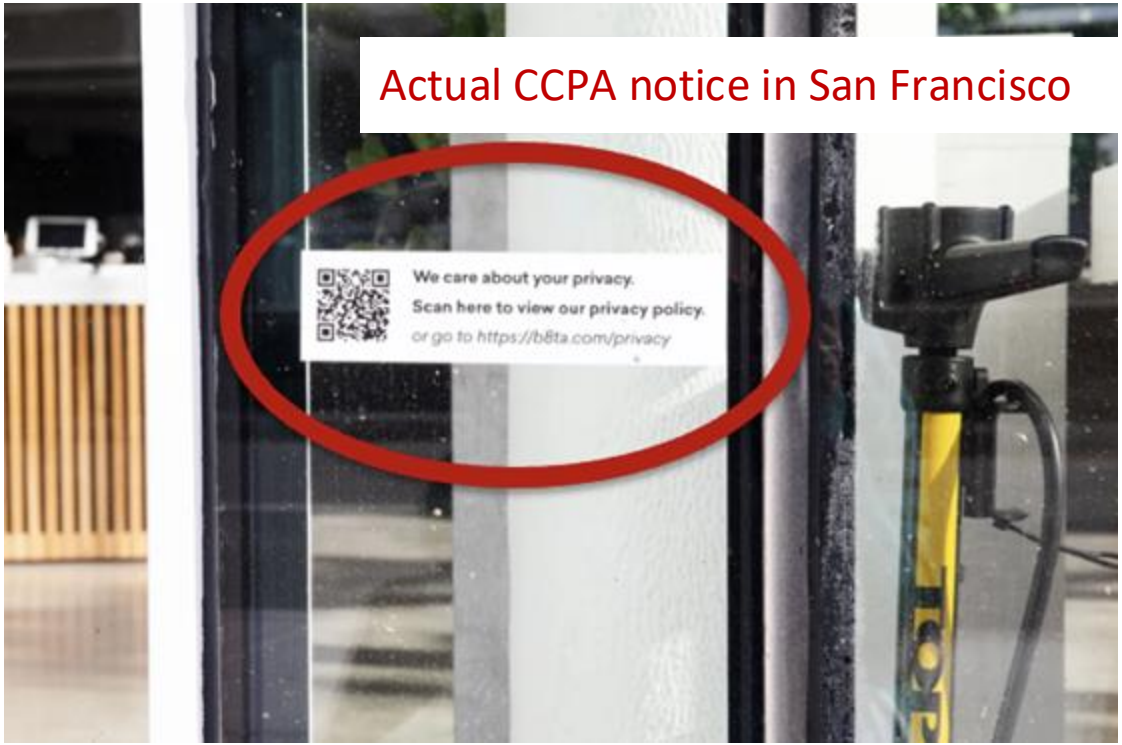
UsersFirst: A User-Centric Threat Modeling Framework for Privacy Notice and Choice

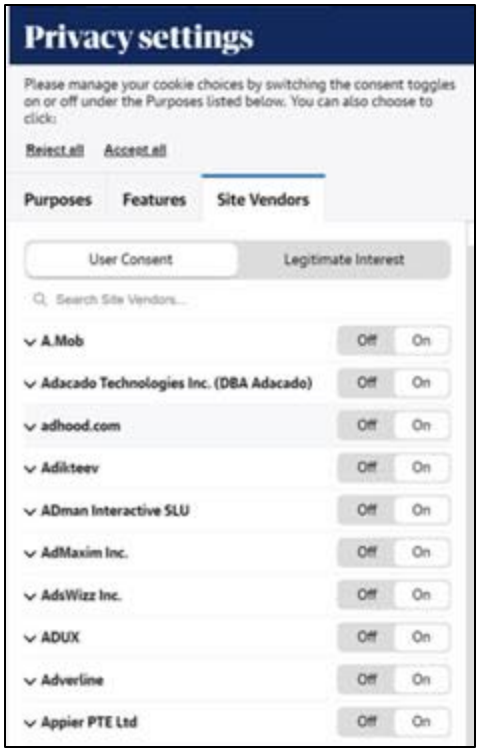
Norman Sadeh and Lorrie Cranor

Carnegie Mellon University
privacy
ENGINEERING

How helpful is this?



…Or this?



Regulatory requirements

- Growing number of notice and choice requirements (e.g. CCPA, GDPR)
- Increasingly including user-oriented considerations
  - Clear and conspicuous “Do Not Sell or Share My Personal Information” (CCPA)
  - Consent must be freely given specific, informed and unambiguous (GDPR)
  - “A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out” (CCPA) - provision against manipulative patterns

Inadequate privacy notices and choices are privacy threats

- Because they do not meet regulatory standards
- Or because they just fall short
  - They do no meet a company's standards
  - Users complain
  - Logs show that users fail to engage
  - User studies indicate that notice and choice are manipulative, difficult to access or confusing users

Source: https://www.boredpanda.com/useless-object-design-the-unusable-katerina-kamprani/

Privacy threat modeling movement

- Desire for a framework that enables organizations to
  - Systematically analyze a product/service for privacy threats
  - Identify available mitigations
  - Document the process
- Existing frameworks
  - LINDDUN
  - MITRE Panoptic
- Inspired by security threat modeling
- Ongoing work developing similar frameworks for AI threats

Need to supplement existing frameworks

- Identify, categorize and mitigate user-oriented threats associated with ineffective privacy notices and choices

Requirements for a new framework

- Informed by research in user-centered design and usable privacy
- Support
  - analysis of existing products/services and the design of new ones
  - systematic analysis and mitigation of user-oriented threats and documentation
  - organizations in different jurisdictions and with varied resources
- Practical: helpful but not overwhelming

Source:https://www.cio.com/article/228328/what-is-togaf-an-enterprise-architecture-methodology-for-business.html

What do we mean by user?

- Users are data subjects who are the target users of privacy notices and choices
- Not just traditional users of the product or service
- Also those whose data is collected and who should be informed and possibly be able to restrict (or consent to) the collection and use of their data

What do we mean by user-oriented threat?

- User-oriented threats are notices/choices that are
  - Difficult to discover and/or use
  - Difficult to comprehend
  - Provide inadequate choices
  - Manipulative

UsersFirst overview

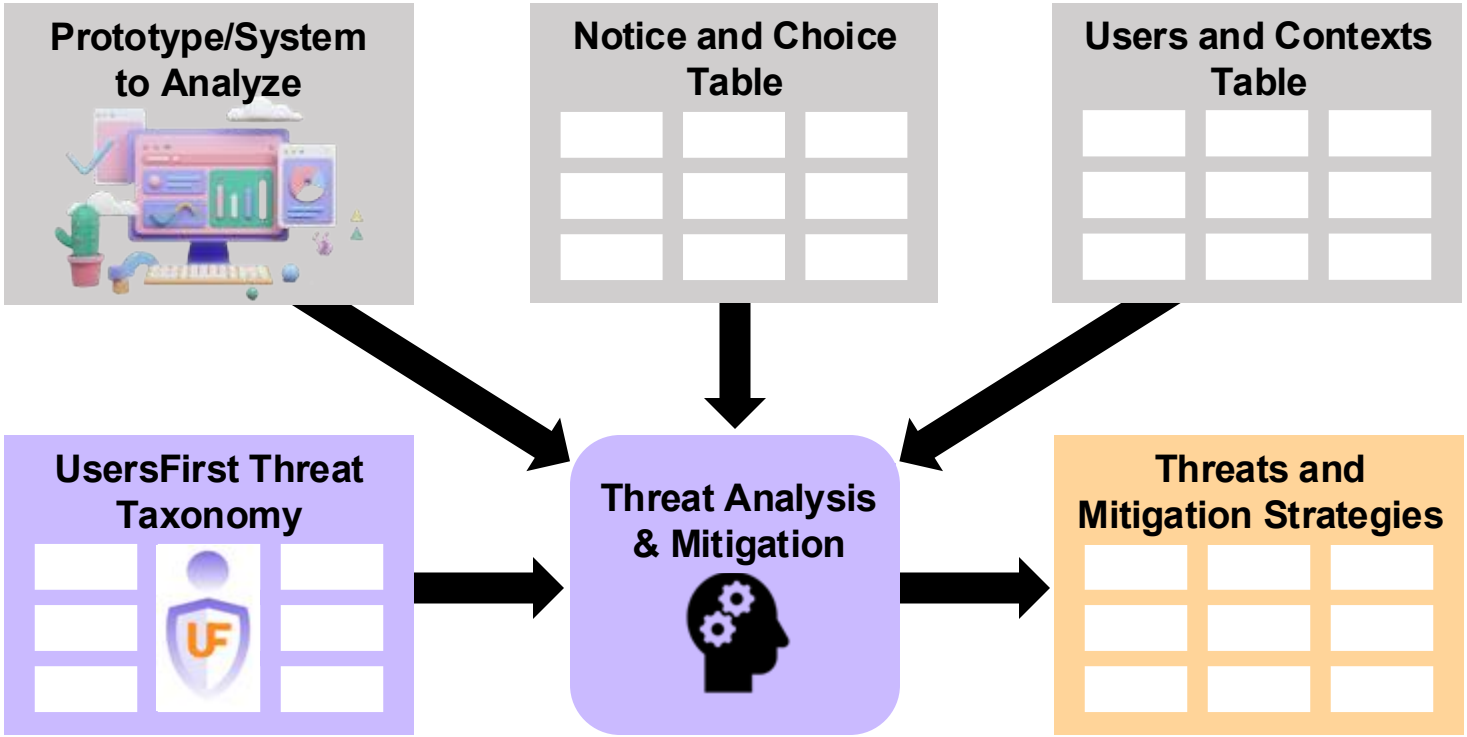
Design phase

- Identify needed notices and choices
- Identify contexts and touchpoints
- Map notices and choices onto touchpoints*
- Design each notice and choice (Skip if existing product/service)

Analysis phase

- Analyze notices and choices for presence of possible threats using threat taxonomy
- Identify possible mitigation strategies

UsersFirst threat analysis phase



Threat taxonomy

Discovery & Use

[DU.1] Nonexistent or difficult to locate or access

[DU.2] Ineffective timing

[DU.3] Scattered presentation

[DU.4] Poor organization, formatting, or presentation

[DU.5] Dysfunctional components

Comprehension

[C.1] Contradictory statement(s)

[C.2] Inconsistent terminology

[C.3] Difficult to understand

[C.4] Consequences not adequately explained

[C.5*] Inadequate feedback

[C.6*] Confusing buttons/toggles/boxes

Appropriate choices

[AC.1*] Limited choice

[AC.2*] Excessive or redundant choice options

[AC.3*] Difficult to modify previous choices

Manipulative Elements

[ME.1] Manipulative statements

[ME.2] Visually manipulative design

[ME.3*] Asymmetric effort required for different privacy protection levels

[ME.4*] Non-privacy protective defaults

[ME.5*] Unexpected choice alteration

Threat taxonomy tables

Discovery and Use

Threat Names	Evaluation Process and Questions
[DU.1] Nonexistent or Difficult to Locate or Access **[DU.1.1]** Non-existent notice/choice **[DU.1.2]** Notice/choice difficult to locate **[DU.1.3]** Notice/choice difficult to access, ineffective interaction channel	Consider ea… relevant to th… and easy to l…
[DU.2] Ineffective Timing	Consider ea… relevant to th… access/be ex… benefit from i…
[DU.3] Scattered Presentation **[DU.3.1]** Lack of Centralized Management **[DU.3.2]** Decoupled Notice and Choice	Is there a ce… notices (e.g., … privacy policy … of data practi… to these prac… taking a glob… multiple notic…
[DU.4] Poor Organization, Formatting, or Presentation **[DU.4.1]** Lengthy Text that Lacks Structure or Effective Navigation Aids **[DU.4.2]** Too Much Effort to Access Necessary Information (links or layered policy) **[DU.4.3]** Poorly Formatted Notices and Choices **[DU.4.4]** Distracting Presentation Elements	Consider ea… relevant to th… choices easy … through multi… choices poor… distracting pr… or audio elem…
[DU.5] Dysfunctional components (links, buttons, switches, etc.)	Consider ea… implemented… as intended.

Comprehension

Threat Names	Evaluation Process and Questions
[C.1] Contradictory Statement(s) or Implementation(s) **[C.1.1]** Conflicting Statement(s) **[C.1.2]** Mismatched Notice Statement and Choice Implementation	Consider statements made across the e… (global perspective) and determine whe… any contradictions or ambiguities that m… resolved. This could include conflicting … well as mismatches between statement… notices and related choices presented t…
[C.2] Inconsistent Terminology	Consider statements made across the e… (global perspective) and look for possible inconsistencies in terminology (e.g., a no… term and a corresponding choice using a…
[C.3] Difficult to Understand **[C.3.1]** Unclear Terms/Statements **[C.3.2]** Use of Legal or Technical Jargon **[C.3.3]** Use of Complex Language	Consider each context and each notice/c… implemented/designed for that context, a… whether it includes terms or statements t… overly technical, or language that is overt…
[C.4] Consequences not adequately explained	Consider each context and each notice/ … determine whether it does a good enoug… explaining the implications associated wi… practices it discusses and the choices av… when it comes to allowing or restricting t…
[C.5*] Inadequate Feedback	Consider each context and each choice … context, and ensure that the user is given… information to determine whether the opt… recently selected has been recorded and… currently active (including in situations wh… has not modified the initial default).
[C.6*] Confusing Buttons/Toggles/Checkboxes	For each context and each choice in that … consider each button/toggle/checkbox and verify that it … is intuitive and easy to use.

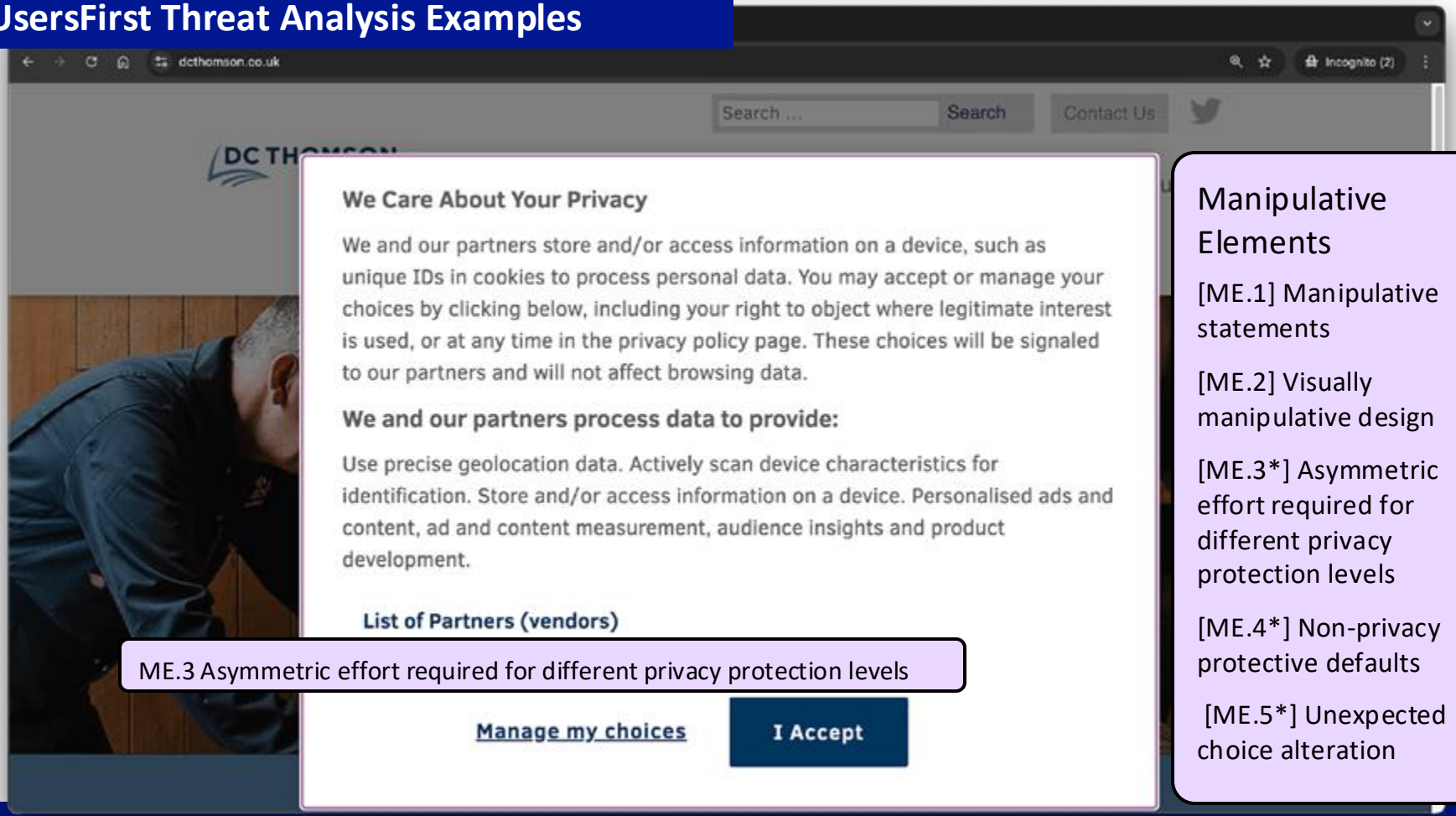
Appropriate Choices

Threat Names	Evaluation Process and Questions
[AC.1*] Limited Choice	Consider each context and each choice and ask whether options users are likely to want in that context are actually available. This includes looking at the granularity of available options.
[AC.2*] Excessive or Redundant Choice Options	Consider each context and each choice in that context and ask whether each choice option is actually useful in that context, or whether some options might be superfluous or redundant. This includes looking at the granularity of available options.
[AC.3*] Difficult to Modify Previous Choices	Consider each context and each choice in that context and make sure that the user can easily modify any selection they have made.

Manipulative Elements

Threat Names	Evaluation Process and Questions
[ME.1] Manipulative Statements	Consider each context and each notice/choice in that context, and ask whether it contains manipulative statements.
[ME.2] Visually Manipulative Design	Consider each context and each notice/choice in that context, and ask whether it contains manipulative visual elements.
[ME.3*] Asymmetric Effort Required for Different Privacy Protection Levels	Consider each context and each choice in that context, and check whether some options are artificially more complex to select than others - with the likely effect of manipulating the user's decisions.
[ME.4*] Non-Privacy Protective Defaults	Consider each context and each choice in that context and check whether defaults are privacy protective.
[ME.5*] Unexpected Choice Alteration	Consider each context and each choice in that context, and determine whether selecting some options might automatically impact other choices without the user's awareness or consent.

UsersFirst Threat Analysis Examples



Manipulative Elements

[ME.1] Manipulative statements

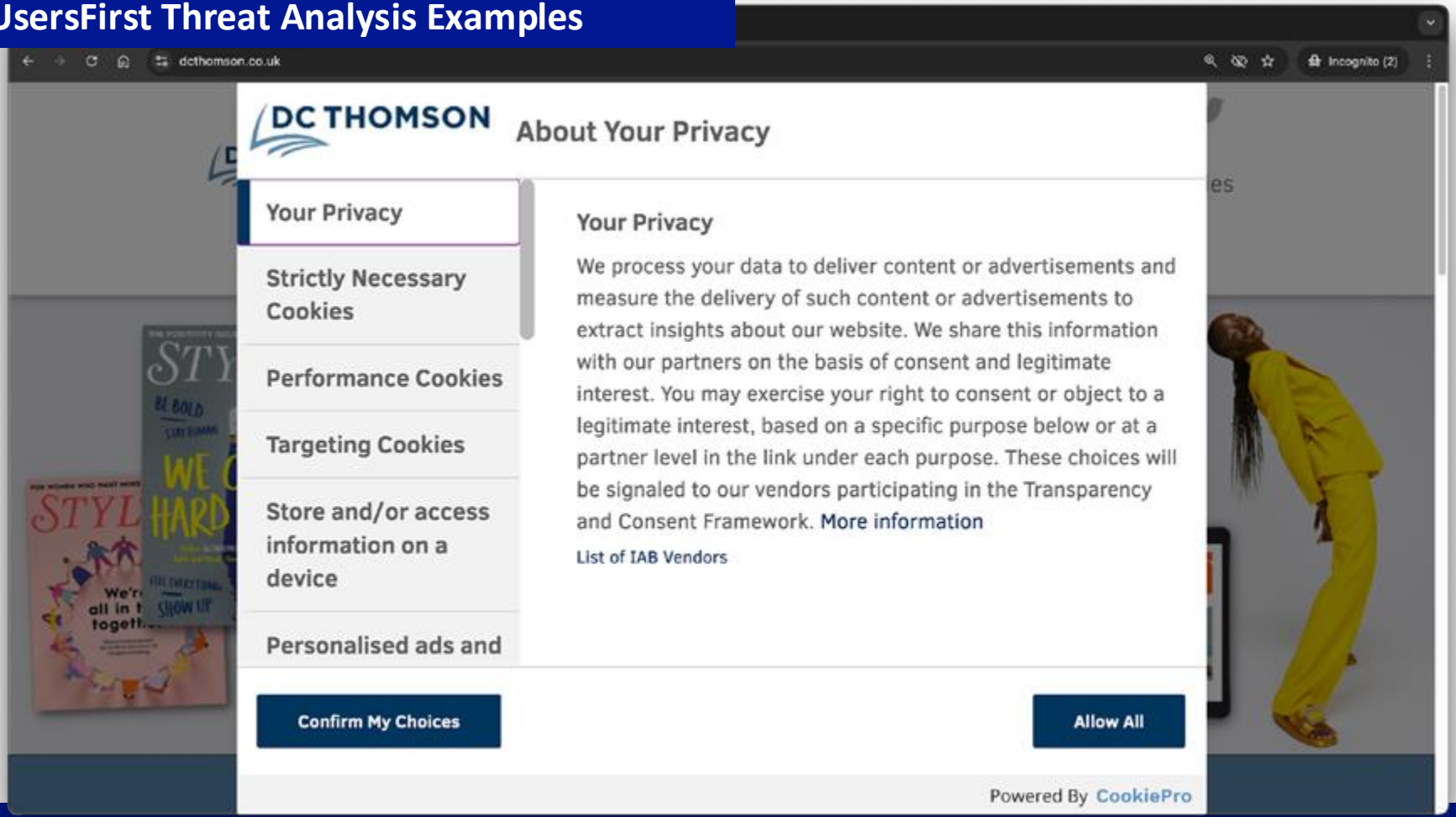
[ME.2] Visually manipulative design

[ME.3*] Asymmetric effort required for different privacy protection levels

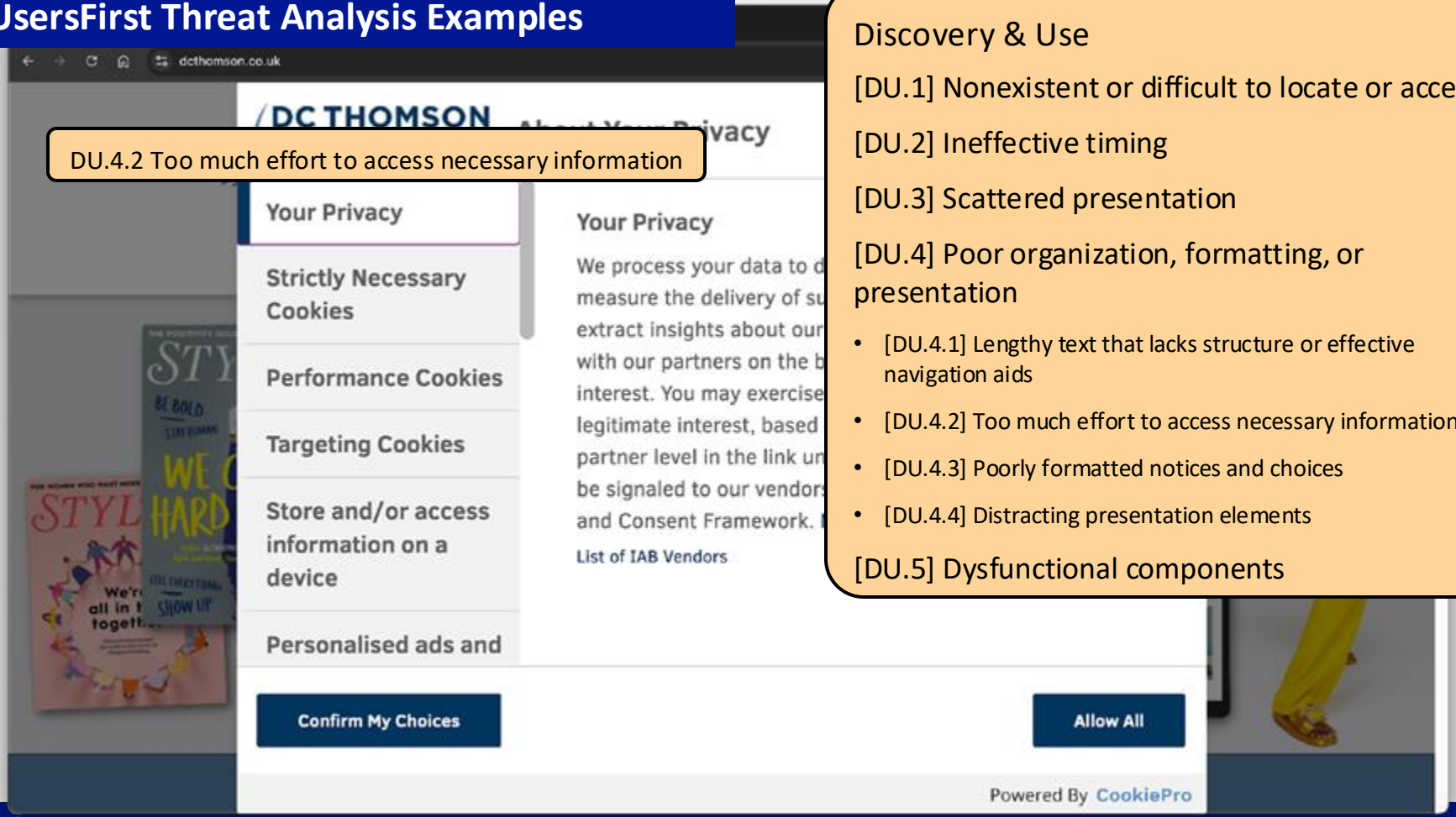
[ME.4*] Non-privacy protective defaults

[ME.5*] Unexpected choice alteration

UsersFirst Threat Analysis Examples



UsersFirst Threat Analysis Examples



DU.4.2 Too much effort to access necessary information

Discovery & Use

[DU.1] Nonexistent or difficult to locate or access

[DU.2] Ineffective timing

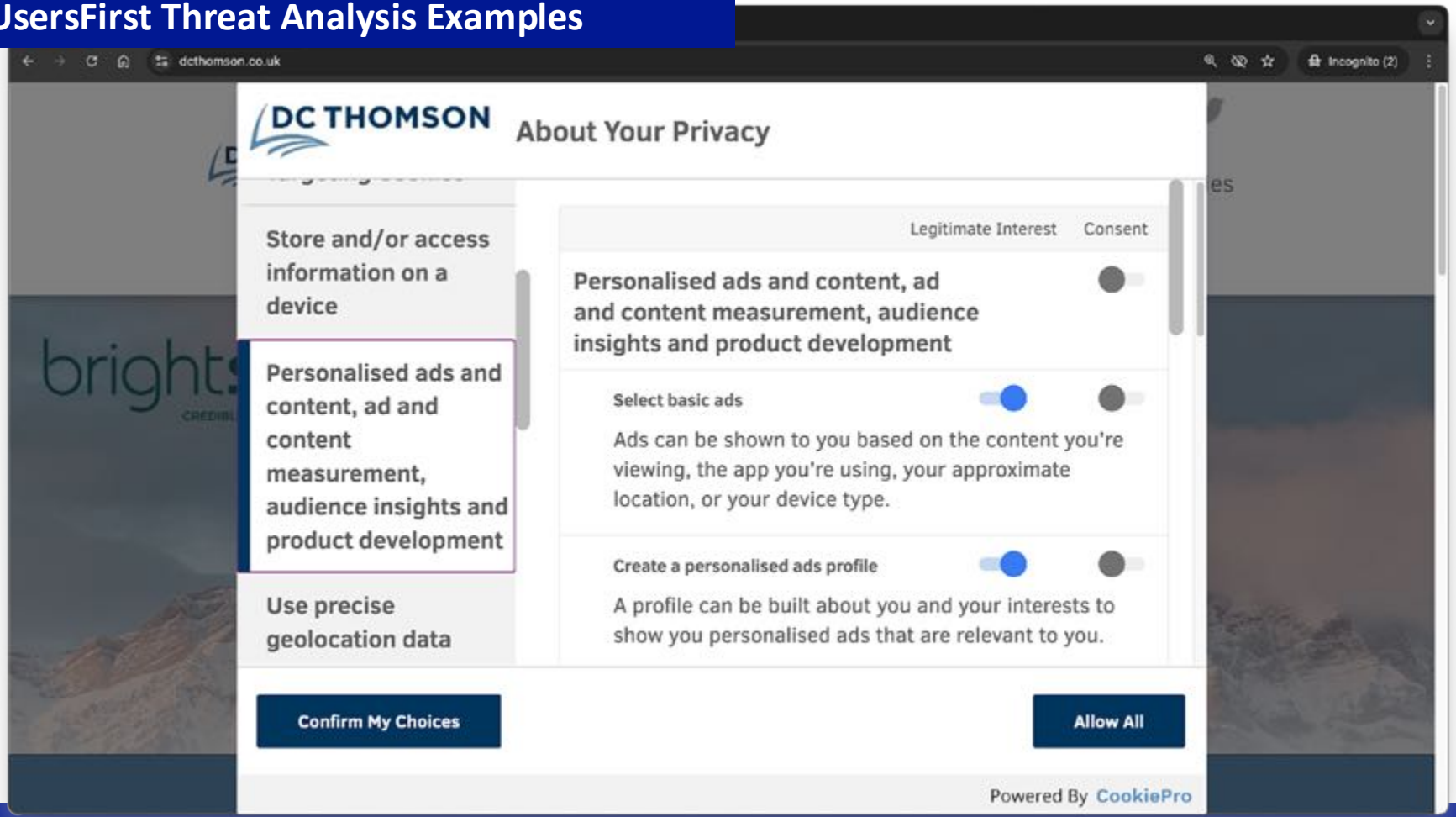
[DU.3] Scattered presentation

[DU.4] Poor organization, formatting, or presentation

- [DU.4.1] Lengthy text that lacks structure or effective navigation aids
- [DU.4.2] Too much effort to access necessary information
- [DU.4.3] Poorly formatted notices and choices
- [DU.4.4] Distracting presentation elements

[DU.5] Dysfunctional components

UsersFirst Threat Analysis Examples



UsersFirst Threat Analysis Examples

Comprehension

[C.1] Contradictory statement(s)

[C.2] Inconsistent terminology

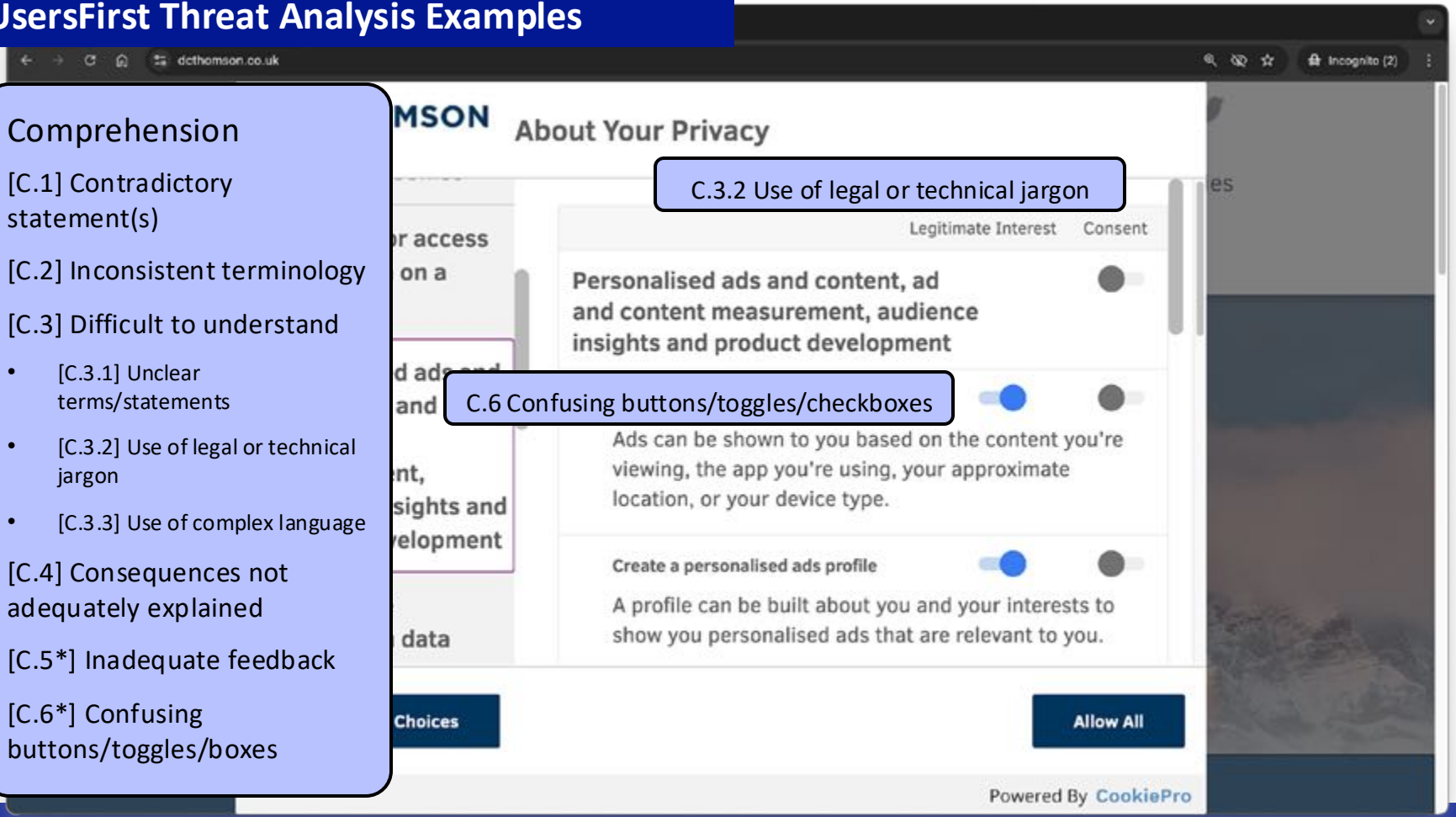
[C.3] Difficult to understand

- [C.3.1] Unclear terms/statements
- [C.3.2] Use of legal or technical jargon
- [C.3.3] Use of complex language

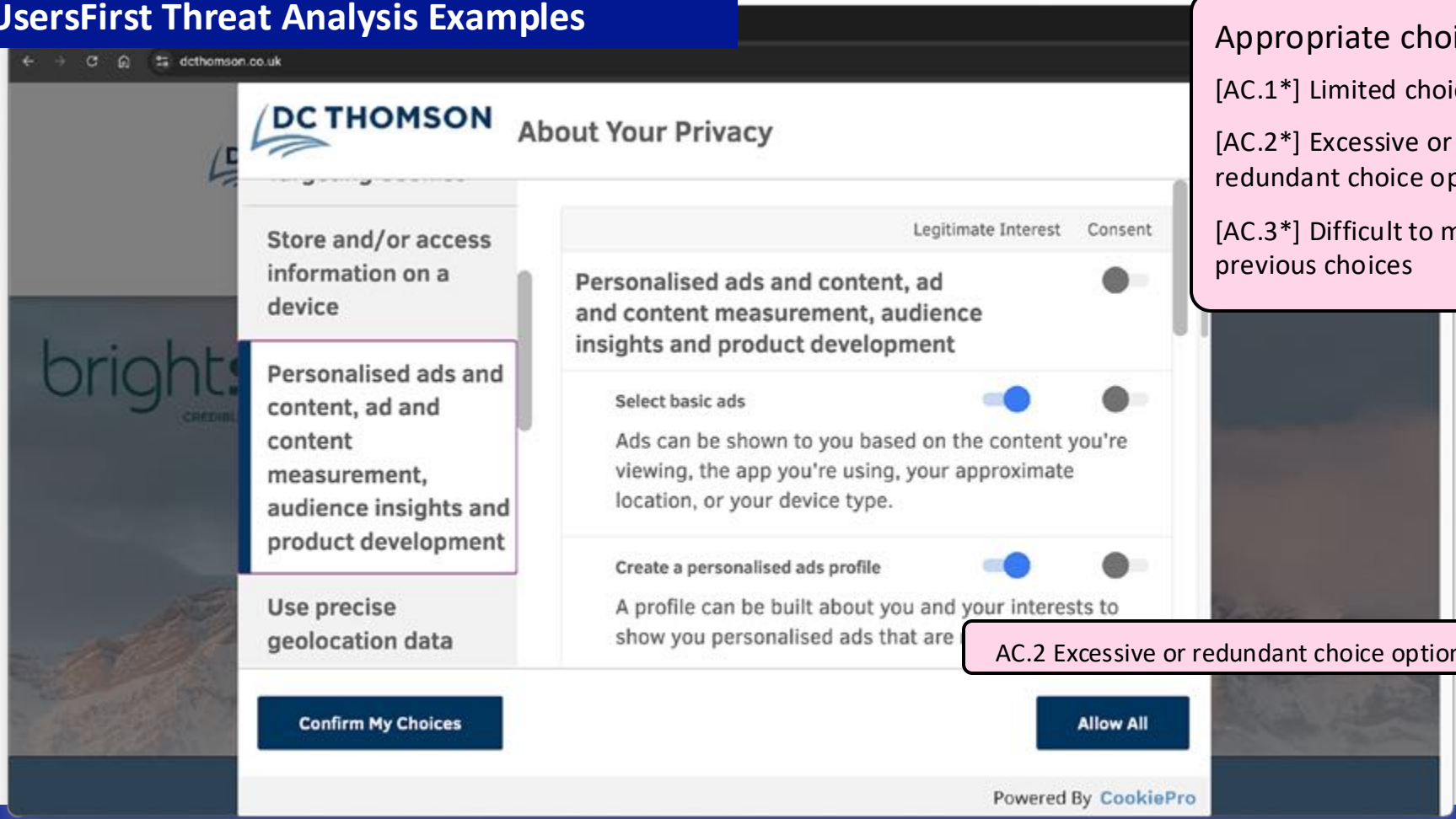
[C.4] Consequences not adequately explained

[C.5*] Inadequate feedback

[C.6*] Confusing buttons/toggles/boxes



UsersFirst Threat Analysis Examples



Appropriate choices

[AC.1*] Limited choice

[AC.2*] Excessive or redundant choice options

[AC.3*] Difficult to modify previous choices

AC.2 Excessive or redundant choice options

Different mitigations for different threats

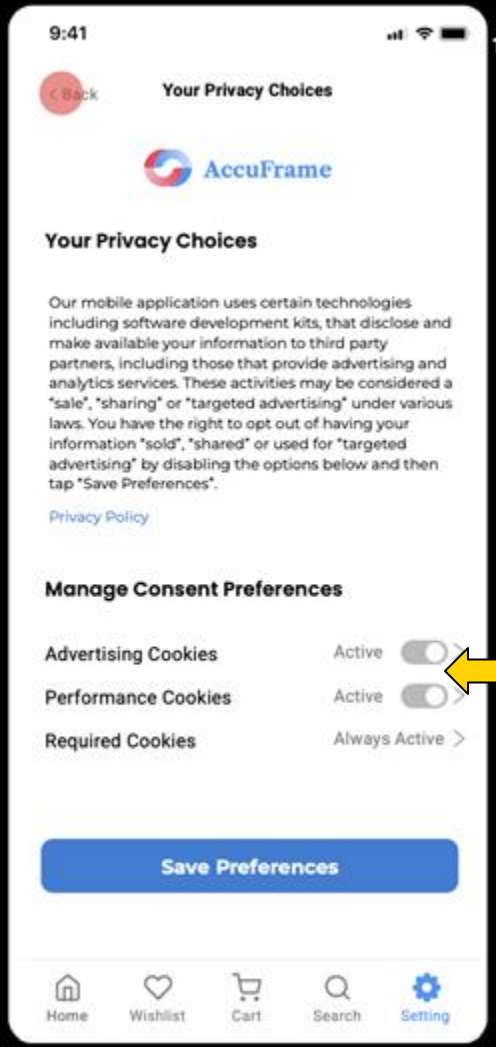
- Discovery and use
  - Introducing a new touchpoint to make accessing notice/choice easier
  - Introducing a dashboard to review data collection and consolidate access to all relevant choices
- Comprehension
  - Simplifying language of a notice or options in a choice
  - Clearly labeling buttons + toggles
  - Ensuring consistent language
- Appropriate choices
  - Changing granularity of choice options
  - Providing clear path for modifying choices
- Manipulative elements
  - Make sure there is an equal path to accept or reject data practice
  - Don’t highlight non-protective choices or make them defaults

Evaluating and refining the taxonomy

- Initial taxonomy developed after extensive review of existing frameworks and notice/choice usability research
- Early in-person interview study
  - 14 privacy students asked to identify notice and choice threats on selected pages of the eBay website
  - Compared no framework, UsersFirst taxonomy, and LINDDUN PRO
  - Found UsersFirst increased participants' success at finding relevant notice and choice threats
- Online interview study
  - 26 privacy professionals and privacy students asked to identify notice and choice threats in 2 fictitious scenarios illustrated by storyboards
  - Compared no framework and UsersFirst taxonomy
  - Participants using taxonomy identified significantly more user-centric threats
- Studies helped us improve taxonomy
- Currently working on more use cases and example materials for website

Goal: Withdrawing consent and agreement for use of virtual try-on tool to protect biometric data

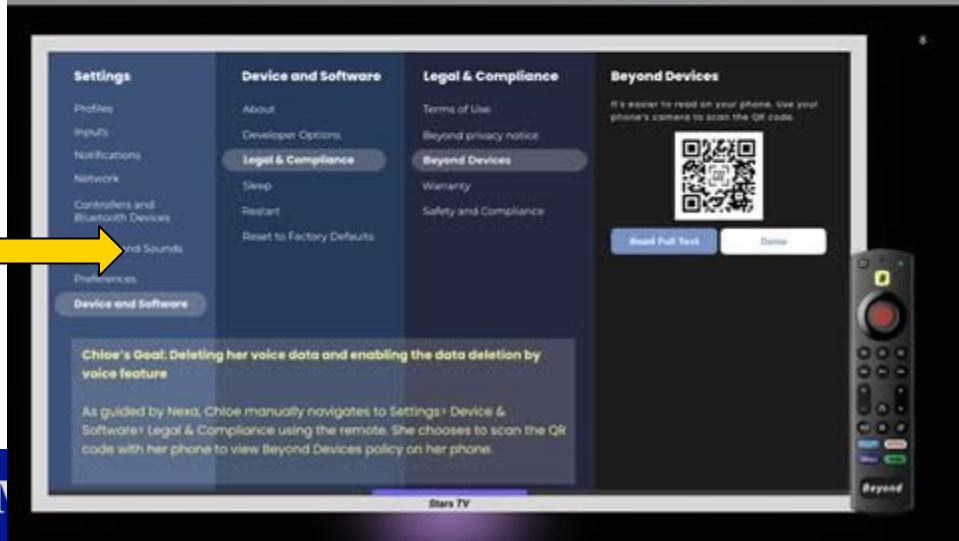
She lands on this page, and is not able to find choices about biometric data.



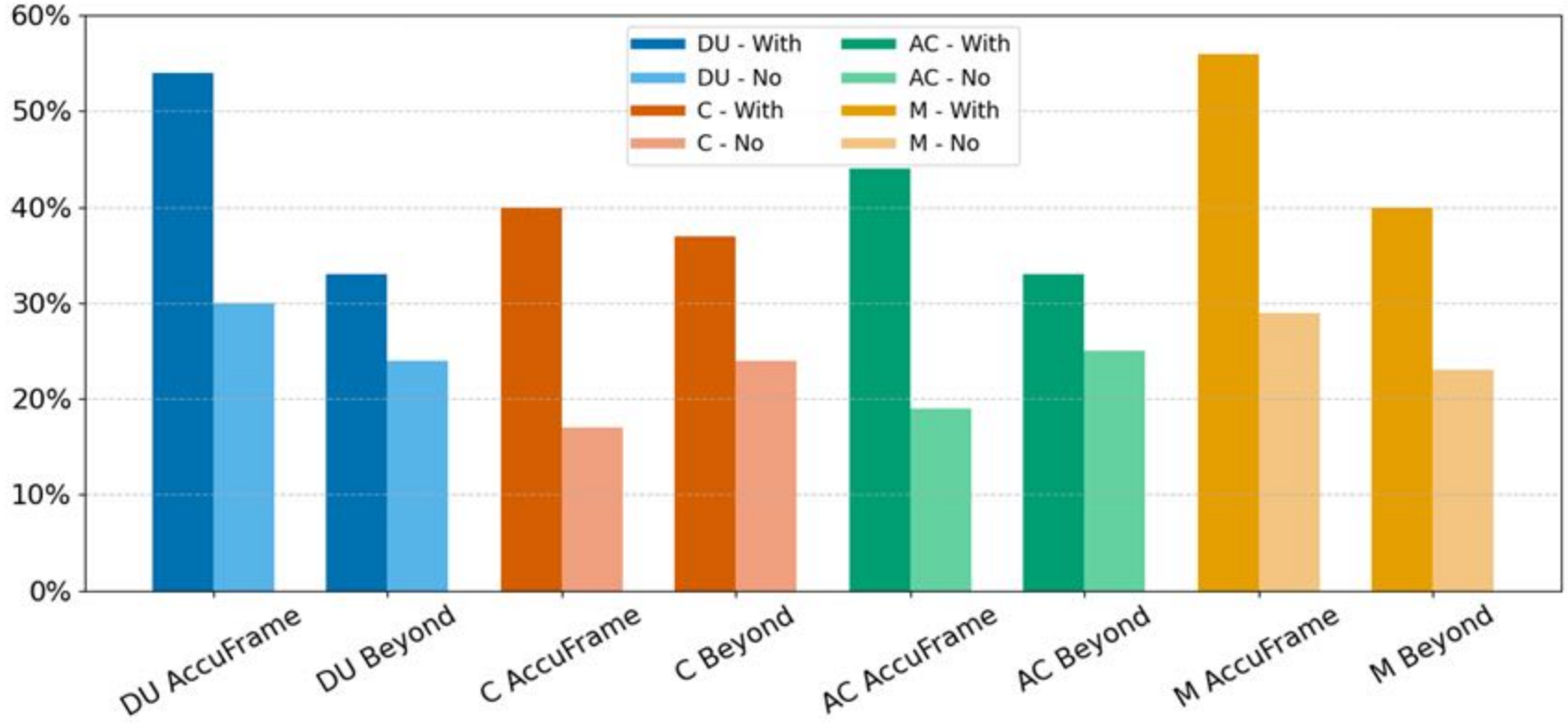
Online study story boards

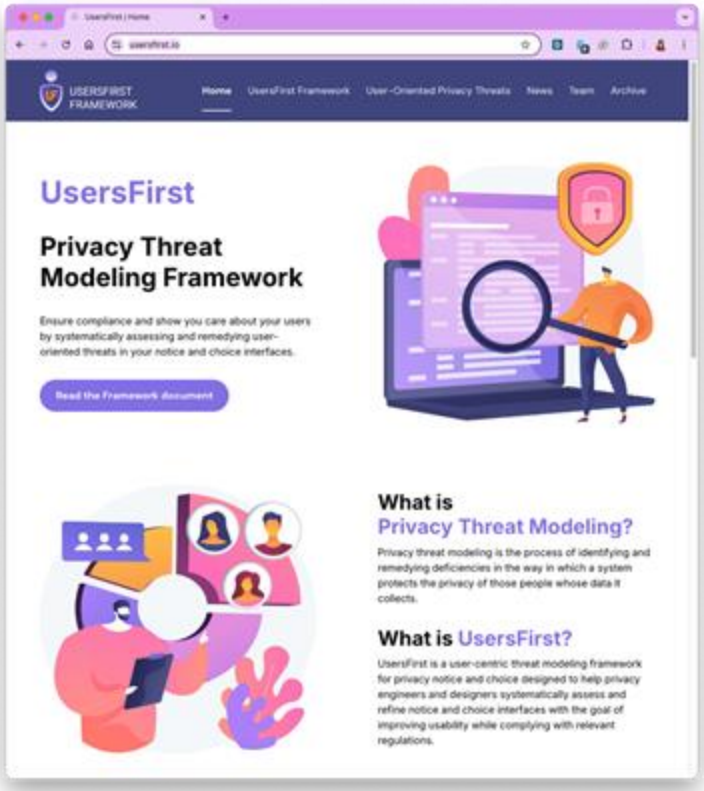
Accuframe

Beyond



Online study results





See **usersfirst.io** for the complete framework, taxonomy, and papers

Norman Sadeh and Lorrie Cranor

Collaborators: Hana Habib, Tian Wang, Alexandra Li, Miguel Rivera- Lanas, Debeshi Ghosh, Sara Patel, Ray Liu, Prahaldh Chandrahasan, Aseem Shrey, Isabel Agadagba, Asmit Nayak

Carnegie Mellon University
privacy
ENGINEERING