Design and Evaluation of the UsersFirst Privacy Notice and Choice Threat Analysis Taxonomy

Xinran Alexandra Li Yu-Ju Yang Yash Maurya Tian Wang
Hana Habib Norman Sadeh Lorrie Faith Cranor
Carnegie Mellon University

1 Introduction

Privacy regulations have increasingly included usability requirements, such as clear, informed consent processes, prominently displayed notices, and avoiding manipulative design patterns [1, 4]. However, current user interface designs for privacy notice and choice (N&C) often involve long and jargon-packed texts that are difficult to understand for average users. Studies have shown that users are unlikely to thoroughly read privacy policies and actively engage with privacy controls [2, 3]. To provide organizations with more systematic guidance on meeting regulatory requirements and designing more usable N&C interfaces, there is a need for privacy threat modeling frameworks that can better identify and mitigate usability-related issues. While existing frameworks, such as LINDDUN PRO and PANOPTIC [5, 6], offer a starting point for identifying privacy threats, they do not offer detailed guidance related to N&C interfaces or provide specific examples or evaluation criteria regarding privacy N&C threats.

UsersFirst is a privacy threat modeling framework under development at Carnegie Mellon University (CMU) designed to help identify and mitigate user-oriented privacy threats associated with N&C interfaces. In this poster, we report on the first user study designed to evaluate the usefulness of an initial version of the privacy N&C threat taxonomy that is part of UsersFirst and evaluated its efficacy as compared to an existing taxonomy (LINDDUN PRO's unawareness threat category). This initial version of the UsersFirst Taxonomy is organized around three major categories of threats (delivery, language & content, and presentation & design) and comprises a total of 27 different threat types. We selected privacy N&C interfaces from a well-known e-commerce platform and conducted semi-structured in-person interview sessions with 14 participants who had prior privacy experience to explore the following research questions:

RQ1 Do privacy practitioners who use the UsersFirst Taxonomy identify more user-oriented threats associated with privacy N&C compared to those who do not use a taxonomy?

RQ2 Do privacy practitioners who use the UsersFirst Taxonomy identify more user-oriented threats associated with privacy N&C than those relying on the LINDDUN PRO taxonomy's unawareness category?

2 Methods

We recruited 14 participants, all of whom were current CMU students either enrolled in a full-semester course in privacy engineering or doing research in privacy at CMU's Cylab Security and Privacy Institute. Students belonging to the first category had prior exposure to privacy threat modeling concepts and the LINDDUN PRO framework through their coursework, while students recruited from Cylab all had at least one year of experience in privacy, either by doing research or working in a related industrial field. All the interviews were conducted in person and lasted approximately 60 minutes, with participants receiving a $20 Amazon gift card as compensation. The study was approved by the CMU IRB. All interviews were audio recorded and transcribed using a transcription software. To ensure the transcription quality, we manually reviewed and refined the transcripts against the audio recordings.

Participants were asked to act as privacy consultants for the selected platform and to examine four privacy N&C web pages on the platform. For each interface, participants were tasked with trying to identify any user-oriented privacy threats they could find. After examining more than 30 popular platforms, including e-commerce, streaming services, and social media, we determined and selected this particular platform due to it exhibiting a lot of threats included in our taxonomy. We asked all 14 participants to first browse and identify

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

threats from the four web pages without the benefit of any taxonomy, and then we randomly assigned seven participants to use the UsersFirst Taxonomy (see Appendix C) and seven participants to use LINDDUN PRO to find further threats (see Appendix D).

We began the interview by asking participants about their prior experience with using N&C interfaces and privacy threat modeling. Then, in the first stage of the interview, we asked them to identify N&C threats on the platform's interface without using any taxonomy by looking at one section in the privacy notice about cookies and similar technologies, one privacy choice page, and two advertisement setting pages. We chose only one specific section from the platform's privacy policy for participants to evaluate because the entire notice would have taken too long to read. We included all privacy choice pages implemented by the platform that we could identify.

For each of these four web pages, we requested that the participant follow the steps presented on an instruction sheet: first, locate the page on their own and skim through the page. Next, while participants navigated through the interface and toggled through various settings, we asked them to think aloud about their discoveries and share their thoughts regarding whether that page matched their expectations and if they considered it understandable for an average user. We then asked participants to write down the privacy issues they could identify on a piece of paper.

In the second stage of the interview, we provided participants with a taxonomy based on the group they were assigned to (LINDDUN PRO or UsersFirst). We asked participants to go through threat definitions (and examples, if any) one category at a time (Delivery, Language & Content, and Presentation & Design) and ask any questions they may have. Then, we asked them to apply the taxonomy to the interfaces they had just examined and voice their rationale for determining whether a threat exists or does not exist.

The last part of the interview sessions involved questions about participants' experience with and without using a taxonomy. Specifically, we asked if they consider the taxonomy easy to use and helpful and if there were any threats that they were confused about. We also asked if they had any suggestions regarding potential improvements to the taxonomy they used. To mitigate potential bias, we ensured that participants were not aware in the first stage of the interview that they would be using a taxonomy in the second stage, nor did we disclose the name of the taxonomy being used during the second stage of the interview. The complete interview script can be found in Appendix A

We compiled a list of 21 "baseline threats" consisting of all privacy-related usability issues, including 14 identified by the authors and 7 additionally identified by participants. We analyzed the transcripts and the privacy issues written down by participants to identify which of the baseline threats each participant identified without using a taxonomy and then with a taxonomy. This was an iterative process, and threats were added to the baseline threat list as we found new threats identified by participants. During the coding phase, a single coder was responsible for mapping participants' responses to the baseline threat list.

3 Results

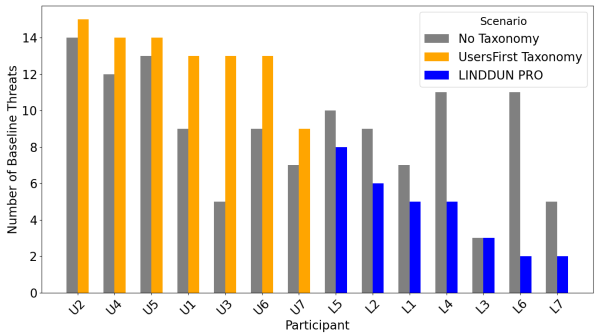


Figure 1: Number of Baseline Threats Identified

Figure 1 presents the number of baseline threats each participant has identified in different scenarios. Without using a taxonomy, participants identified between 3 and 14 of the baseline threats (mean = 8.93). We found that the UsersFirst Taxonomy allowed all participants to identify more threats than when using no-taxonomy, and six out of seven participants assigned using UsersFirst identified more than half of the baseline threats (n = 21). All participants assigned to use the UsersFirst Taxonomy identified more threats than those assigned to use LINDDUN PRO (an average of 13 threats out of a total of 21 for UsersFirst Taxonomy users and 4.43 threats for LINDDUN PRO users).

We examined the reasoning participants articulated for determining whether each threat in the UsersFirst Taxonomy was presented on the selected web pages. Participants were not always in agreement about whether a threat existed due to differences in their interpretation of the threat definitions and some subjectivity inherent in the task. For example, participants observed a binary privacy choice, which some considered straightforward and desirable, while others found insufficient and associated it with the "lack of choices" threat in the UsersFirst Taxonomy.

When we asked participants to comment on their experience with using the assigned taxonomy, participants in both groups found their taxonomy helpful for identifying overlooked threats. Participants who used UsersFirst commented that it was easy to use and helped them better organize their thoughts, while LINDDUN PRO's users commented that understanding the taxonomy to a degree to be able to apply it requires considerable effort.

Acknowledgments

The researchers gratefully acknowledge the support of the Digital Transformation and Innovation Center at Carnegie Mellon University sponsored by PwC.

References

[1] European Commission. Data protection in the EU, 2024. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en.

[2] Duha Ibdah, Nada Lachtar, Satya Meenakshi Raparthi, and Anys Bacha. "Why should I read the privacy policy, I just need the service": A study on attitudes and perceptions toward privacy policies. *IEEE access*, 9:166465–166487, 2021.

[3] Jonathan A Obar and Anne Oeldorf-Hirsch. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1):128–147, 2020.

[4] State of California. California Consumer Privacy Act (CCPA), Mar 2024. https://oag.ca.gov/privacy/ccpa.

[5] Stuart Shapiro, Cara Bloom, Ben Ballard, Shelby Slotter, Mark Paes, Julie McEwen, Ryan Xu, and Samantha Katcher. The panoptic™ privacy threat model. Technical report, December 2023. https://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/1dsumclm9ao4aiq0cvbvsgn24p.

[6] Laurens Sion and Wouter Joosen. LINDDUN PRO Privacy Threat Modeling Tutorial. Technical report, 2023. http://www.linddun.org/pro.

A Interview Script

A.1 Introduction

Opening Hello, and thank you for participating in our study today. My name is [], and I'll be the interviewer today. Joining me is [], who will be responsible for taking notes. We are part of a research team that focuses on understanding how different frameworks can help identify privacy vulnerabilities in digital interfaces. I want to assure you that all the information we collect today will be kept confidential. At any point of time during the interview, if you want to terminate your participation, please let us know. If you participate until the end of this interview, we will send an Amazon gift card of $20 within the same week. We will be recording this session to ensure we accurately capture your feedback and thoughts. Here is the consent form for you to review and sign. Please let me know when you have finished reading it or if you have any questions. [Once they sign consent forms] [start screen recording]. Do you agree with the terms listed in the consent form, and do we have the consent to record this interview session?

A.2 General Questions

- **Q1** Can you share your demographic information, including your gender, age, and the highest level of education?
- **Q2** Have you encountered the concepts of privacy notice and choice in digital interfaces before? If so, can you give an example?
- **Q3** Can you share your experience with privacy threat modeling?

A.3 Scenario 1: No-Taxonomy Phase

Here's an instruction sheet with several tasks you will need to complete. We will walk you through the entire process, so please don't feel overwhelmed. We first present you with an official definition of privacy notice and choice. Introduction to privacy notice and choice: A privacy notice is basically a presentation of terms, often in the form of a privacy policy or terms of use agreement, that systems implement to inform users of their data rights and explain data practices involved in the system. A privacy choice is enabled by systems that allow users to select different levels of control with regard to the terms as indicated in the privacy notice.

You will be shown a digital interface using our team's laptop and asked to act as xxx's privacy consultant. You will use the project team's account so you can navigate through the website as a logged-in user to evaluate its notice and choice implementation. Throughout this interview, you will not be asked to input any of your personal information.

Refer to the instruction sheet (B).

- *Task A We ask you to focus only on Cookies & similar technologies in its privacy notice (section 9).*
- *Task B The platform implements one privacy choice page.*
- *Task C The platform implements two advertisement setting pages. (For C2, if it takes the participant longer than 2 minutes to find the page, the interviewer should ask them to take a look at the account settings page).*

A.4 Scenario 2: With-Taxonomy Phase

At this point, we hand participants the actual taxonomy.

Various privacy threats arise when users experience potential loss of control over personal information. We now give you a taxonomy that you can use to identify privacy threats, which includes [for Group 1: five threats that belong to the unawareness category with definitions and examples of threats] a table with categorized privacy threats, and you can go to later pages to view respective definitions, ways of evaluation, and examples of the specific threat. You can click the outline on the left to go to specific sections or to go back to the top.

Please take a couple of minutes to only focus on the "Delivery" category of the taxonomy. Try your best to familiarize yourself with the definitions of each threat in the Delivery category and ask any questions you have. You don't need to think aloud about this part, but you are encouraged to voice any questions you may have.

Now, we will ask you to start using the threats from the "Delivery" category to identify threats in the platform's privacy notice and choice. Throughout the threat identification process, we ask that you circle on the paper version of the taxonomy the threats that you identify and cross out the ones you think does not apply, and give verbal justifications that include 1) sharing which threat you find/not find and 2) how you identify/not identify this threat.

Follow a similar process for the other two categories.

A.5 Post-taxonomy Questions

we will now ask you some questions about your thought process during the threat identification process and any suggestions you may have regarding the provided taxonomy.

- **Q4 Taxonomy Comprehension** Are there any threats that you find its definition hard to understand?
- **Q5 Ease of Use** How easy or difficult was it to identify privacy threats using the taxonomy we provided?
- **Q6 Usefulness** Did you feel that the taxonomy/framework guided your thought process? If so, how?
- **Q7 Improvements** Can you suggest any improvements or changes to the taxonomy/framework?

A.6 Closure

As we come to the end of our session, I'd like to take a moment to thank you for your time today sincerely. The taxonomy that we presented to you during this interview is [one that we developed for organizations to more effectively identify privacy threats in their notice and choice interfaces/the LINDDUN framework that is most related to notice and choice]. The goal of this study is to compare a framework that we developed to LINDDUN regarding threat identification in notice and choice. Your contribution is incredibly valuable to our research, and we're grateful for the perspectives you've provided. Before we conclude, do you have any questions about the study, our research, or anything else we discussed today? I'm here to provide any additional information or clarity you might need. [Q&A] You will receive an Amazon gift card of $20 via email within a week to thank you for your participation. We truly appreciate the time and effort you've put into today's session. Have a wonderful day!

B Instruction Sheet

B.1 Examine Privacy Notice (Task A)

- Explore the platform to find section 9: Cookies & Similar Technologies in the privacy notice.
  - Reflect on your expectations for this section and whether the actual content meets them.
  - Express any thoughts or concerns about the effectiveness and understandability of this section.
- Document any identified privacy issues, providing a description of your findings and thoughts.

B.2 Examine Privacy Choice (Task B)

- Locate the platform's privacy choice page.
  - Discuss your expectations for this page and its alignment with your actual findings.
  - Assess the page's usability and clarity for users.
- Note any privacy issues discovered and share your insights and reflections.

B.3 Examine Advertisement Settings (Task C1 & C2)

- Identify the platform's advertisement settings page(s).
  - Consider your expectations for these pages and whether the pages meet those expectations.
  - Evaluate the understandability and user-friendliness of these pages.
- Record any privacy concerns found in sections C1 and C2, elaborating on your analysis and viewpoints.

C *UsersFirst* Taxonomy

Notice & Choice Threats with 3 categories.

x.NC.x threats apply to both Notice and Choice; **x.N.x** threats apply to Notice only; **x.C.x** threats are applicable to Choice only.

You can click on any underlined headers/labels to directly access the definition, evaluation questions, and examples of specific categories or threats.

Threat Category	Notice	Choice
1. Delivery	*[1.NC.1]* Difficult to Locate *[1.NC.2]* Ineffective Timing *[1.NC.3]* Ineffective Channel *[1.NC.4]* Decoupled Notice and Choice *[1.NC.5]* Lack of Centralized Dashboard	
		[1.C.1] Lack of Choice for Certain Channels *[1.C.2]* Difficult to Modify One's Choices
2. Language & Content	*[2.NC.1]* Unnecessarily Lengthy Text *[2.NC.2]* Mismatched Notice Statement and Choice Implementation *[2.NC.3]* Contradictory Statement(s) *[2.NC.4]* Unclear Statement(s) *[2.NC.5]* Inconsistent Terminology *[2.NC.6]* Difficult to Understand *[2.NC.7]* ManipulativeStatement(s)	
		[2.C.1] Less Privacy Protective Defaults *[2.C.2]* Consequences not adequately explained *[2.C.3]* No or Inadequate Feedback *[2.C.4]* Confirmshaming
3. Presentation & Design	*[3.NC.1]* Poorly Designed/Organized Notices and Choices *[3.NC.2]* Distracting Visual/Audio Effects	
	[3.N.1] Too Many Embedded Links	*[3.C.1]* Inadequate Granularity *[3.C.2]* Excessive Choice Options *[3.C.3]* Unequal Paths to Different Privacy Protective Levels *[3.C.4]* Visually Manipulative Design *[3.C.5]* Unexpected Choice Alteration *[3.C.6]* Confusing Buttons/Toggles/Checkbox

1. Delivery

Threats in the delivery category are related to the effective delivery of a privacy notice or choice.

[1.NC] Delivery Notice & Choice Threats

[1.NC.1] Difficult to Locate

Definition:

Refers to when users are unaware of the presence or find it difficult to locate the privacy notice or choice of a system/service (regardless of the delivery channel).

Evaluation Question(s):

- Are the users **unaware of the presence** of a privacy notice or choice for the system/service?
- Do the users **find it challenging to locate** the privacy notice or choice of the system/service? Consider:
  - Can users locate the privacy notice or choice within a **reasonable amount of time**?
  - Are choices located on the **main page** of a website?
  - Does the system employ a **visually misleading interface** that intends to hide/make less salient the links that lead to privacy notices or choice?

Examples:

- Privacy notice for the IOT sensor is available on the company's website, but the users are not aware of it.
- The user needs to access the website's directory 8 levels deep to locate the privacy choice.
- It takes the user 5 minutes to actively locate the privacy notice or choice on the website.

[1.NC.2] Ineffective Timing

Definition:

Refers to user ignorance caused due to privacy notices or choices being presented at inopportune timing.

Evaluation Question(s):

- Does the timing of the notice or choice **impede the user's capacity** to comprehend the privacy notice or choice?

Example(s):

- The privacy notice is presented to the user during the app installation stage after the sign-up process when it's unlikely for users to pay enough attention.

[1.NC.3] Ineffective Channel

Definition:

- A channel for delivering privacy notices/choices refers to the platform or device through which users communicate.
- Ineffective Channel refers to privacy notice/choice delivery that neglects the use of the primary channel when technically feasible.

Evaluation Question(s):

- Is the privacy notice **delivered through an effective channel**?
    - **Effective**
        - Privacy notices/choices are provided outside the primary system or service if the primary system does not have an effective channel for providing a notice.
        - For example, IoT devices, wearables, etc., may provide a privacy notice/choice through the mobile app used to configure the device.
        - Privacy notices/choices are provided via public channels if the identity of the user is unknown. Eg. public notices for surveillance cameras.
    - **Ineffective**
        - E-commerce websites that do not display a privacy notice/choice change on their website but only send users an email notification.
        - Smart speakers cannot accept voice commands to convey a privacy notice via audio and instead require users to look up privacy notices on a website.

[1.NC.4] Decoupled Notice & Choice

Definition:

Refers to situations where either no corresponding choice is provided for certain data practices included in the notice, or it is difficult to locate the corresponding choice.

Evaluation Question(s):

- **Notice-Choice Alignment**: Are users presented with each notice followed by its corresponding choices?
- **Choice Accessibility from Notice**: Are choices available corresponding to notices easy to find? (i.e., are there direct links I can click on in the notice that can successfully lead me to its corresponding choices?)

[1.NC.5] Lack of Centralized Dashboard

Definition:

Refers to whether or not the user has a singular centralized place (e.g., website, IoT devices, privacy dashboard, etc) to find all privacy notices and submit their privacy choices.

Evaluation Question(s):

- Does the user **need to visit multiple locations** to access information on data practices or submit their privacy preferences for a specific system/choice?

Example(s):

- The system implements a privacy notice page, several privacy policy pages, and some pages detailing state privacy laws in a scattered and disconnected manner.

[1.C] Delivery Choice Threats

[1.C.1] Lack of Choice for Certain Channels

Definition:

- A channel for delivering privacy choices refers to the platform or device through which users communicate.
- Refers to not being able to edit privacy choices for some channels and having to switch to other channels.

Evaluation Question(s):

- Does the user have to inconveniently switch to other channels when they want to change their privacy settings?

Example(s):

- A user have to go to a website to change their privacy setting after finding out it's not achievable in their mobile app?

[1.C.2] Difficult to Modify One's Choice

Definition:

Refers to whether the system offers the capability and/or options for users to modify their choices after the choice has been submitted to the system, and if it is easy for users to carry out that modification process.

Evaluation Question(s):

- Does the system/service **prevent the user from re-modifying or retracting** a privacy preference after submission?
- How long it takes for an average user to find the places to initiate choice modification, and can the average user find it at all?

2. Language & Content

Threats in the language & content category are related to the content/statements presented in the privacy notice or choice.

[2.NC] Language & Content Notice & Choice Threats

[2.NC.1] Unnecessarily Lengthy Text

Definition:

Refers to privacy notices or choices that are excessively long and contain a large volume of information without providing an effective summary, table of contents, or other navigation aids.

Evaluation Question(s):

- Is the privacy notice **too long** for users to read and understand the data practices?
  - Is there an effective summary, table of contents, or other navigation aids to allow users to quickly access critical notice information without reading the entire policy?
- Is the length of the privacy notice justified by its content?
- Does the Choice page include **so much text** that users may feel overwhelmed?
- Is it required of users to read **excessive amounts of content** in order to become knowledgeable enough to make decisions?

[2.NC.2] Mismatched Notice Statement and Choice Implementation

Definition:

Refers to statements in the privacy notice on choice implementation that are **not consistent** with the system's actual choice implementation.

Evaluation Question(s):

- If a notice indicates that there is a way for users to control certain data practices, is that achievable

in the choice interfaces?

Examples:

- Statement - “Users are able to withdraw their consent to share their personal information.”
    - Actual practice - There is no privacy choice on the website that allows users to withdraw their consent.

[2.NC.3] Contradictory Statement

Definition:

Refers to conflicting statements within the notice/choice about the same data practice(s).

Evaluation Question(s):

- Does the privacy notice/choice include contradictory statements?

Examples:

- We do not collect personal data, though we do collect email addresses from users during registration.

[2.NC.4] Unclear Statement

Definition:

Refers to the use of unclear or imprecise words or phrases in privacy notices/choices, leading to potential confusion, ambiguity, unclearness, or multiple interpretations.

Evaluation Question(s):

- Are there **hedging words** in the privacy notice/choice? (e.g., may, would, possible, could, etc.)
- Do the terms used in the notice/choice have **multiple possible meanings** or interpretations?
- Does the notice/choice make it clear enough **whom they are referring to** when discussing different parties involved with certain data practices, such as third parties?

Examples:

- Are there any ambiguous words in the privacy notice/choice?
- We **may** collect and process your data for internal or external marketing purposes
- Your information **may be** used to improve our services
- We’ll be sharing your data with **third parties** *(which third party?)*

[2.NC.5] Inconsistent Terminology

Definition:

Refers to the use of different terms throughout the notice/choice to describe the same concept or data type.

Evaluation Question(s):

- Does the privacy notice/choice exhibit inconsistency by **using different terms interchangeably** for the same concept or type of data?

Examples:

- ‘opt-out’ vs ‘unsubscribe’
- ‘data sharing’ vs ‘data disclosure’

[2.NC.6] Difficult to Understand

Definition:

- Refers to the use of language in a privacy notice or choice that makes it challenging for the intended audience to understand the content. This can involve the use of jargon, overly long or complex sentences, or incorrectly assuming the reader's level of preexisting knowledge.

Evaluation Question(s):

- Does the privacy notice/choice text contain:
  - Legal jargon/technical terminologies/slang words/acronyms, difficult to understand for average readers?
  - An overwhelming amount of legal clauses or subclauses?
  - References to laws or regulations without explanation?
- Does the privacy notice/choice use examples and analogies to clarify or explain complex concepts?
- How **effectively** can users understand the intended meaning of each choice?
- Are the sentences in the choices **clear and straightforward**, or do they contain convoluted language that may be difficult for users to grasp?

Examples:

- Legal jargon
  - "In the event of a **force majeure** event, we shall not be liable…"
  - "**Notwithstanding** anything to the contrary **herein**, we reserve the right to retain your data…."

[2.NC.7] ManipulativeStatement(s)

Definition:

Refers to the use of subtle language to manipulate users into taking less privacy-protective actions.

Evaluation(s):

Does the systems' privacy notice and choice include statements that **manipulatively associate less privacy-protective actions with positive outcomes,** such as improved user experience, benefits for others or society, or other desirable results?

Example(s):

- Instead of saying "share your data," a nudged version might be phrased as "enhance your experience by sharing your data."

[2.C] Language & Content Choice Threats

[2.C.1] Less Privacy Protective Defaults

Definition:

Refers to setting the default values of privacy attributes to less protected ones.

Evaluation Question(s):

- Does the system or service offer default privacy settings that are **less privacy-protective** than other options, requiring users to adjust them for higher levels of protection manually?

[2.C.2] Consequences not adequately explained

Definition:

Refers to the system not providing a clear explanation regarding the consequences of each choice.

Evaluation Question(s):

- Does the system provide insights into the **likely outcomes** of each user's choice?
- Does the system offer **individualized recommendations** or **detailed descriptions** for available choices?

Examples:

- "By using the Service, you agree to the collection and use of information in accordance with this policy."

[2.C.3] No or Inadequate Feedback

Definition:

Refers to no feedback or insufficient feedback in terms of whether the privacy settings have been successfully updated after users submit their choices or the current state of privacy settings.

Refers to a choice mechanism neglecting to offer meaningful feedback to a user regarding:

- The full effect of privacy choice selection
- The current state of privacy settings

Evaluation Question(s):

- Does the system/service neglect to **confirm to users that their privacy preferences** have been successfully updated? (e.g., popup notices, icons, emails, etc.)
- Does the system/service promptly offer **transparent and timely feedback** to users?
- Can users readily **check the current state** of their privacy settings?

[2.C.4] Confirmshaming

Definition:

Refers to using guilt-based, manipulative language or content to influence users toward an action.

Evaluation Question(s):

- Does the system encourage users to make a particular choice, potentially inducing feelings of guilt or discomfort if they do not engage with the service or feature offered?
- Is the **language** used for motivation **biased**, potentially evoking negative emotions like guilt and shame rather than remaining neutral?

3. Presentation & Design

Threats in the presentation & design category are related to presentation, format, or design of privacy notice or choice.

[3.NC] Presentation & Design Notice and Choice Threats

[3.NC.1] Poorly Designed/Organized Notices or Choices

Definition:

Refers to privacy notices/choices that are poorly formatted and thereby fail to effectively convey important information to the users.

Evaluation Question(s):

- Is the layout of the privacy notice/choices clear and organized?
- Does the notice/choice use **clear headings, bullet points, or other visual aids** to enhance readability?
- Is the **font size, style, and color scheme** chosen for the notice/choice easy to read?
- Is the privacy notice/choice optimized for **both desktop and mobile users** in terms of design and formatting?
- Are the choices interfaces with **poorly selected color contrast** that decreases their readability?

[3.NC.2] Distracting Visual/Audio Effects

Definition:

Refers to visual or audio presentations (e.g., additional text, sounds, videos) that could disturb users when they read the privacy notice or make privacy decisions.

Evaluation Question(s):

- Are users capable of reading privacy notices and making privacy choices **without being disturbed by any designs** implemented by the system?

[3.N] Presentation & Design Notice Threats

[3.N.1] Too Many Embedded Links

Definition:

Refers to privacy notices that contain too many links in their text, which results in providing less meaningful information in the main body and increases users' burden by requiring them to click on multiple links for more information.

Evaluation Question(s):

- Does the privacy notice include many links to the degree that users are **incapable of eliciting useful information** without actually visiting the links?
- Are the links in the privacy notice embedded in a way such that users will click on them?

[3.C] Presentation & Design Choice Threats

[3.C.1] Inadequate Granularity

Definition:

- Refers to sets of user privacy choice options that do not reflect user expectations regarding a reasonable range of possible preferences in a given context.

Evaluation Question(s):

- Are the available options for users **overly extreme** and with no middle ground, therefore not capable of being aligned with users' needs?
- Are users **exclusively offered two distinct options** without any middle ground or customization possibilities? (e.g., Accept/Decline, Yes/No)

    - Note: If the situation logically necessitates only two possible options and allows users to communicate their privacy preferences effectively using binary choices, this threat can be ignored.

Examples:

- In an IoT environment, for instance, primary users are sometimes presented with two extreme choices: either allow their guests to use their accounts with full access or have them use guest accounts that have strict restrictions regarding the functions they can use.
- For location based services, having the option to share location only while actively using the application rather than allowing the application to constantly track location.

[3.C.2] Excessive Choice Options

Definition:

Refers to whether the system provides too many choices or requires too much effort for users to make effective decisions or exercise certain privacy rights.

Evaluation Question(s):

- Does the system/service overwhelm users with **an excessive number of privacy choices**, potentially impeding their decision-making process?
- Does the system/service force users to **fill in an excessive number of elements/forms/requirements,** potentially putting too much burden on users (e.g., deletion request)?

[3.C.3] Unequal Paths to Different Privacy Protective Levels

Definition:

Refers to a type of deceptive/dark pattern (*dark patterns: trick users into taking an action that is not in their best interest*) in which the users need to take more steps for privacy-protective action compared to accepting all the default settings (which may lead to privacy invasion).

Evaluation Question(s):

- Does taking the privacy-protective action (e.g., managing/ rejecting cookies) take the same amount of effort/steps as taking the privacy-invasive action (e.g., accepting all the cookie settings)?

[3.C.4] Visually Manipulative Design

Definition:

Refers to a type of deceptive/dark pattern where the interface encourages users to take invasive privacy actions by using particular enticing font or button colors, different font or button sizes, or manipulative bundling and layouts.

Evaluation Question(s):

- Does the visual representation subtly **encourage users**, particularly average users, to **select the less privacy-protective option**?

[3.C.5] Unexpected Choice Alteration

Definition:

Refers to when user choice leads to unexpected consequences, especially with regard to other choices.

Evaluation Question(s):

- Does the system inform users of the consequences of their choices, including automatic changes to other settings?
- Are users clearly notified about all changes to their settings, even those they did not directly select?
- Do presets or hierarchical choice interfaces clearly convey the choices associated with each top-level setting?

[3.C.6] Confusing Buttons/Toggles/Checkbox

Definition:

Refers to situations in which privacy choice options are largely based on users' own interpretation, resulting in users being incapable of expressing their preferences as desired.

Evaluation Question(s):

- Are the choices implemented effectively so that **users can tell if a choice indicates "yes" or "no" by the design** (color, style, text labels, etc.)?
- Can users **easily understand** what will be selected once the button, toggles, or checkbox has been set to a particular value?

Example(s):

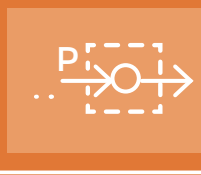
- For a cookie choice – a green button could be "accept all" or be more privacy-protective based on its design
- When toggles are not labeled with words, it can be difficult to determine their state based only on position or color
- A cookie banner with an unlabelled X or close button does not convey to users what choice is made when they close the banner

D LINDDUN PRO

NO TRANSPARENCY

Hotspot

INBOUND FLOW/ ...
PROCESS WITH
PERSONAL DATA



Threat source

ORGANIZATIONAL

The data subject is insufficiently informed about the collection and further processing of their personal data.

1. Are personal data being collected and/or processed?
2. Is the data subject insufficiently informed about this collection or further processing activities?

- It is unclear to the data subject with which third parties their data will be shared because no notice is provided.
- The data subject was not informed at collection time about the purpose or the retention period of their personal data.
- The notice provided to the data subject was not written in clear and plain language.

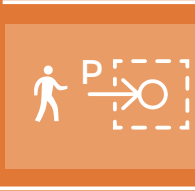
- Transparency (notice) is a data subject right [GDPR].
- This threat can be triggered at collection time, but applies to all further processing activities.

- Both collection directly from the data subject and collection from a third party should be communicated to the data subject.

NO USER-FRIENDLY PRIVACY CONTROL

Hotspot

INBOUND FLOW
BY **USER** WITH
PERSONAL DATA



Threat source

ORGANIZATIONAL

The system does not provide user-friendly privacy control.

(e.g. default settings, feedback & awareness tools, user-friendly privacy preferences support)

1. Does the system process personal data?
2. Are there no privacy-preserving default settings and/or is there no user-friendly support for the data subject to set privacy preferences or provide awareness information?

- When visiting a website for the first time, it requires navigation through several tabs and slide several switches to set the cookie settings and other privacy preferences (no privacy by default, no user-friendliness).
- When posting on social media, the post is made public by default (no privacy by default, no feedback and awareness tools to educate the data subject on the consequences of these privacy settings).

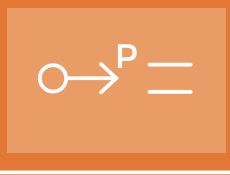
- Mainly relevant for systems directly collecting personal data from users (or indirectly through communication metadata) and systems targeted at sharing personal data (e.g. social media).

- Privacy-friendly settings should be the default.
- The data subject should be able to easily control his privacy settings.
- Raising privacy awareness can nudge the data subject into a more privacy-aware behavior.

NO ACCESS OR PORTABILITY

Hotspot

STORE PERSONAL DATA



Threat source

ORGANIZATIONAL

The data subject does not have access to their personal data or is not able to port personal data to another platform/vendor/...

1. Are personal data being stored?
2. Is a process lacking that can extract data (in both a human understandable and computer interpretable format) for an individual data subject?

- A wearable device's sensor data are sent to a lifestyle tracking app, but the user is unable to access the statistics and deduced information based on his data that the app has collected and processed.
- A data subject does not have the means to request their data, neither directly through the system, or indirectly (e.g. a request to a helpdesk which generates the requested data set and forwards it to the data subject.).

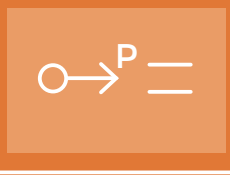
- Access and data portability is a data subject right [GDPR].
- Does not apply to data that infringes other data subjects' privacy, corporate secrets, etc.

- This access can also exist outside of the system. (e.g. a helpdesk request)
- Data portability only involves personal data that was provided directly by the data subject.

NO ERASURE OR RECTIFICATION

Hotspot

STORE PERSONAL DATA



Threat source

ORGANIZATIONAL

The data subject cannot request erasure or rectification of personal data.

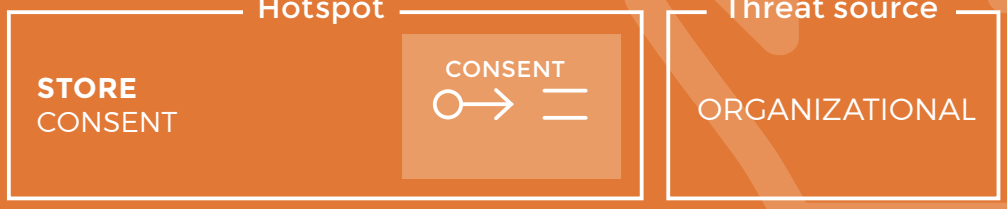
1. Are personal data being stored?
2. Is a process lacking that can delete and rectify (a subset of) data related to a specific data subject?

- A data subject requests deletion of his social media data, but only his account is revoked, the actual data remain.
- The data subject moved and wants to update their address in the system, but is unable to.

- Request of erasure and rectification is a data subject right (under certain conditions) [GDPR].
- Deletion can only be requested 'within reason'.

- The request can also be made outside of the system (e.g. helpdesk), it however should always be technically feasible to delete the data.
- A data subject can only request rectification of data to increase accuracy.

INSUFFICIENT CONSENT SUPPORT



Data subject consents are are not properly taken into account by the relevant processes and data are still being processed with a missing or withdrawn consent.

1. Does the system require user consent to process personal data? Does the system fail to take the consent into account?
2. Are means lacking for the data subject to explicitly provide or withdraw consent or are the consents not taken into account for processing operations (e.g. access control)?

Wearables data are being used for a research study, but

- The data subject has never given his consent
- The data subject decides to revoke his consent, but there is no technical revocation support
- The system only stops collecting new data but continues its analysis with the previously collected data.

- A consent should always be freely given and thus also be revocable. The system should thus support the consequences of a newly obtained or revoked consent.

- This can be a feature directly available to the data subject or it can be done indirectly (e.g. helpdesk). In both cases, an internal process should be in place to support this.