Best practices

- Be aware of what you do
  - Do
- Stay up to date
- Resources
  - Browser vendors and web platform developers
  - Privacy organizations
  - Governmental organizations
- Looking inward
  - Do
- Prevent overreach and control access
  - Document your uses
  - Have processes and rules around handling user data
  - Make avoiding overreach be the path of least resistance
  - Pushing back with alternatives, not stop energy
  - Do

Over this whole course, certain themes have come up again and again. Protecting your users' privacy involves knowing the minimum that you need about them, being honest and transparent with what you need and why, and removing what you have as soon as you no longer need it. You are also responsible for what others are able to do and are allowed to do with your users' data, and that means that you need to be able to explain honestly and transparently what that is. Any data that you don't need, you should not have; any data that you do need, you should be able to explain why you need it, and for how long.

In larger organizations, there may be roles or teams dedicated to tracking the latest technical changes in your deployment environments and browsers, and to understanding the implications for technical and legal changes on your users' privacy. But a smaller organization still needs to be conscious of user privacy, how a changing environment can affect decisions already made, and what needs to be taken into account for decisions you make from now on. This module summarizes some best practices for how you can stay in touch with your privacy choices and requirements, and those of your users.

Be aware of what you do

The first best practice here is *understanding*. You need to be aware of what you know about your users, and why you know it; you need to be aware of what your partners know about your users, and how they found it out. This should be a documented part of your privacy policy. It is difficult and time-consuming to put this list together at first, but more importantly it's also eye-opening for you and for the business. It can often come as a surprise (and not a nice surprise) just how much data you collect and store about your users. Documenting it will give you a level of awareness, not just into data collection and privacy, but into the user experience of your systems and into the underlying software as well. There are frequently dusty corners or superseded requests which are in need of updating and which have been forgotten about.

Do

For each piece of data that could be tied to a user, explicitly document:

- A specific list of what it is collected for.
- When it will be deleted (and how it can be deleted by the user, not only by your own team).
- How you collect it.

Ensure that it is gathered only at sufficient granularity to answer these questions alone.

This documentation is for internal use and should be full and complete, but it can be valuable to document this publicly for users, because it is important to establish an atmosphere of trust. This is not only beneficial in general terms for the customer relationship, but your users are more likely to volunteer the data you need to make business decisions if they are confident it will not be misused. This public documentation is linked to your more general privacy policy (in fact, it will form the great part of your privacy policy), and having this written in a form that your users can understand (alongside the legal language) helps to build the trust relationship.

Stay up to date

The second-best practice is to *stay up to date*. This whole industry moves quickly as a general rule, and privacy is a fast-changing field; staying up to date can itself be a challenge. Technology that's available to you will alter frequently, but user expectations will also alter just as fast. It is important to not fall behind, and if you can stay ahead, then there is a real competitive advantage to be had by staking out a position as privacy-preserving. Managing user privacy and understanding how the industry may be changing may not be all of someone's job, and you do not need to be experts, but it should be *some* of someone's job. Dedicate some of the training or conference budget to staying in touch with industry trends and regulatory updates.

It can be difficult to keep up with changing attitudes and best practices in privacy. There isn't a convenient single place to go for this. This is partially because privacy protection is a wide-ranging field which impacts on many different parts of many different industries. But the very topic of how best to protect the privacy of your users and others is heavily disputed and there are many different and often conflicting approaches. In this course, we have laid out a path to follow and some best practices, but it will be useful to you to synthesize your own approach as best fits your goals, your organization's , and your users' needs. We have compiled a list of resources available for you, your management, and the team around you to help you stay up to date with changing norms and what currently constitutes the best things to do.

Some privacy changes made by browsers are technical in nature, and need to be understood by dev teams. Consider, for example, the change to SameSite=Lax by default on cookies. This change affected features on some sites, and so may have needed technical changes. It was announced in advance and trialed before being finally rolled out. This is a good example of the sort of change that can affect user privacy (in this case, that change was an improvement) and may also need changes to your apps to correctly deal with.

Resources

Browser vendors and web platform developers

For most web development teams, the best places to stay up to date with the latest industry practices on privacy and user protection are the browser vendors and consumer data protection organizations. For announcements and press releases, this means the various browser vendor team blogs: a good portion of these are about technologies and things unrelated to privacy, but where there are privacy-related announcements, they'll show up there:

- Webkit (https://webkit.org/blog/)
- Chrome (https://developer.chrome.com/blog/ and https://blog.chromium.org/)
- Firefox (https://hacks.mozilla.org/)
- Edge (https://blogs.windows.com/msedgedev/)
- Samsung Developers (https://developer.samsung.com/blog).

To get a sense of what the browsers plan to implement and to work out their stances on upcoming and proposed APIs that you're thinking of using, there are status pages and positions pages:

- WebKit (https://webkit.org/status and https://github.com/WebKit/standards-positions)

- Chrome (https://chromestatus.com/features and https://developer.chrome.com/tags/deprecations/ for things being removed)
- Edge (https://developer.microsoft.com/en-us/microsoft-edge/status/)
- Firefox (https://mozilla.github.io/standards-positions/)

Privacy organizations

Of course, the browser vendors' positions are only one input to this conversation. There are also organizations pushing for improving privacy protection over the current state, and it's worth keeping tabs on them. The list is long, but here are just a few examples:

- The EFF's Privacy issue (https://www.eff.org/issues/privacy).
- The Open Rights Group's digital privacy initiative (https://www.openrightsgroup.org/category/online-privacy).
- IAPP (https://iapp.org/).

Governmental organizations

To keep a closer eye on this whole area, there are also other actors in the field to follow. Governmental organizations' decisions and their approaches have some of the greatest impact:

- European Data Protection Board in the EU.
- ICO in the UK.
- The California Privacy Protection Agency in California.
- Data Protection Africa
- IAPP's overview of data protection across Asia.

Mainstream media privacy reporting can often focus primarily on "big tech" firms and governmental organizations, which may seem removed from work done at a smaller company or organization. It's also often very US-centric. But even so, it's useful to keep aware of what the rules might be in the future, so that you can be prepared, as can the team and the management structures around you.

It's also worth checking out Understanding Privacy, published in November 2022 by Heather Burns, which gives a really good look at the whole field of data privacy and what you need to know about it. Recommended!

Looking inward

Staying up to date also means staying up to date with your own stance. As part of *understanding* your own software, you will have conducted audits and reviews of your own data collection and your third-party partners. These audits are not a one-time-only thing: they should be repeated at regular intervals and kept updated as software changes. It can be useful to mandate that the privacy audit documentation is kept updated as part of development, just as other technical documentation is. If a new release collects more data, then updating the privacy audit to include what is collected and why and when it will be deleted is of similar importance to a new release's APIs being described in the public documentation.

Do

- Stay up to date with how the industry and user expectations around privacy may be changing over time. It's often the case that someone on a team is particularly interested in privacy-related topics, even if there isn't the budget or sufficient need for a full-time role. Consider formalizing this by making privacy an official part of someone's job, with accompanying benefits for the responsibility.
- Make keeping the privacy audit documentation from "Understanding" earlier, part of your documentation process just like API docs are.
- Re-run the audits of which data you collect and which third parties you use, either on a regular basis or when major features change; test your software as a new user to discover what information is asked for, and add this to the audits.

Prevent overreach and control access

The third best practice is to *prevent overreach*: that is, to avoid doing more with data than you committed to, and to avoid speculatively gathering data in case it becomes useful in the future. That involves adapting your processes so that you set the culture you want around protecting user privacy. Cultural change is difficult, but once accomplished it will largely maintain itself, which is easier.

Document your uses

Consider one of the best practices discussed earlier, that of documenting what exactly user data is collected for. This documentation is important for you to understand what you do and why, but it is

equally important to ensure that this rule is obeyed. If someone suggests using already-gathered data for new analyses, push back on that suggestion, because that's not what the data was gathered for. This is helped by other aspects of data understanding: that data is only gathered at the lowest acceptable granularity, and is deleted after being used, because it's impossible to reuse existing data for new analyses if there is no existing data.

Have processes and rules around handling user data

This can be difficult. It's hard to explain the nature of the user relationship in these situations, when there may be insights to be gained and nothing preventing that other than a promise previously made. But it's important to consider that the user entrusted the data to you for a specific purpose, and you (and your team) shouldn't abuse it for something else. A good approach here is to require some amount of process around access to user data. It is very important to avoid inserting a mandatory "privacy" component into every working process as a substitute for actually caring about the issue, because it can quickly become a "checkbox" feature that everybody ignores (and nobody likes more paperwork, especially if it's paperwork that nobody reads).

Make avoiding overreach be the path of least resistance

But there is a chance to use the annoying nature of bureaucracy slightly for your own benefit here! If mining existing collected data requires filling out a "privacy request" where the new analysis is justified and recorded, then projects which don't really need that access are quite likely to avoid it in order to avoid the bureaucracy, or in order to avoid being named on the paperwork. You may already have policies in place around the security of user data: saved account details are restricted and not available to employees without justification. Consider tying privacy requirements to these existing policies. If there's some consideration of user privacy built into your processes at an early stage, that consideration can quickly become a routine part of planning. It's vital that architects, developers, and marketing do not see privacy protection as an onerous externally imposed restriction, but as a core part of the customer relationship.

Pushing back with alternatives, not stop energy

With the preceding best practices in place, you will have gathered user data for only specific and measurable aims, and your user base will have been informed of those aims and understand them. However, you will also have a large collection of user data, and it's quite common that the business

will seek to use that data for reasons other than those for which it was gathered. It's your goal to push back on those uses, but it's important to do so by providing alternatives. Imagine that you've requested that your users provide an age bracket that they fall into: 18-25, 25-35, 35-50, 50+. You did this in order to measure which types of products are most bought by different age brackets, and you explicitly informed users that's why their age was requested. If someone then suggested that they could use that data to send advertising email to every user under 25, that's a new and undeclared use for existing data, and so isn't allowed. But your intention here should be to find a way of meeting the business need without using data for things that weren't declared. If you push back on this without proposing any alternative, then user privacy will start to seem like the externally imposed restriction warned against earlier, rather than a core part of why your users trust you. As much as possible, avoid adding stop energy to processes: the only thing worse than a bald "computer says no" is "internal regulator says no". Instead, consider other ways you could meet that goal without using users' personal data to do it: perhaps use the list of products purchased as a guide for who to email, or avoid targeted distribution entirely. Help your team understand why your users trust you, and what that trust is founded upon, and then help them do what they want and what your users want. Make privacy work for you.

Do

- Require a (short, simple) written justification from a named employee for access to user data.
- Add user privacy requirements as early as possible in your processes.
- Avoid adding privacy concerns as a mandatory "checkbox" feature.
- Enforce the deletion of data as defined earlier.
- Help the rest of the team understand how to achieve their goals without compromising your users' privacy.

□□□ #2
□ □□□ □□□ 2026-10-31 22:54:17 UTC
□ □□□ □□□ 2026-10-31 22:54:18 UTC