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

School of Computer Science, Carnegie Mellon University

Study Motivation

- Privacy regulations increasingly emphasize usability of privacy notice and choice (N&C) interfaces
- But N&C interfaces are often lengthy, full of jargon, and difficult to find and exercise choices
- A privacy threat modeling framework is needed to help identify and mitigate N&C threats

Research Questions

Do privacy practitioners who use the UsersFirst Taxonomy identify more user-oriented threats associated with privacy N&C than they identify

1. without the use of a taxonomy?
2. with the LINDDUN PRO taxonomy's unawareness category?

Study Design

- Semi-structured in-person interviews with 14 participants with prior experience in privacy
- Between-subjects (**LINDDUN PRO** VS **UsersFirst Taxonomy**) and within-subjects design (**No Taxonomy** VS **With Taxonomy**)
- Participants were asked to identify privacy N&C threats on four privacy notice and choice pages on a well-known ecommerce platform, initially **without taxonomy** and then **with one of two randomly assigned taxonomies**
- We identified **21 threats**, including **14** identified by the authors and **7** additionally identified by participants

Results

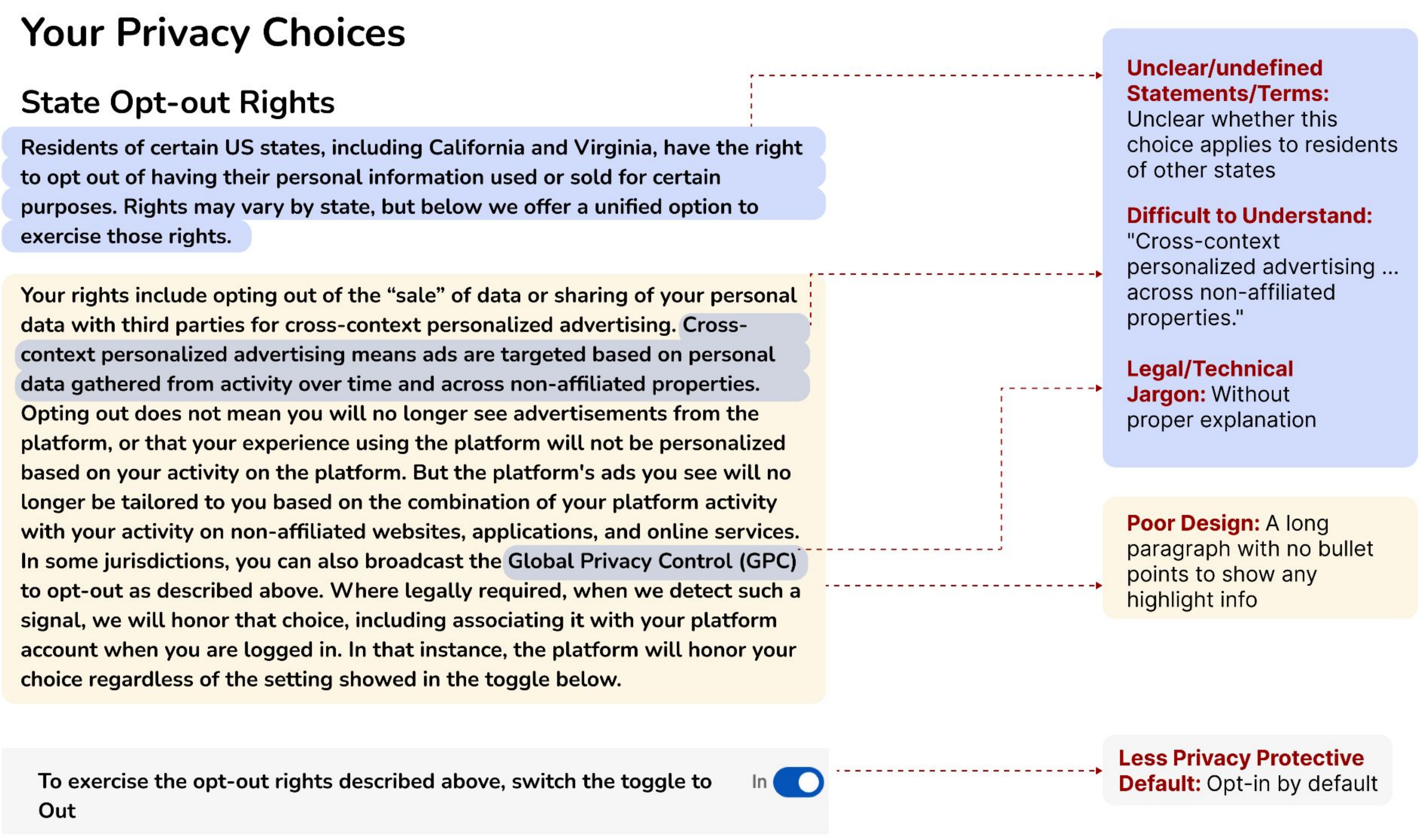
Summary of UsersFirst Taxonomy

Threat Category	Notice	Choice
Delivery	Difficult to Locate, Ineffective Timing, Ineffective Channel, Decoupled Notice and Choice, Lack of Centralized Dashboard	
		Lack of Choice for Certain Channels, Difficult to Modify One's Choices
Language & Content	Unnecessarily Lengthy Text, Mismatched Notice Statement and Choice Implementation, Contradictory Statement(s), Unclear Statement(s), Inconsistent Terminology, Difficult to Understand, Manipulative Statement(s)	
		Less Privacy Protective Defaults, Consequences Not Adequately Explained, No or Inadequate Feedback, Confirmshaming
Presentation & Design	Poorly Designed/Organized Notices or Choices, Distracting Visual/Audio Effects	
	Too Many Embedded Links	Ineffective Granularity, Excessive Choices Options, Unequal Paths to Different Privacy Protective Levels, Visually Manipulative Design, Unexpected Choice Alteration, Confusing Buttons/Toggles/Checkbox

Summary of LINDDUN PRO Unawareness

Unawareness	No Transparency, No User-Friendly Privacy Control, No Access or Portability, No Erasure or Rectification, Insufficient Consent Support

Privacy threats found on the platform's Privacy Choices Page



Your Privacy Choices

State Opt-out Rights

Residents of certain US states, including California and Virginia, have the right to opt out of having their personal information used or sold for certain purposes. Rights may vary by state, but below we offer a unified option to exercise those rights.

Your rights include opting out of the "sale" of data or sharing of your personal data with third parties for cross-context personalized advertising. Cross-context personalized advertising means ads are targeted based on personal data gathered from activity over time and across non-affiliated properties. Opting out does not mean you will no longer see advertisements from the platform, or that your experience using the platform will not be personalized based on your activity on the platform. But the platform's ads you see will no longer be tailored to you based on the combination of your platform activity with your activity on non-affiliated websites, applications, and online services. In some jurisdictions, you can also broadcast the Global Privacy Control (GPC) to opt-out as described above. Where legally required, when we detect such a signal, we will honor that choice, including associating it with your platform account when you are logged in. In that instance, the platform will honor your choice regardless of the setting showed in the toggle below.

To exercise the opt-out rights described above, switch the toggle to Out

Unclear/undefined Statements/Terms: Unclear whether this choice applies to residents of other states

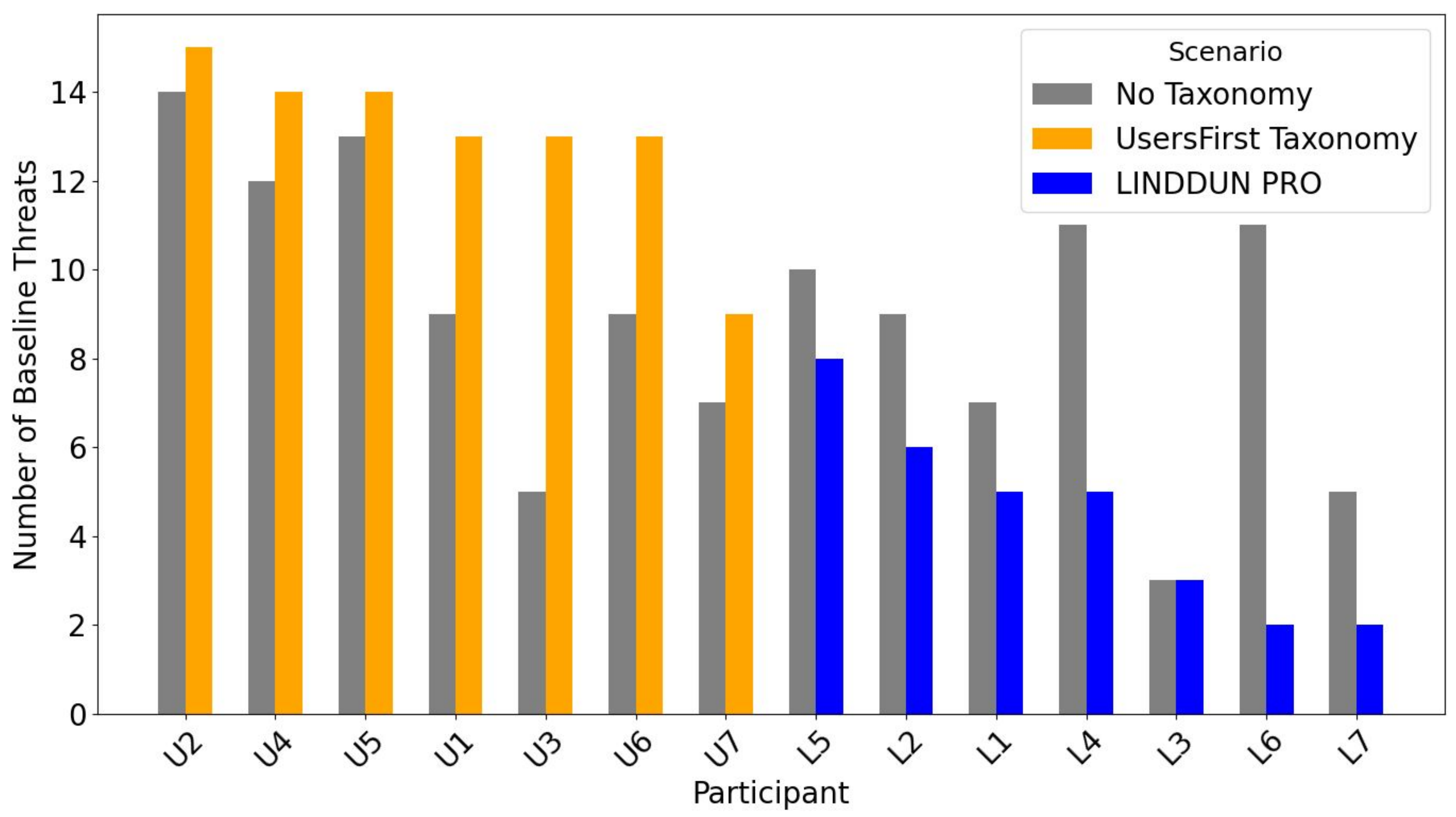
Difficult to Understand: "Cross-context personalized advertising ... across non-affiliated properties."

Legal/Technical Jargon: Without proper explanation

Poor Design: A long paragraph with no bullet points to show any highlight info

Less Privacy Protective Default: Opt-in by default

Number of Threats identified by Participants



- UsersFirst Taxonomy enabled all participants to identify more threats than when using no-taxonomy and most participants (6 out of 7) to identify more than half of the 21 threats we identified
- UsersFirst Taxonomy helped participants identify more threats (μ = 13) compared to no-taxonomy (μ = 9.86) and LINDDUN PRO (μ = 4.43)
- 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
- UsersFirst participants found the taxonomy easy to use, guided their thought processes and helped capture threats missed in the no-taxonomy scenario
- LINDDUN PRO users commented that understanding the taxonomy enough to be able to apply it requires considerable effort

Acknowledgements

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