouped into a Selective Consent design, which allows for granular control.

CONSIDERATIONS

- Grouping consents can support more understandable consent moments.
- Reducing the number of individual notifications helps reduce consent fatigue.

AVOID

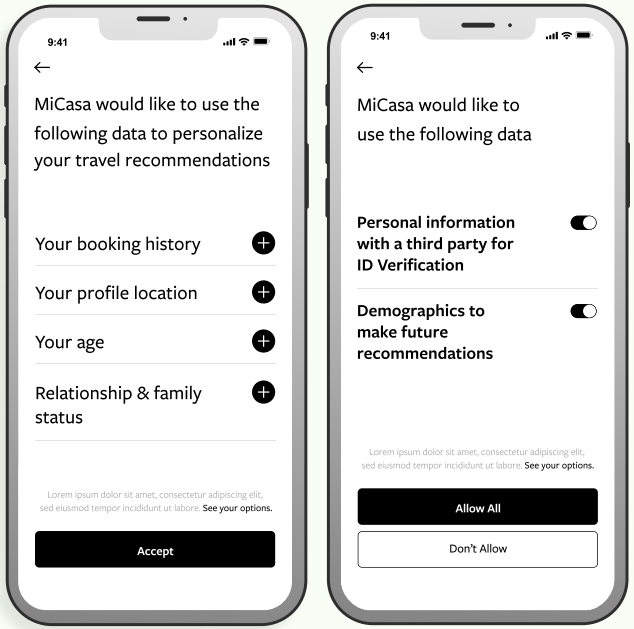


x6 Separate Consents

1 minute

- Increased user fatigue
- Lower engagement
- Higher drop-off rate
- Poorer privacy outcomes

BEST PRACTICES



x2 Grouped Consents

20 seconds

- Improved user experience
- Increased engagement
- Maintains user control
- Better privacy outcomes

Supporting commentary

How these principles have been applied around the world

Research into consent and consumer psychology has shown that when an individual faces information overload, they are likely to simplify the decision-making process.[1] They may do this by:

- Discarding or ignoring a great deal of information
- Forming simple heuristics
- Focusing on a manageable subset (or essentializing).

This is why techniques to reduce the cognitive load or simplify information can actually promote transparency. Usability research aims to overcome complexity through interfaces that give manageable and easy-to-understand options.[2]

Some researchers have advocated for "soft paternalistic" approaches that reframe choices in a way that makes it more likely users will make selections that benefit them.[3] This has also been referred to as "nudging". A nudge will encourage someone towards a choice, but will never restrict other choices.[4]

1. Ram, N. (2008). "Tiered Consent And The Tyranny Of Choice." University of Baltimore Law.

2. Acquisti, A., Et al., (2017). "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online." ACM Computing Surveys.

3. As above.

4. Verena Zimmerman. (2023). "Nudges and Informed Consent? Challenges for Privacy Nudge Design", Human Factors in Privacy Research.

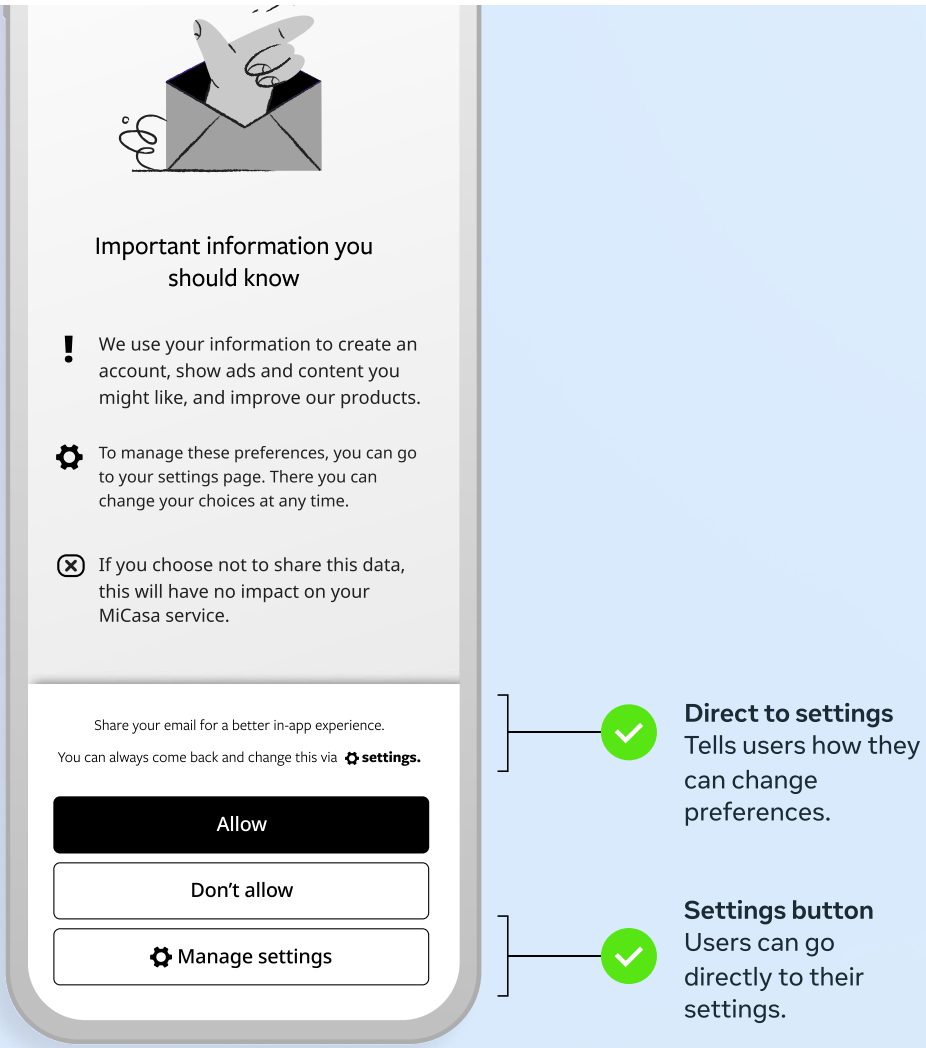
CONSENT BEST PRACTICE

Let people change their minds

Best practice consent involves letting people **change their minds,** rescind the consent or modify their settings.

Product makers should:

- → Let people know how a consent decision can be revisited while the request is being made.
- → Periodically remind people of the choices they have made and how those choices can be reviewed and revisited.
- → When a user is trying to access a feature that requires data processing they have previously declined, or when their actions don't align with their privacy settings, re-prompt them with a consent decision.
- → Proactively prompt users to review a previous choice when they believe the user might want to revisit that choice.



Present a consent moment again when users signal a change of mind

GUIDANCE

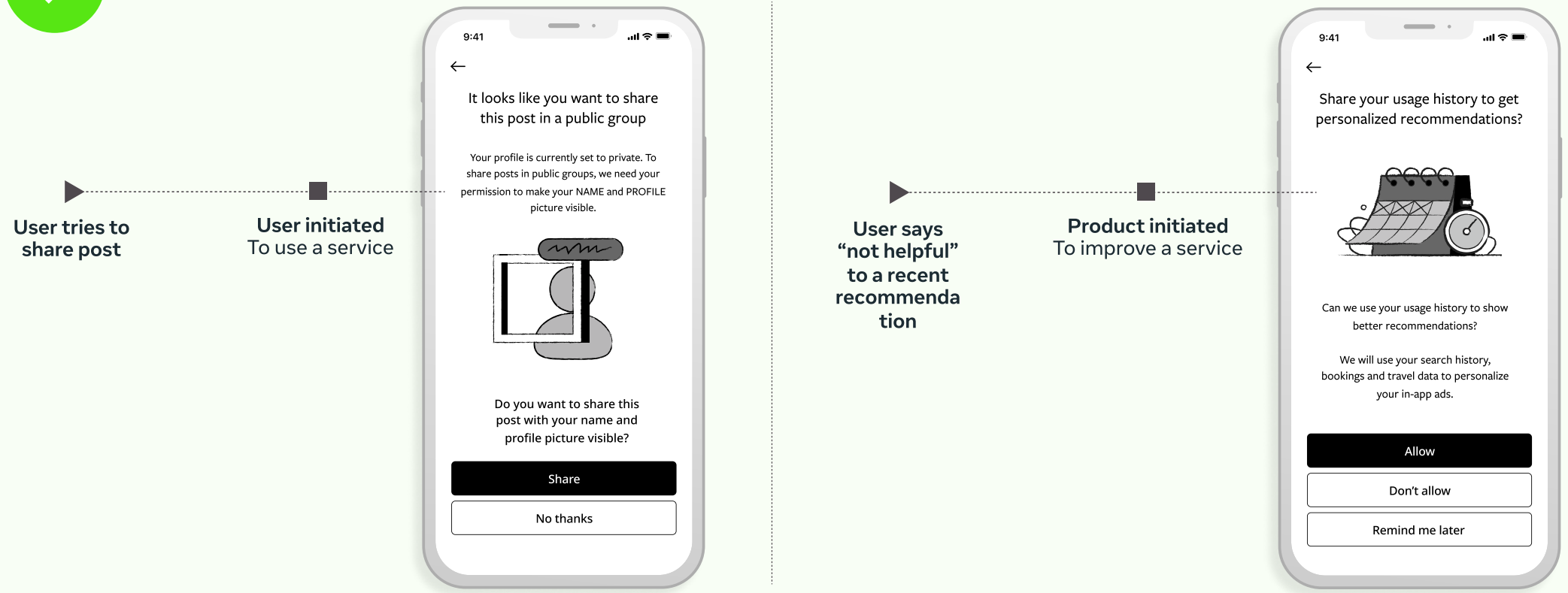
When a user's **actions** don't align with their privacy settings, product makers should re-prompt them with a consent decision.

User initiated is when a user is trying to access a service or feature, which needs a consent that they have previously declined. For example, they may try to share a photo, prompting an app to ask for permission to access their camera.

Product initiated is when a company seeks to get consent for a data processing activity, often to improve a service. For example, when an app asks for search history to improve search results.

CONSIDERATIONS

- Respect people's privacy decisions by limiting company-initiated asks.
- Company-initiated triggers are appropriate in some cases when based on a user's actions.



Before a user revokes consent, share the consequences in a fair and balanced way

GUIDANCE

When a user changes their mind and **revokes consent**, product makers should let them know of any consequences or **irreversible outcomes**.

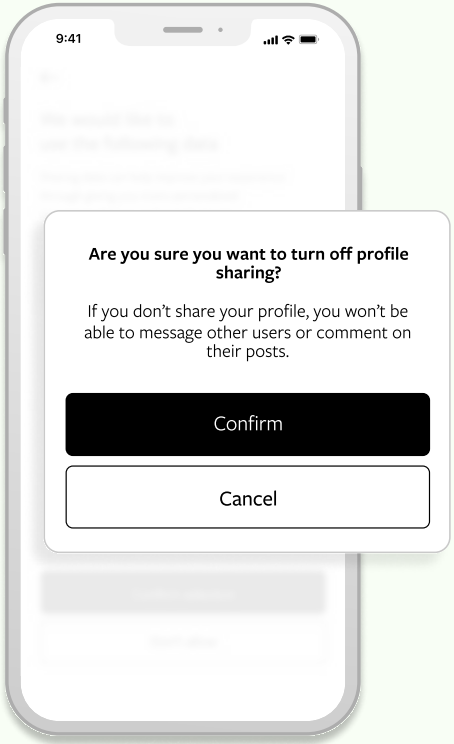
This should be expressed clearly, and state the outcome in a way that sets a user's expectations, without discouraging them from revoking consent.

As the second example shows, using **overly emotional language** or emotional steering can cross the line and be considered manipulative.

CONSIDERATIONS

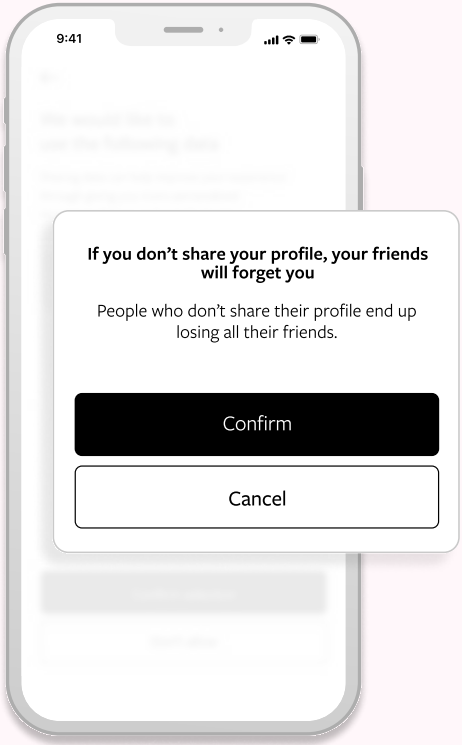
- Ensure people understand the consequence of revoking a consent, especially if it leads to deactivation or data being permanently deleted.
- Express these consequences in a fair and balanced way.
- Use manipulative language to overstate the consequences of revoking consent.

BEST PRACTICES



Realistic consequences
Describe realistic or factual consequences, or implications for their experience of the product.

AVOID



Emotional or manipulative claims
Speculative or extreme emotion-based warnings that manipulate a user into data sharing.

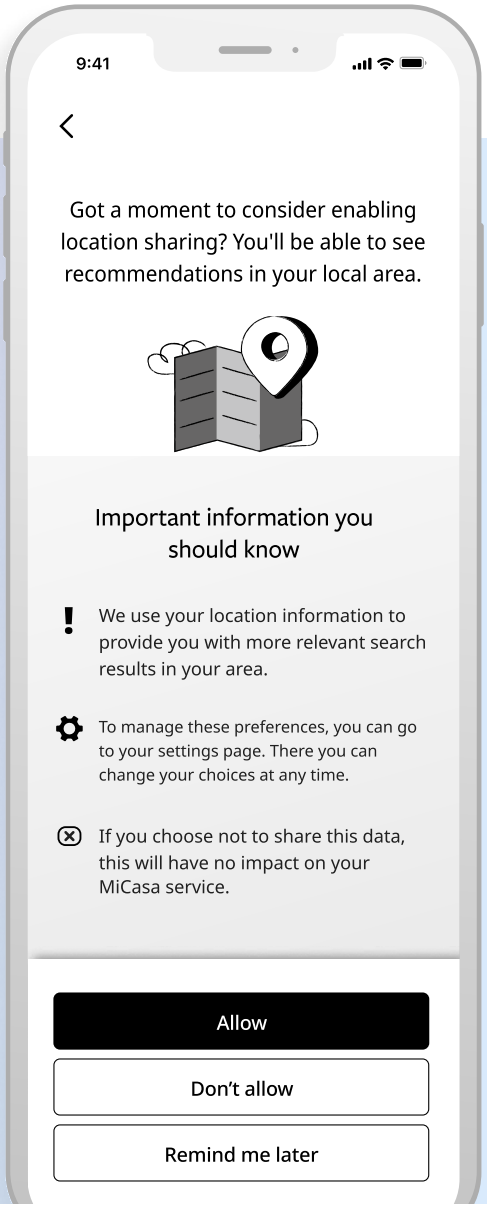
CONSENT BEST PRACTICE

Be selective to support a user journey

Best practice consent is selective about the **right time** to deliver a consent moment. Good timing means not rushing the user to a decision, and avoids over-taxing them with frequent requests.

Product makers should:

- → Consider whether to ask for consent **upfront** (during onboarding) or **in context** (when a user accesses a relevant feature).
- → Leverage dismissibility (or "remind me later") so as not to rush a decision.
- → Limit the frequency of consent requests and space them out at thoughtful intervals.
- → Limit the total number of consent requests for a processing activity or data sharing.



Right time
Lets user know why they might consent at this time.

Option for reminder
User can choose a time that suits them.

Reminders for optional consents over time are helpful, not nagging

- People make more informed decisions if they can delay their response to a consent request, until they have time to make a considered choice.
- Providing reminders at reasonable intervals avoids “forced timing” and artificial urgency.

Over multiple days

Day 1

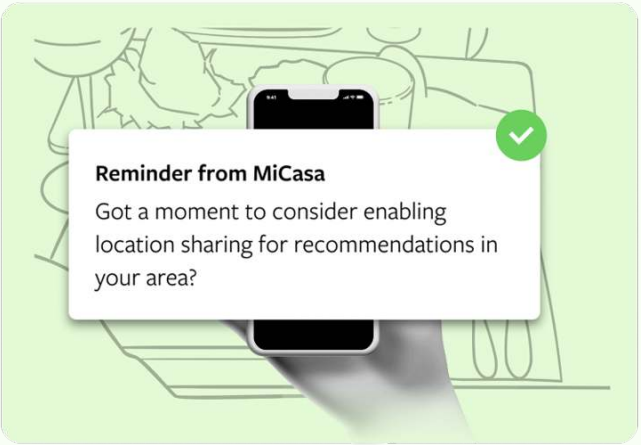
Request 1
In-context notification

The user receives a consent request, but their bus has just arrived so they hit “remind me later”.

Day 2

Request 2
Push notification

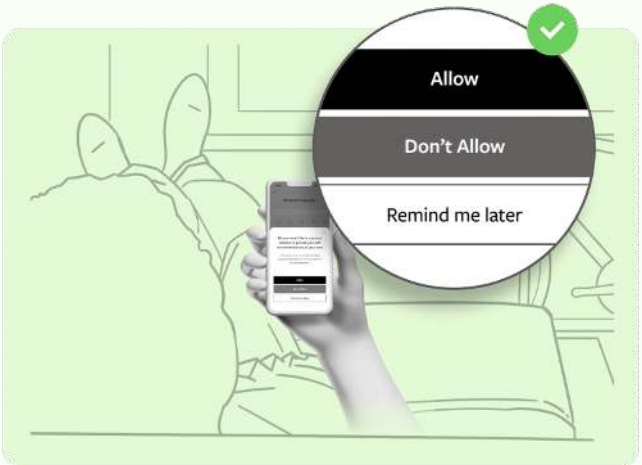
The next day, they receive a reminder, but they're out to dinner so they don't respond.



Day 4

Request 3
In-app reminder

Two days later, the app asks them again. They now have the time to make an informed decision to allow or deny the request.



Don’t nag users with repeat requests within a short period

Multiple requests made in a single session, a single product experience or one sign up flow goes beyond helpful reminders and **risks nagging**.

Provide reminders for optional consents over a longer period for a more positive user experience.

1 day — Request 1

2 days — Request 2

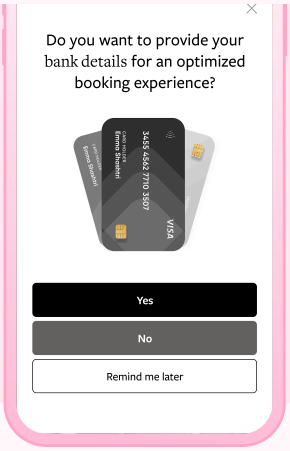
4 days — Request 3

Over a single session

1 min

Request 1
In-context notification

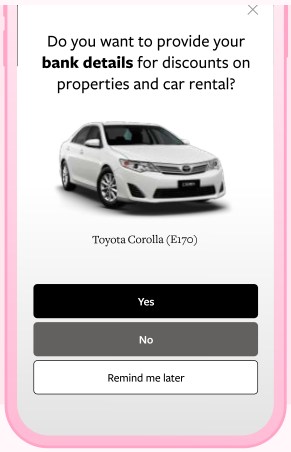
User receives a request to provide their bank details during sign-up.



2 min

Request 2
Repeat notification

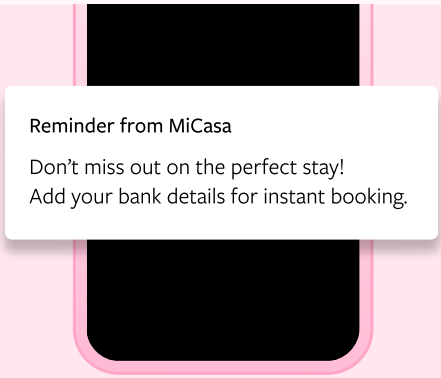
Despite deferring their decision, they receive a second request in the same onboarding flow.



3 min

Request 3
Push notification

They then receive a third request before they finish sign-up.



When a consent is necessary, forced timing is called for

GUIDANCE

When a consent is **necessary** - that is, a user will need to consent to use a service - **forced timing** is a positive user experience. It communicates the fact that consent is not optional for this service.

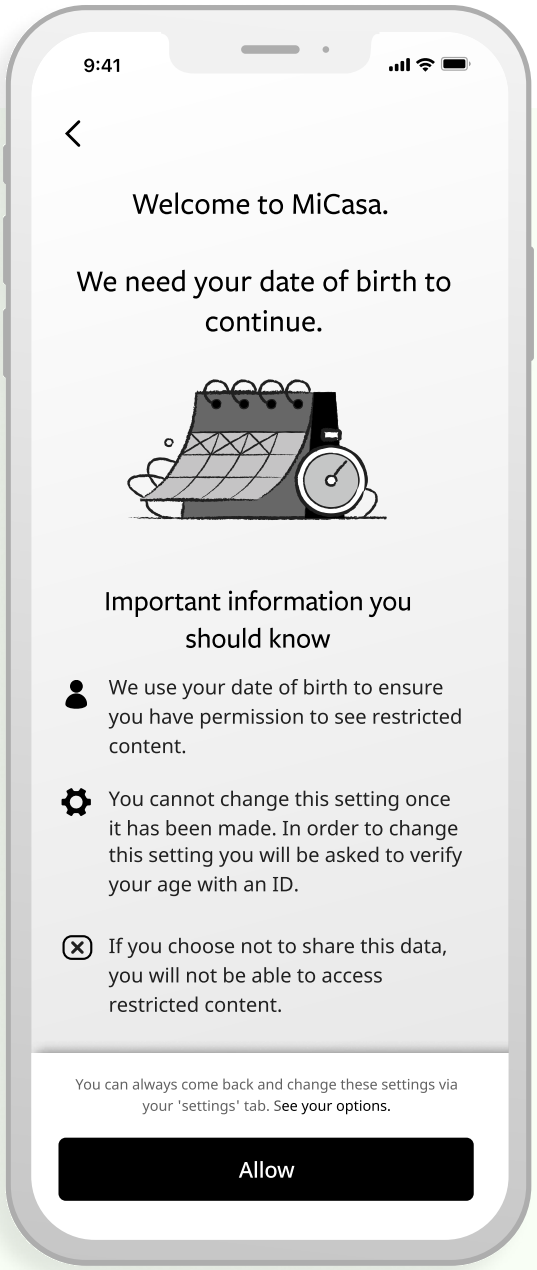
Conversely, allowing a user to delay a necessary consent may **confuse or cause annoyance**, requiring them to revisit the consent to use the app or product.

CONSIDERATIONS

- Determine when a consent request is necessary.
- Be explicit about the reason for collecting data at this moment.
- Over-using forced choices in a product or flow.

BEST PRACTICES

Necessary data
Lets users know they need to share now to access the service.



Clear explanation
Short and clear explanation of why data is needed now.

Forced timing
No option to dismiss.

Supporting commentary

How these principles have been applied around the world

Nagging is a dark pattern that is defined by repetition or "persistence that... can ultimately wear down the consumer into the desired action."[1] It is different to other dark patterns in that it does not rely on deception. Some commentators have noted that this lack of deception means it sits outside of the usual paradigm regulators use for thinking about consumer harms related to consent.[2]

There is no clear-cut line between nagging that causes harm and a helpful nudge. Some commentators have said a distinction is whether the ask is for something that benefits the user, or is just something the company would prefer.[3]

For example, repeatedly asking a user to update software that fixes a security issue is unlikely to be considered a dark pattern. However, repeatedly asking a user to turn on push notifications (something the company would prefer they do), may be considered nagging.

This will depend heavily on context. As Alison Hung writes,"the distinction between a nag and a nudge is an unstable, dynamic one: what might be an annoying nag to some might be a helpful nudge to others."[4]

1. Alison Hung. (2021). "Notes: Keeping Consumers in the Dark: Addressing 'Nagging' Concerns and Injury', Columbia Law Review.

2. Tim Wu. (2017). "Blind Spot: The Attention Economy and the Law", 82 Antitrust LJ 771, at p. 778 : "Regulators . . . don't have a paradigm for thinking about consumer harms that are not deceptive or involve physical or financial harm, but rather arise from the seizure of attention and consequential cognitive impairments."

3. Alison Hung. (2021). "Notes: Keeping Consumers in the Dark: Addressing 'Nagging' Concerns and Injury', Columbia Law Review.

4. As above.