Trust, Transparency and Control Labs

Published July 2024

Assessing the Success of Privacy Education Products

Meta

Summary

Product makers implement a wide variety of privacy education tools in their apps to inform users about data practices and empower them to make informed privacy choices. They are generally understood to be helpful, but measuring the effectiveness of privacy education can be challenging.

In this report, we explain the challenges with assessing the success of privacy education products and share Meta’s approach to measuring effectiveness through case studies on Instagram’s location data transparency feature and Meta’s Privacy Policy updates.

At Meta, our approach involves defining specific, contextual success criteria for each privacy education experience, designing with these outcomes in mind, and using fit-for-purpose methods such as feedback surveys to ensure those goals are met.

Introduction

> **Technology companies provide users with a variety of privacy controls and settings. Product makers deploy these tools in their apps in the hope that they can improve user experiences, but measuring the effectiveness of privacy education can be difficult. In this report, we share Meta's approach to measuring the effectiveness of privacy education. Our goal is to help product makers understand the approaches to measuring success, and the inherent trade-offs and blind spots in any such effort.**

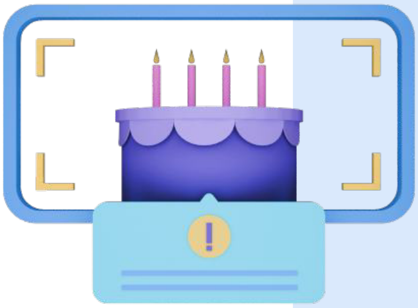
At Meta we design privacy controls to provide users with a choice over how we collect, use and disclose their personal information on our apps. There are tensions when designing privacy and data control experiences. On the one hand, it is important for users to be able to understand these settings in order to build confidence in managing their privacy and having an overall positive experience online. On the other hand, privacy is highly personal and good privacy education should meet highly diverse users where they are. For example, the digital literacy and language comprehension of our users differs widely around the world. This is where privacy education comes in - it involves educating users on how to effectively use privacy tools, settings, and resources, empowering them to make informed privacy decisions. This knowledge is essential as it allows users to navigate the online world with a better understanding of the implications of their choices. Typically when measuring whether a non-privacy product feature (such as adding a new reaction emoji to posts) is effective, one can look at the data and determine, for example, how many people use the feature. However, when the measurement involves a privacy tool, it is more complicated. In order to determine whether a privacy product is successful, one cannot just look at how many users engage with the tool, can find the tool or know about the tool, but it is also important to understand users' privacy expectations and perceptions, such as their confidence in understanding privacy on the app or their confidence in their ability to manage their privacy on the app.

Technology companies are often asked to share their assessment approach to particular privacy education and tools. We presented to our global privacy expert stakeholder roundtables about our privacy education tools and the challenges with assessing such tools more generally. Our stakeholders expressed that the presentation was informative and recommended that we share this information broadly to increase awareness of the diverse purposes different privacy tools can serve, and thus the necessary diversity of assessing their success (this article).

Privacy Education at Meta

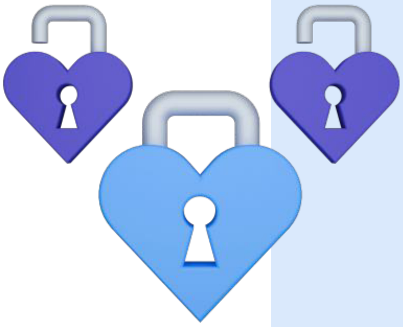
> **At Meta, we recognize the importance of educating people who use our products about privacy, thus enabling them to make informed choices while using our apps such as Facebook, Messenger and Instagram.**

Privacy is highly personal and there are a wide variety of user privacy interests and concerns. For example, there are those who want the broadest possible reach of their content, those who want a narrow audience limited to friends and family, those who are concerned with maintaining siloed identities, and so on. These differences result in a challenging effort where we need to balance the importance of addressing various user concerns and privacy expectations while building a tool that can also benefit billions of people. Below are examples of just some of our privacy education products. Privacy education can take many different forms, which impacts how each of these products are measured. One product may be built to improve awareness of an existing privacy feature, whereas another product may be built to improve user understanding of privacy topics, and both of these purposes necessitate different privacy measurements.



Tool Tips

On Facebook, for example, a tooltip (small pointer to a feature with a short explanation) sometimes appears when users are about to post a video publicly. This reminds them that their content could be visible across Meta products and in search engine results. This prompt provides an opportunity for users to review and confirm their privacy choices, ensuring they are making the decision that best suits their intentions.



In-the-moment suggestions

These provide in-the-moment suggestions to a user who may benefit from one of our privacy tools. For example, Instagram provides a suggestion to users who may benefit from Instagram's 'Your Activity' tool: after an Instagram user removes 3 likes from posts or reels, Instagram prompts them to consider using the bulk unlike option in 'Your Activity' to unlike more posts or reels.

Facebook Privacy Check-up

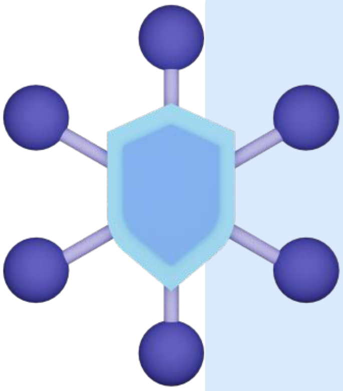
Facebook's Privacy Checkup is a simple tool that makes it easier for users to see and review their privacy settings on Facebook. This education tool shows several distinct topics to help users control who can see what they share, how their information is used and how to take actions to strengthen their account security.

Instagram Settings Check-up

Instagram's Settings Check-Up is a guided flow for users to review and update their most important safety and privacy settings in a way that is right for them. This is meant to be a check-in point for users to think about which settings are best for them and streamline their decisions to select the right settings to meet their needs.

Default Settings

On Facebook and Instagram, users who are under the age of 16 (or under 18 in certain countries) are defaulted into more private settings when they join. We then highlight how teens can choose a more private experience and explain how to change their privacy settings. For example, on Facebook, we encourage teens to consider more private settings for: Who can see their friends list, who can see the people, Pages and lists they follow, who can see posts they're tagged in on their profile, reviewing posts they're tagged in before the post appears on their profile, and who is allowed to comment on their public posts.



Privacy Center

Beyond the many individual privacy education features across Meta's apps, we have established central resources like the Privacy Center, which launched in early 2022 and serves as a central hub for users to learn about Meta's data practices, explore our privacy policy, and discover how to manage their privacy settings effectively. For instance, users can find out how location data works across Facebook and Instagram, and what they can control. They can also learn about generative AI at Meta and how it works, and change or delete their information from chats with AIs from Meta.

Challenges with assessing the effectiveness of privacy education products

> Measuring the effectiveness of privacy education products/features can be challenging. Since each product has a specific purpose, ranging from improving findability to enhancing clarity, they require different success metrics. We employ various measurement strategies, three of which are described below, and each have their own strengths and limitations.

First, surveys, while valuable for gathering direct user feedback, require large sample sizes and considerable resources, and are used selectively (shortly after a product launches and sometimes on a recurring basis thereafter) to avoid user fatigue. Next, usage data helps in assessing whether privacy controls are easily found and adopted by users, though it does not always reflect users' true feelings about their privacy - a phenomenon known as the "Privacy Paradox". Lastly, behavioral proxies are also informative as they rely on user behavior on our apps. Behavioral Proxies means you would look at whether users' behavior on the platform changes after introducing the new privacy education product. For example, people changing their audience more, posting more, clicking more. These are a good way to measure the effectiveness of privacy education products because they are based on logging, so it is more efficient than collecting answers manually via surveys. However, similar to the other ways of measuring, there are limitations in its application. Looking at user behavior does not reveal the user's perceptions and therefore cannot inform about whether a user is confident in their privacy. Since it is not always as simple as one method that tells an organization exactly what it wants to know, we like to use a variety of the ways to measure where possible.

Understanding the effectiveness of privacy education is similar to understanding the utility of an everyday product's manual: not everyone will engage with it the same way. Some users may never consult it, others may use it sporadically, and some may rely on it heavily only at certain times when they have a specific need for it. Knowing how many people use the manual or how often they use it isn't that helpful if what you want to determine is whether the manual is useful. Therefore, our goal is not just to increase the rate of usage of our privacy tools but to ensure that they are effective when users choose to engage with them, aiming to facilitate specific outcomes based on their immediate needs and goals. This approach underscores our commitment to not just providing privacy education but ensuring it is impactful, addressing the needs of our users effectively.

How We Develop and Assess the Success of Privacy Education Products at Meta

Our approach to developing privacy education at Meta is deliberate and focused on specific outcomes. We start by determining what success looks like for each privacy education experience - be it increasing awareness of a particular setting, enhancing users' confidence in how their data is used, or ensuring that certain information is accessible to users with different levels of literacy and digital literacy. We then design and develop experiences with the desired outcomes in mind. Throughout the development process, we use various methods such as surveys for user feedback and usage data analysis to ensure that the tools are meeting their intended purposes.

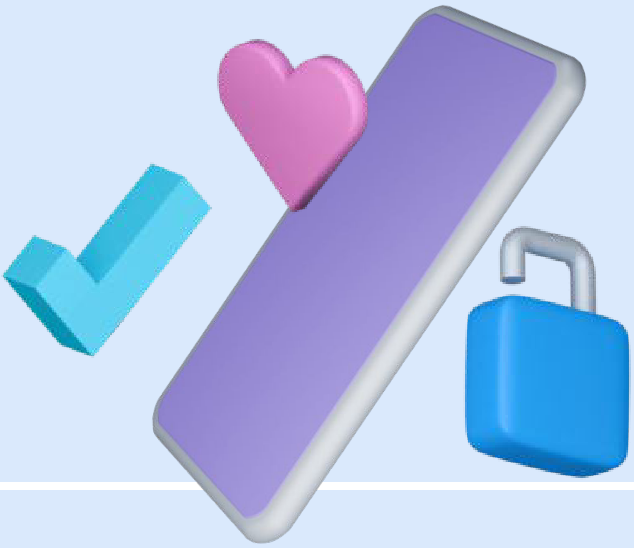
For example, if the education experience is intended to increase awareness for a specific privacy setting, we would measure whether awareness of that setting changes after introducing the education. In contrast, if the education experience is intended to help people feel more confident about how their data is used for ads, we might measure how confident people feel about that after engaging with the education. The following case from Instagram is an example of how we chose to measure specific context and assess its success.

Case study 1

Instagram’s Data Transparency Experiment

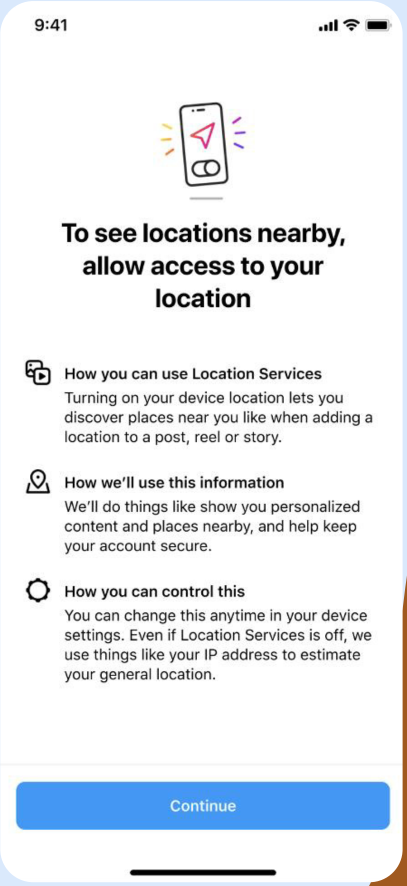
The Instagram team sought to improve the user’s overall privacy perceptions by providing better transparency into how location data is used on the platform. Specifically, the team built a solution to provide an educational “pre-prompt” before a user is asked to allow Instagram to use your location. This location permission flow is triggered whenever a user on Instagram shares their location for the first time. To improve the experience and provide additional transparency, we explained to users why we ask for their location data before they saw a screen seeking permission for location data.

As part of this test, the team considered measuring success via on platform user behaviors such as click rates or opt-ins, but ultimately the team decided that measuring perceptions of privacy, specifically the user’s confidence that Instagram settings or features can help protect their privacy, would be a better way to assess progress against the goal of improving user perceptions. In the study, we compared a test group of users who saw the new educational pre-prompt, to a control group of users who saw the existing location prompts without the pre-prompt.



The team used a survey (triggered shortly after the users saw the device permissions screen) to assess users' confidence in their ability to control their privacy in both the control and test group (N = ~1400 Instagram users on Android phones). The group that saw the educational pre-prompt reported significantly higher confidence than the group that did not see the pre-prompt. We learned that this education experience (i.e., pre-prompt) increased confidence in the settings and features of Instagram to protect their privacy.

Educational screen that the test group saw



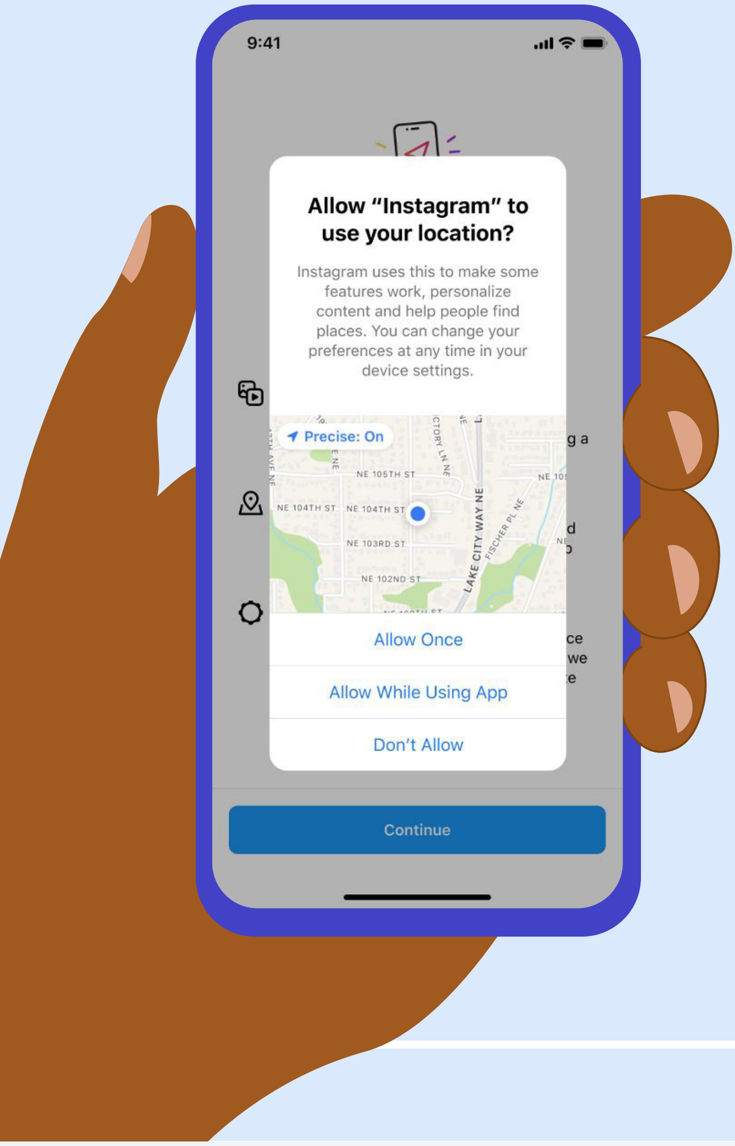
To see locations nearby, allow access to your location

How you can use Location Services
Turning on your device location lets you discover places near you like when adding a location to a post, reel or story.

How we'll use this information
We'll do things like show you personalized content and places nearby, and help keep your account secure.

How you can control this
You can change this anytime in your device settings. Even if Location Services is off, we use things like your IP address to estimate your general location.

Standard device permissions screen



Allow "Instagram" to use your location?

Instagram uses this to make some features work, personalize content and help people find places. You can change your preferences at any time in your device settings.

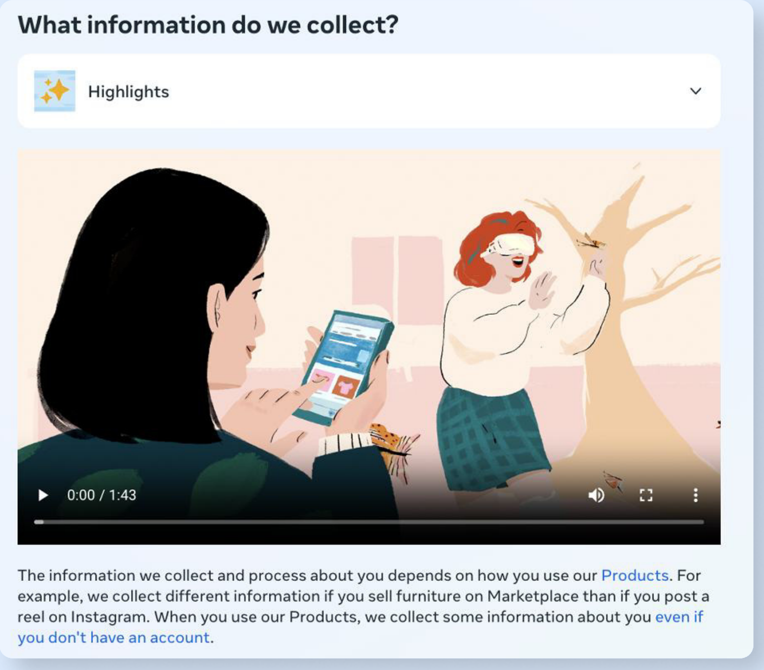
Case study 2

Meta's Privacy Policy

Privacy policies have been criticised as being heavy on legal jargon. That being said, a company's privacy policy is a document where users can learn about their data privacy rights and how a company processes their personal information. It is therefore important that privacy policies are written not just for the regulators who assess them, but rather can also be understood by the users whose data is impacted. Users have varying degrees of privacy and digital literacy and therefore a variety of techniques can be incorporated into privacy policies to enhance explainability. We aimed to make our Meta Privacy Policy easier to read for our users with an objective grade-level readability score known as the Flesch-Kincaid sale. We compared the readability score across the current Meta Privacy Policy and a soon-to-be updated Meta Privacy Policy to ensure we were meeting our goal of making the policy easier to read. The Meta Privacy Policy at that time scored around the collegiate level, while the updated Meta Privacy Policy scored at the secondary school level. This objective form of measurement helped us achieve a goal for the Meta Privacy Policy to be written at an appropriate reading level given our user base. When we released our improved Meta Privacy Policy in May 2022, this Meta Privacy Policy's text and design more clearly stated our data practices at an accessible reading level.

We also have heard from our privacy stakeholders that audiovisual resources and visuals are helpful tools to unpack privacy concepts for users. We therefore updated our Meta Privacy Policy with section highlights to help ease the explainability of the Meta Privacy Policy. It is intended to be a summary of each section which can support users with different levels of digital literacy, such as youth. In addition, we have illustrations and videos in the Meta Privacy Policy to help offer aids and alternative ways to bring privacy closer to our users. For example, we updated our images in 2023 to provide more visual resources. In order to help users understand complex terms used throughout the policy, we also clarified terms with short, easily-accessible definitions where a user can click on the term to reveal a short explanation.

Case study 2

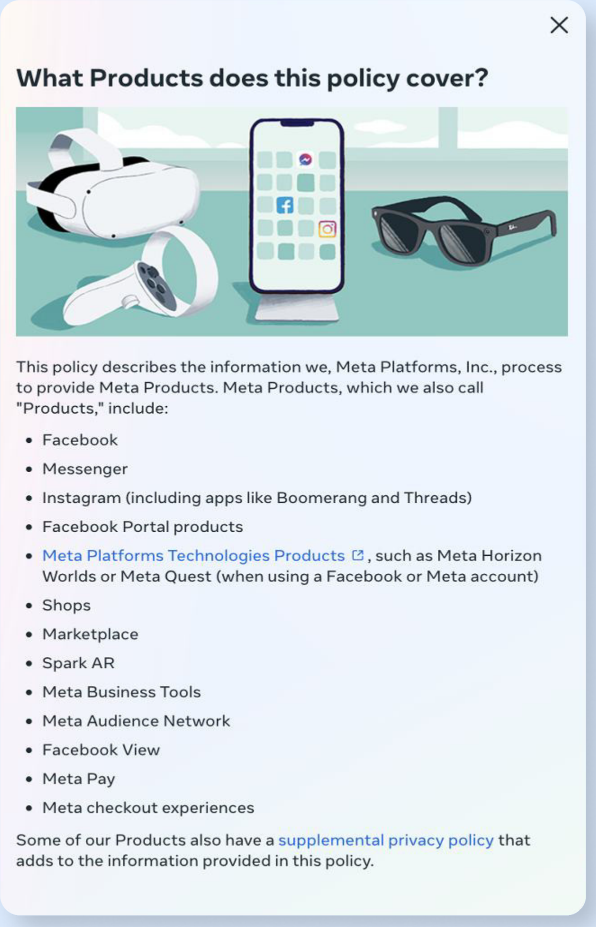


What information do we collect?

The information we collect and process about you depends on how you use our Products. For example, we collect different information if you sell furniture on Marketplace than if you post a reel on Instagram. When you use our Products, we collect some information about you even if you don't have an account.

← **Video from Meta privacy policy**

Illustration from Meta privacy policy →



What Products does this policy cover?

This policy describes the information we, Meta Platforms, Inc., process to provide Meta Products. Meta Products, which we also call "Products," include:

- Facebook
- Messenger
- Instagram (including apps like Boomerang and Threads)
- Facebook Portal products
- Meta Platforms Technologies Products, such as Meta Horizon Worlds or Meta Quest (when using a Facebook or Meta account)
- Shops
- Marketplace
- Spark AR
- Meta Business Tools
- Meta Audience Network
- Facebook View
- Meta Pay
- Meta checkout experiences

Some of our Products also have a supplemental privacy policy that adds to the information provided in this policy.

Conclusion

> Privacy measurement is a very complex topic as it is difficult to quantify how effective it is.

Ultimately, we want our education products to meet users' needs as best they can — to help us determine if they're doing that, we collect user feedback and iterate on our education products when we get a signal that there's a need to include additional information to help users feel sufficiently informed. As we develop more and more of these education products, our teams will get a better sense of where to set the bar. Despite challenges in assessing effectiveness, it is important that companies continue to develop privacy education products and improve their existing ones as users are increasingly interested in learning about their privacy choices and benefit from the privacy education options available to them.