Top Tips to Lower the Risk of a Privacy Investigation

November 10, 2023

Julie Rooney
Head of US Privacy
Deputy General Counsel
OpenX

Julia Tama
Co-Chair, Privacy & Data Security
Venable LLP

Privacy+ Security Forum

Agenda

Privacy+ Security Forum

- Ad Tech and Data Sharing Technologies
- Privacy Policies and Notices
- Chatbots and Session Replays
- Effective Opt-Outs and Deletions
- Location Data or BSSIDs
- Review of Third-Party Data Suppliers

Where Do FTC Cases Come From?

Privacy+ Security Forum

- Consumer Complaints
- Media Reports
- Academic Research Papers
- Proactive Reviews
- Industry Sweeps

Ad Tech & Data Sharing Technologies

Privacy+ Security Forum

Overview

Pixels (and similar technologies) are designed to collect certain data and share this data with third parties.

These technologies may share information that could be considered sensitive—e.g., health-related data.

Risk may arise, for example, when:

Web development teams install pixels or similar tools without consulting the privacy team.

An organization does not have contractual limits in place on what third-party recipients can do with such data.

Compliance Tips

Privacy+ Security Forum

- Inventory pixels and other sharing technologies on each relevant website or application.
- Establish communication and review processes between development/engineering teams and privacy/legal/compliance teams.
- Limit pixels and similar data sharing to those where business benefits outweigh legal risks.
- Make sure privacy policy reflects pixel practices and consider providing notice outside the privacy policy if pixel use is significant.
- Ensure contractual agreements with third parties that receive data include restrictions and terms.
- Comply with state law requirements for disclosures to third parties, including sales provisions if applicable.

Privacy Policies & Other Privacy Notices

Privacy+ Security Forum

Overview

Privacy policies (and other notices) are both:
(1) Necessary notice to consumers of data practices and
(2) A potential basis for enforcement.

Risk may arise, for example, when:

Material changes are made without obtaining consent from consumers whose data the organization has already collected.

Including excessive or flowery statements about an organization's approach or commitment to privacy.

Representations about practices (e.g., collection or deletion) do not match or do not adequately disclose practices.

Including seals or signals showing compliance with a privacy program where program compliance is not complete.

Compliance Tips

Privacy+ Security Forum

- Make sure all material practices are disclosed.
- Build in flexibility for the future.
- If making a material change to privacy practices, provide notice and obtain consent for the change from consumers whose data the organization has already collected.
- Ensure consistency across privacy representations made in different places and to different audiences.
- Review third-party agreements for consistency with the organization’s privacy policy.
- Avoid confusing privacy settings or other consumer choice interfaces.

Chatbots and Session Replay

Privacy+ Security Forum

Overview

- All 50 states and the federal government have laws relating to wiretapping or surveilling communications. Many state laws require the consent of all parties prior to recording or intercepting a communication.

- **Session-replay tools** allow a website operator to record a user's interactions with the website, typically for improvement purposes.

- **Chatbots** allow a website operator to use a third party to interact with consumers and answer questions.

- Recent **class-action lawsuits under wiretapping laws** have alleged that the use of session-replay technology constitutes wiretapping and a violation of the relevant statute.
  - Wiretap statutes may provide for **statutory damages**, raising the risk of litigation.
  - In 2022, cases in the Third and Ninth Circuits raised but did not definitively answer the issue of **whether notice in a privacy policy would be sufficient** to avoid liability under wiretapping statutes. These cases also inspired dozens of plaintiffs' suits.

Compliance Tips

Privacy+ Security Forum

- Confirm whether session replay or similar technologies are in use on an organization's online properties. Take account of whether an organization serves consumers in one-party or multi-party consent states.
- As noted with pixels, establish clear lines of communication between development/engineering teams and privacy/legal/compliance teams.
- Limit tools to those where business benefits outweigh legal risks.
- Make sure privacy policy reflects all practices and consider providing notice outside the privacy policy, such as in chatbot interface.
- Ensure contractual agreements with third parties that receive data include appropriate restrictions and terms.
- Comply with state law requirements for disclosures to third parties, including sales provisions if applicable.

Effective Opt-outs & Deletion

Privacy+ Security Forum

Overview

An organization may choose to offer consumers the ability to opt out of certain data processing and/or the ability to delete data.

A right to opt out of certain processing (e.g., for targeted advertising or for sales of personal information) and a right to delete data are also common features among state privacy laws.

Risk may arise, for example, when:

A company represents that it will opt consumers out of certain data processing or delete data about consumers but lacks the capacity to do so.

Some data or processing that should be subject to a consumer's opt-out or deletion request is excluded from the processing of actioning the request—e.g., the way data is stored makes it easy to overlook certain data.

An organization makes an opt-out effective for a limited time without clear notice to the consumer.

Default settings are not clear.

Compliance Tips

Privacy+ Security Forum

- Account for the full range of data processing with each consumer that submits an opt-out or deletion request. An inventory of the organization's data and corresponding practices may be useful.
- Ensure that all choices offered to consumers can be executed effectively and fully.
- In general, opt-outs should remain effective unless or until the consumer chooses to opt back in.
- If technical (or other) considerations limit how choices are executed, communicate these limitations clearly.

Location Data or BSSIDs

Privacy+ Security Forum

Overview

Location data can reveal information about a consumer, such as their home or place of work, healthcare visits for sensitive conditions, or school attendance, among others.

A basic service set identifier ("BSSID") identifies a wireless access point and therefore corresponds to a physical location.

Risk may arise, for example, when:

Incorporating software development kits that will collect location data from an app.

Drafting and presenting notices associated with location data collection.

Collecting BSSIDs, even if the BSSID is not matched to the location.

Compliance Tips

Privacy+ Security Forum

- Provide adequate notice to consumers of location data collection and use in privacy policies and, where appropriate, via just-in-time notices.
    - As a best practice, notices should state the purposes for location data collection, such as whether they will be shared for location-based advertising.
- Ensure location consents or permissions apply to all location data collection and use practices.
- Limit location data collection to what is necessary for business processes.
- Software development kits and apps should communicate about practices and privacy compliance so that requirements do not “fall through the cracks”.

Review of Third-Party Data Suppliers

Privacy+ Security Forum

Overview

Any entity that knowingly collects data from a child or from child-directed properties must comply with the Children's Online Privacy Protection Act ("COPPA").

Risk may arise, for example, when:

Users are asked to provide age information in any form, even if a property is not intended to appeal to children.

User journeys suggest children under 13 can register for a service without parental consent by misrepresenting their age.

Content of third-party properties is reviewed before collecting personal information, such as reviews for content categorization or quality purposes.

Compliance Tips

Privacy+ Security Forum

- Do not solicit age information from users unnecessarily.
- If age information is collected, implement neutral age–gates (e.g., do not suggest a child can register without an adult by lying about their age).
- If age information is collected, exclude children (if permitted by COPPA) or comply with COPPA as required.
- If reviewing third–party properties for content, then implement robust policies and training to make sure child-directed properties are identified and treated correctly.
- Note that “directed” to children includes properties that target children as one of their audiences, even if not the primary audience.
- If applicable, review state laws for requirements for minors under age 13 and, in some cases, for teens.

Other Tripwires

Privacy+ Security Forum

Compliance Tips

Privacy+ Security Forum

- Look out for old code; your organization may be collecting more than you think!
- Collect and share only what you need.
- Review repeatedly and in depth; processes can break over time.
- Take a “consumer’s eye” view to catch obvious compliance mistakes or dark patterns.
- Respond to consumer requests promptly and effectively.
- Work with reputable data suppliers, and if you sell data, sell it only to reputable customers.

Practical In-House Advice

Privacy+ Security Forum

- Be present and proactive
  - Stay ahead of the business and consistently remind them you are there
- Be aware of your audience
  - Speak their language, be their partner, and explain your thinking
- Be skeptical
  - Don’t drink (all of) the Kool-Aid
- Check and re-check; train and re-train; audit and re-audit
  - Ask the same question five times to five different people
- Don’t let perfection get in the way of progress

Questions?

Privacy+ Security Forum

Thank you!