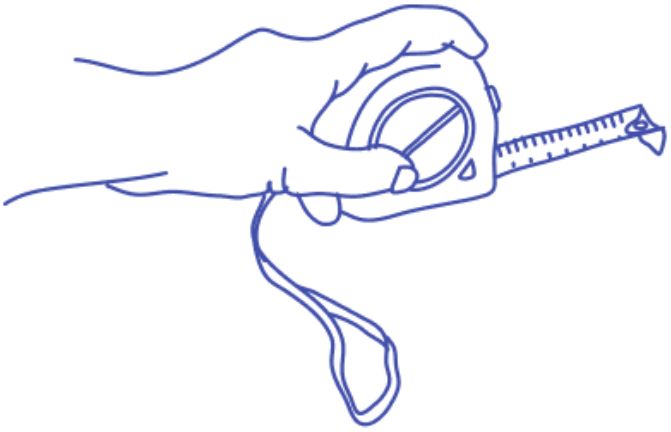
superbloom

Privacy Experience Heuristics

Measuring whether users can perceive privacy in technical products



Introduction

The Privacy Experience Heuristics measure whether users of a product can find, use, and understand the product's privacy features. A product that performs better on the Privacy Experience Heuristics isn't just doing a better job with privacy: it's doing a better job in a way people will notice. Our goal with these heuristics is to bridge the gap between privacy practices and the end user's experience. We hope this helps take privacy from being a technical compliance issue to a feature set that people like and value about a product.

What can be evaluated?

This methodology is designed to evaluate online platforms, desktop and mobile apps, and social media services. It can be used for any digital product or service, but is most interesting for products where users provide some personal information to the product.

The Privacy Experience Heuristics are not a guide to legal compliance. In some cases, the heuristics measure features that correspond to legal requirements (e.g. Article 17 of the GDPR requires that users can request deletion of their data). However, privacy regulations do not regulate product design, but rather the policies and processes behind the product. The Privacy Experience Heuristics sets a standard for what users can see, find, and understand, independent of what is legally required.

We use the term "product" in the heuristics to refer to the product, service, tool, or technology being evaluated, and "company" to refer to the organization(s) and/or group(s) that create and maintain it.

You may need to adapt the heuristics if you would like to evaluate:

- Hardware
- IoT devices
- Products offering AI features (we're working on this)
- Communities, online or offline

Authorship

This methodology was co-authored by the Security and Privacy Team at Vinted and the technology activism nonprofit Superbloom in late 2023 and early 2024. Read more about the methodology at sprblm.cc/privacyexperience.

How to use

These heuristics are designed to be used by someone external to the company. No internal information is needed to score the heuristics.

You will need access to a device that runs the product (i.e. for an iOS app, you need a device running iOS), and you will need to download the app or software if applicable. If the product offers accounts, you will need to create an account. You may also need to create sample posts, listings, or other content in order to fully experience the product.

If the product is freemium, you do not need to purchase a premium account to evaluate the product. Privacy is not a luxury, and privacy features should be available at all price tiers.

Scoring

Using the product itself and any other publicly available information, determine for each heuristic whether the product passes the heuristic fully, partially, not at all, or whether the heuristic is not applicable.

If you can't find an answer after a thorough search, but the heuristic should apply to the product, score a 0. Use your judgment when deciding how exhaustively to dig for a feature or a piece of information. Since the heuristics evaluate the *privacy experience*, passing a heuristic indicates that certain information or features need to be findable by an ordinary user.

Pass	The product fulfills this heuristic.	2 points
Partial pass	The product fulfills this heuristic fully, but it is hard to find information about it, or hard to find where to set, change, or influence it. OR The product fulfills this heuristic in part, but not in full. The evaluator sees an attempt to meet the heuristic, or progress towards meeting the heuristic.	1 point
No	The product does not fulfill the heuristic.	0 points
Undeterminable	The evaluator was not able to determine using publicly available information and personal use of the product whether the product fulfills the heuristic.	0 points
Not applicable	The heuristic does not apply to this product.	Excluded from score and averages

Determine a section score for each of the three sections as follows:

Points scored / applicable heuristics = section score

Heuristics

Smooth

These heuristics indicate a smooth privacy experience. People can just start using the product without being hassled or burdened with too many choices. They can trust that the default settings will meet a majority of their needs.

Corresponds with Privacy by Design, Principle 2: Privacy by Default.

Heuristic	Rationale	How to measure	Score
Privacy policy is understandable to a layperson.	Users can see that the company wants them to understand the privacy policy.	We go into detail about how to measure "understandable to a layperson" in Appendix, Assessing User-Facing Legal Documentation.	
Users are informed of changes to privacy policy in understandable language.	In many jurisdictions, including the EU and UK, users need to be informed of changes to the privacy policy they have agreed to, and a lack of response is determined to be equivalent to consent. This is usually done via emails written in dense legal language, which does not constitute informed, affirmative consent.	If changes to privacy policy are summarized in plain language above the legal language, **pass**. "Plain language" means language nonspecialists would use when talking to each other.	
When creating a new account, users are required to enter only information necessary to use the product.	If a field is required, that should mean it is required for the product to be used. It should not mean that the company wants to know this information for advertising purposes.	If a field whose information is not necessary for core function of the product is marked with "required," **no pass**. If the product does not have user accounts, **not applicable.**	

Users are not nudged to enter information if they can still use the product without entering that information.	Nudging users to enter personal information, when the product also functions without this information, is a way to try and get more information out of people than they may be willing to provide. Entering personal information may seem to be in a user's best interest. For example, users with no profile photo may experience difficulty interacting with others in the product. However, whether the tradeoff is worth it is for them to decide, not you. Do not nudge them to upload a profile photo unless the product doesn't work without it.	If users are nudged to enter unnecessary information, but there is a prominent "skip" or "no thanks" option that makes the nudge not occur again, **partial pass**. A notification that "your profile isn't complete" when the user can fully use the product indicates **no pass**.	
Users can reject cookies that are not essential to the product or website's function.	To pass, users must be able to reject cookies – even if the law doesn't require it. In some jurisdictions, such as the EU and UK, it is legally required to allow users to reject cookies. As data protection legislation advances across the globe, this will hopefully be the case in more jurisdictions. Meanwhile, privacy-friendly products can lead the way by offering this option even where it is	If there is no option to reject cookies on a website or web app, **no pass**.	

	required.		
Rejecting non-essential cookies is possible with only 1 click.	Many websites and products that alert users about cookies first ask users to go to a "review choices" screen (or similar). They may then even require toggling additional cookies off, in order for all non-essential cookies to be denied. This fulfills the letter of the GDPR and similar legislation, but it makes users highly unlikely to reject cookies.	If the first prompt to accept cookies also has a "Reject nonessential cookies," **pass**. If the first prompt contains "review choices" (or similar), but the second window has a "reject nonessential cookies" option visible without further clicking, scrolling, or toggling, **partial pass**.	
Signups for newsletters, offers, and extra services are opt-in.	Users should choose actively to receive communication, with no chance of accidentally opting in.	If the option to receive a newsletter, a weekly special offer, product updates, or any other company communication is deselected by default, **pass.** If the option is selected by default, **no pass.** If the evaluator receives any communication from the product that they didn't know they were signing up for, **no pass.**	

Supportive

These heuristics indicate a well-supported privacy experience. People are nudged towards actions that are in their interest. Personal data collection is minimized. The product warns or even forbids people from doing things that would compromise their privacy. People know there are guardrails in place to protect them, both from the company and from other people.

Corresponds with Privacy by Design, Principle 3: Privacy Embedded Into Design; Principle 5, End-To-End Security; Principle 1, Proactive not reactive.

Heuristic	Rationale	How to measure	Score
Metadata is removed from uploaded images.	Few users are aware that images contain metadata; this metadata could be used to determine their location and other personal information without their knowledge.	If uploaded images do not contain the following data, pass: Camera settings Date and time Location If uploaded images contain 1 or 2 of these, but not all 3, partial pass.	
Users are informed about the status of message encryption.	Members should be made aware whether their messages are encrypted or not.	If a notice explaining whether or not messages are encrypted appears in the message dialog box, pass. If encryption information is only found in the privacy policy, partial pass.	
The product only requests permissions related to its use.	Developers can request access to many different device permissions that may not be related to the app's use. Though users are given the chance to deny the permission, many people are likely to click "allow" just to be done with the process and use the app. Permissions that may be requested include: ● Camera ● Microphone ● Notifications ● Contacts ● Calendar ● Bluetooth ● Smart home information ● Call log ● Ability to make calls ● Files on device (not photos)	If the evaluator tries out all the main features of the product and no requests to enable unrelated hardware are made, **pass.** If the product requests access to a permission that does seem related to the product's core functions, but the request appears right away instead of waiting for the evaluator to attempt to use the feature, **partial pass.** If the product requests access to a permission that does not seem related to the product's core functions, **no pass.** (Example: a website requesting to send notifications scores a "no pass," unless the website has to do with timers, messaging, or something	

	• Health data, including physical activity like step count • Nearby devices • Location (general) • Location (precise)	time-sensitive.)	
Users can block other users	Peer-to-peer interactions always carry a risk: a transaction can turn into threats, harassment, or other unwanted messages. Users need to be able to protect themselves by blocking other users.	If it is possible to block other users within the messaging/communication interface, **pass.** If it is possible to block other users but not within the messaging/communication interface, **partial pass.**	
Users can report other users	In order to keep user interaction safe, users need to be able to report suspicious activity: fraud, harassment, or other violations of the product's terms of service. In both cases, the report needs to be easy to submit within the product, and the interface should not be a barrier to reporting.	If it is possible to report other users within the messaging/communication interface, **pass.** If it is possible to report other users but not within the messaging/communication interface, **partial pass.**	

Empowering

These heuristics make a privacy experience feel empowering. People can control their experience, change their settings, and understand what's going on. They can exercise their legal rights, whether that's accessing their data or lodging a complaint.

Corresponds with Privacy by Design, Principle 6: Visibility and Transparency; Principle 4, Full-Sum, Not Zero-Sum.

Heuristic	Rationale	How to measure	Score

Users are able to steer the recommendations shown to them.	Being able to control personalization leads to higher user satisfaction, as well as a perception of transparency.	If users can access a non-personalized feed in the same place as the personalized feed is shown, **pass**. If users can access this feed but only by disabling a setting in the settings panel, **partial pass**. If the product doesn't have a feed or recommendations, **not applicable**.	
Users can delete search history	Being able to delete search history may be important if the search history contains sensitive information.	If users can delete their searches and history in context (e.g. from the search screen), **pass**. If users can delete their searches and history from within "privacy settings" or similar, **partial pass**. If the product doesn't have search, **not applicable**.	
Users can request a copy of their data in the interface	To pass, users must be able to request a copy of their data – even if the law doesn't require it. In some jurisdictions, such as the EU and UK, it is legally required to allow users access to their data. As data privacy legislation advances across the globe, this will hopefully be the case in more jurisdictions. The feature needs to be available in the interface. If the option is buried (for example, an email address provided with no instructions on how to submit the request), it	If users can request a copy of their data within the app interface, **pass**. If users can request a copy of their data within the interface but it is more than 2 clicks deep in the settings panel, **partial pass**. If the app sends users to a website where they need to enter additional information, **partial pass**. If the app provides an email address where users can request their data, **no pass**. If users cannot request a copy of their data, **no pass**.	

	might as well not be offered, since most users will not find it or use it.		
Users can control what information is shown in their profiles	Harassment can happen between users based on information shown in profiles. A profile containing more information may improve the product experience for some users. For others, it makes them more vulnerable. Which data to show is for each user to determine in their individual situation, not a choice the company should make for them.	If it is possible to make all fields in a profile private except for username and general location, and it is possible to do this in the profile edit screen, **pass**. If it is only possible to do this somewhere other than the profile edit screen, such as in the privacy settings, **partial pass.** If it is not possible to make photo, specific location, or full name private, **no pass**. If the product does not have user profiles, **not applicable.**	
Users can view how their profile looks to others	Users need to be able to make an informed choice about how their profile should appear.	Can users view the “public version” of their profiles other than by searching for their own username? If so, **pass**. If the product does not have user profiles, **not applicable.**	
Users can easily create an account without linking the account to another service.	Though some users may prefer a single sign-on through Google or Facebook, linking their accounts, others may prefer to keep their accounts separate.	If users can create an account using an email account, a phone number, or similar, **pass.** If users need to click a link to create an account with an email address/phone number, and this link is smaller and/or less prominent than the options to create an account with e.g. Google or Facebook, **partial pass.** If the product does not have user accounts, **not applicable.**	
The product allows users to delete accounts.	If the product is not an app, users should be able to delete their accounts from within the website.	If a website allows users to take all steps to delete their accounts, **pass**. If an app allows users to either delete their account, or directs them to a	

	Apps that allow or require account creation should allow users to delete their accounts, either in the app or in a flow that is linked from the app. (According to the Apple App Store guidelines, deleting an account should also delete data from developers' servers, though we have no way to verify this in the evaluation process.)	website where they can delete their account, **pass**. If users need to write an email, send a message, or make a phone call to delete an account, **no pass.** If the product does not have user accounts, **not applicable.**	
Users are periodically prompted to review their privacy choices.	Many users are occasional users of products and platforms. They may have forgotten what their choices were when they first signed up, and those choices might not be relevant any more.	If members are prompted to review their privacy settings, **pass**.	

Appendix: Evaluating User-Facing Legal Documentation

In order to determine whether a customer-facing legal document (e.g. privacy policy or terms and conditions) is easy to read, we need to define what “easy to read” means. In an ideal case, the evaluator could ask comprehension questions of actual users, but this is often not practical. The following rubric approximates roughly how comprehensible a legal document might be to an end user.

There are 24 possible points in the scale below. Few documents will score all 24 points – we don’t expect any documents to earn the full score. A score of above 16 is quite good; we would count it as passing. A score above 8 is still better than many legal documents, and we would consider it a partial pass.

Clarity of purpose and rights	Is the purpose of the document stated? **Score 1** if yes. **Score 0** if no. When you start reading the document, do you have an idea of what sorts of topics will be covered in it? **Score 1** if yes. **Score 0** if no. Are the user’s rights stated? **Score 1** if yes. **Score 0** if no. Are actions and choices available to the user stated? **Score 1** if yes. **Score 0** if no.

	Does the document state how to exercise those rights and/or take those actions? **Score 1** if yes. **Score 0** if no.
Length	If you have read the same type of document from other companies, does this seem to be more concise than average to you? **Score 2** for an average to short document. **Score 1** for a slightly long document. **Score 0** for a very long document.
Use of plain language	**Positive** Is the language used easy to understand? Are familiar phrases present? When you read it aloud, does it sound like something you would say? **Negative** When you read part of the document aloud, can you easily think of a clearer way to say it? Are there words you don't understand? Are there references to laws without links or summaries? **Scoring** **Score 6** for language you easily understand. **Score 3** for language you can mostly understand. **Score 0** for a document written in technical language.
Organization, structure, and navigability	Is there a summary or "TL;DR" at the beginning of the document? Are the sections hyperlinked, i.e. reachable via links or a table of contents? If either of these are present, **score 2.** If there is no other navigation but the document is divided into sections, **score 1.** If the document is a long series of paragraphs with no overarching organization, **score 0.**
Accessibility features	Is there enough contrast between type and background? **Score 1** if yes.

	Score 0 if no. Is there whitespace around the text and between sections? **Score 1** if yes. **Score 0** if no. Are alternative formats available (e.g. audio, plain language, translations)? **Score 2** if yes. **Score 0** if no.
Examples or scenarios	Does the document include examples or scenarios to illustrate key points? If so, **score 2.**
Definitions or glossary	Are definitions of words available, either in a separate glossary section or inline? (The legal writing construction "X, hereinafter referred to as Y" doesn't count as a definition.) If so, **score 2.**

Acknowledgements

Last updated: January 2025

Authors: Abhishek Sharma, Veszna Wessenauer, Molly Wilson

This blog post is based on a session at MozFest 2024, "Elevating Privacy: Centering User Experience," presented by Veszna Wessenauer, Mascha Arnst, and Jasper Enderman.