Training Developers' Privacy Awareness with Enforcement Cases

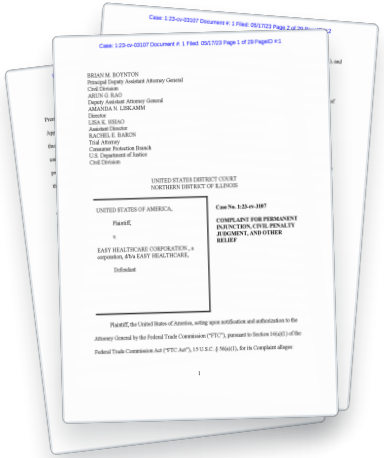
Shao-Yu Chu

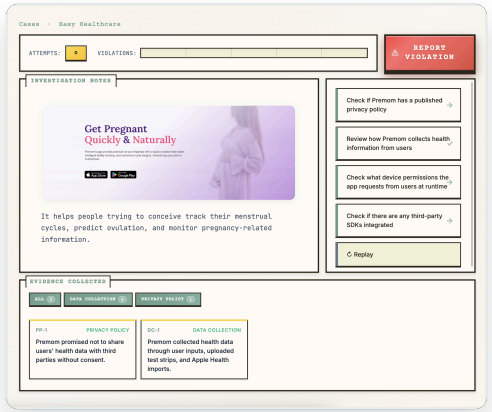
Xu Wang

Haojian Jin

UC San Diego

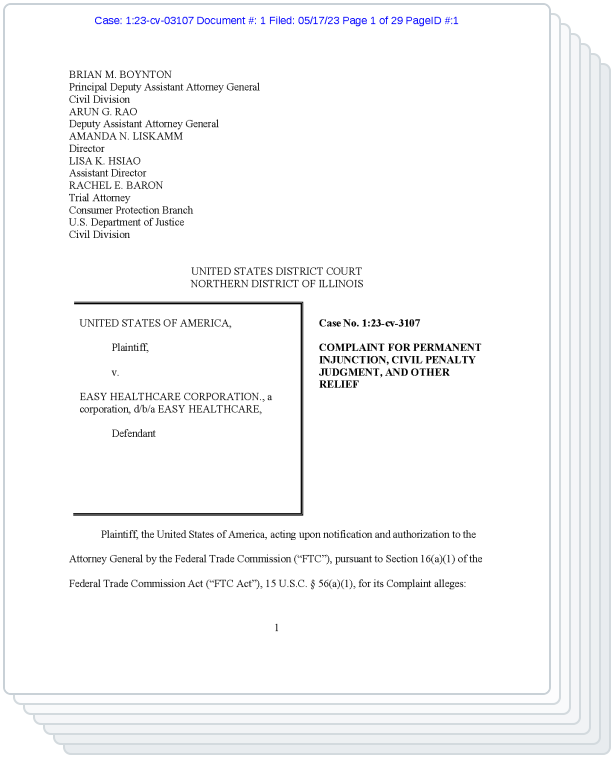
UNIVERSITY OF MICHIGAN





An enforcement case

- **Premom** — a fertility app
- Users log their periods
- The company promised never to share users' health data
- 2023: FTC found it shared with third parties anyway



Case: 1:23-cv-03107 Document #: 1 Filed: 05/17/23 Page 1 of 29 PageID #:1

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division
ARUN G. RAO
Deputy Assistant Attorney General
AMANDA N. LISKAMM
Director
LISA K. HSIAO
Assistant Director
RACHEL E. BARON
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
Civil Division

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

UNITED STATES OF AMERICA,

Plaintiff,

v.

EASY HEALTHCARE CORPORATION., a corporation, d/b/a EASY HEALTHCARE,

Defendant

Case No. 1:23-cv-3107

COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC"), pursuant to Section 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 56(a)(1), for its Complaint alleges:

1

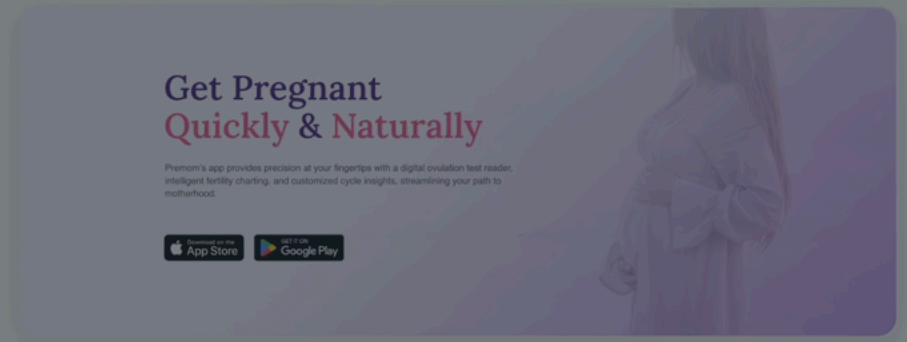
29-page complaint

Cases › Easy Healthcare

ATTEMPTS: 0 VIOLATIONS:

REPORT VIOLATION

INVESTIGATION NOTES



It helps people trying to conceive track their menstrual cycles, predict ovulation, and monitor pregnancy-related information.

- Check if Premom has a published privacy policy →
- Review how Premom collects health information from users →
- Check what device permissions the app requests from users at runtime →
- Check if there are any third-party SDKs integrated →
- ↻ Replay

EVIDENCE COLLECTED

Investigate the c

Navigate the large evidence space

privacy policies, data collection practices, access permissions, SDK integrations, etc.

Learning that sticks

1. Hold attention
2. Figure it out yourself
3. Ground practices in realistic scenarios

Privacy is everyone's job

Developers' decisions shape users' privacy.

But most were never taught to see it.

How do we help developers — and the students who will become them — be more privacy-sensitive?

How developers learn privacy today

Training courses

Concept question

Which best describes **PII**?

a b c d

Scenario question

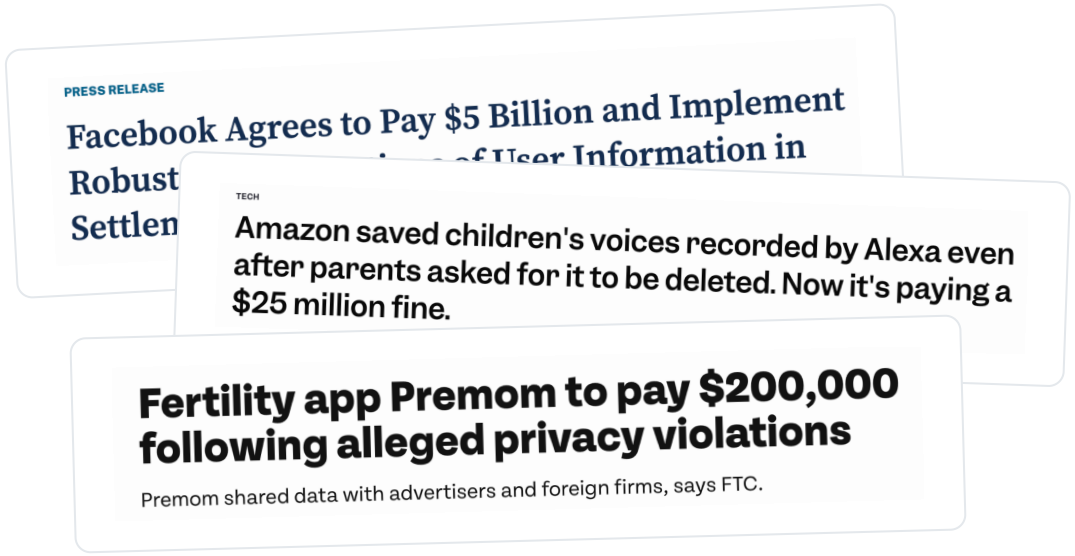
Which violation occurs?

a b c d

1. Not realistic
2. Short attention window

How developers learn privacy today

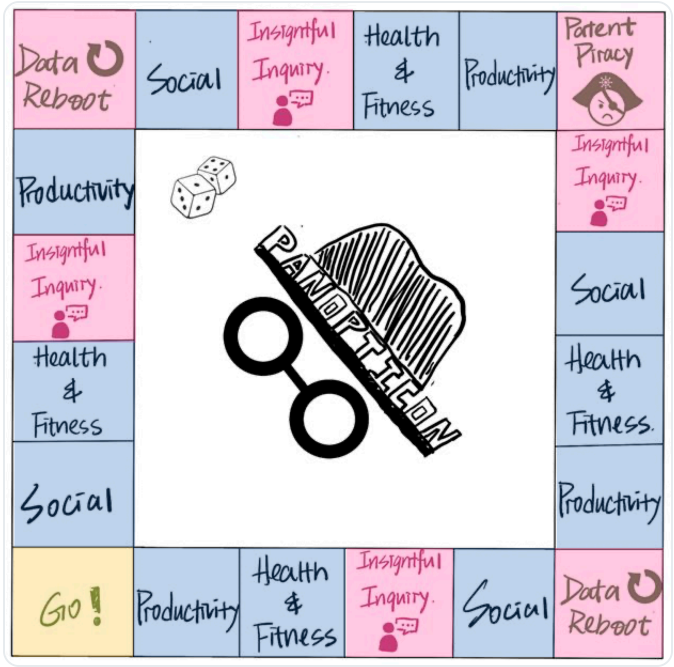
Lessons in the wild



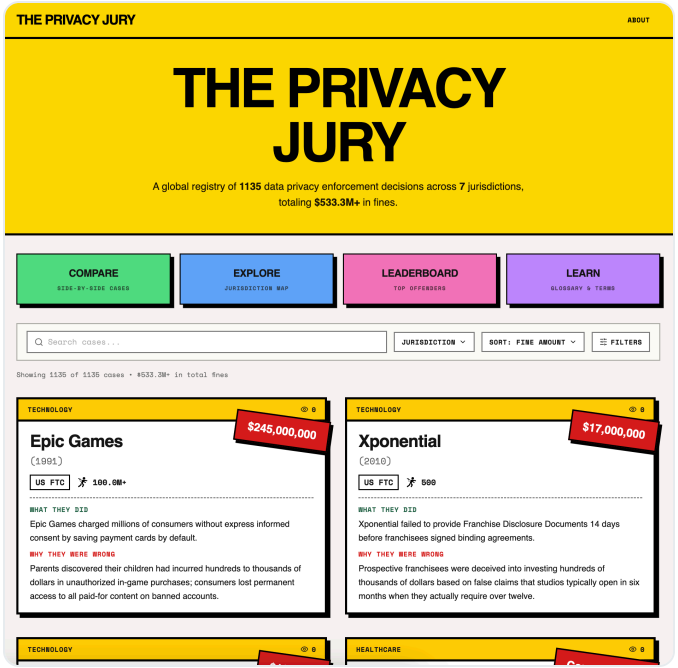
1. Sparse signal
2. Feels like others' problem

Tahaei, M., Frik, A., & Vaniea, K. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. *CHI'21*.

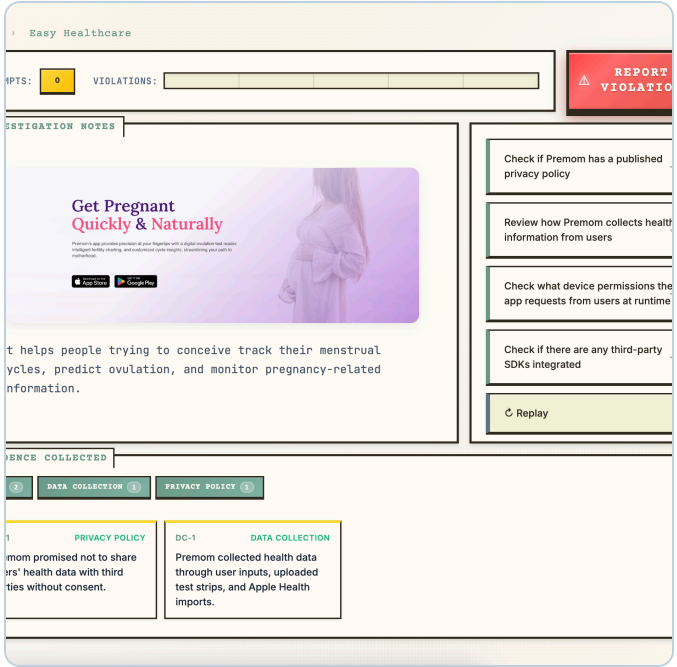
Our work on privacy training for developers



Panopticon



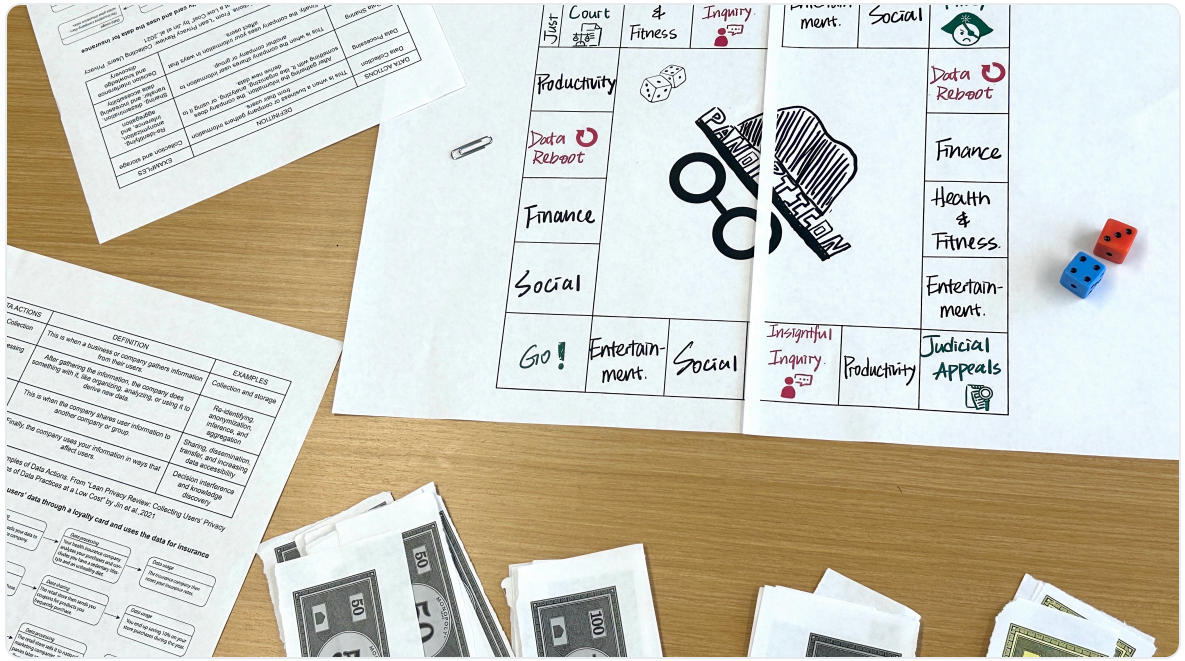
Privacy Jury



Privacy Detective

Panopticon

Board game for teaching privacy design

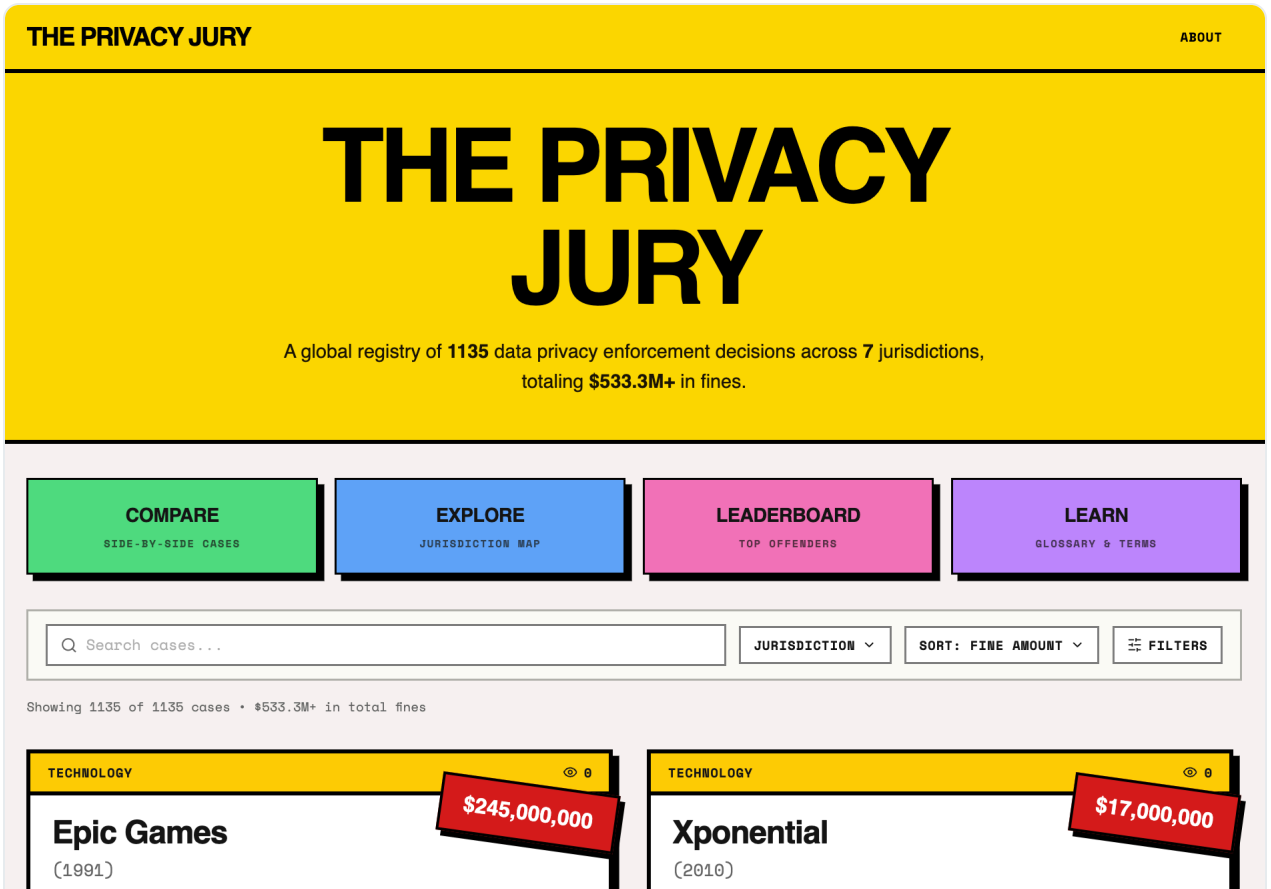


- Monopoly, reimagined as data economy
- Own digital service
- Propose → critique → refine designs

Tian, Y., Chu, S.-Y., Liu, Y., & Jin, H. Panopticon: The design and evaluation of a game that teaches data science students designing privacy. *PoPETs'25*.

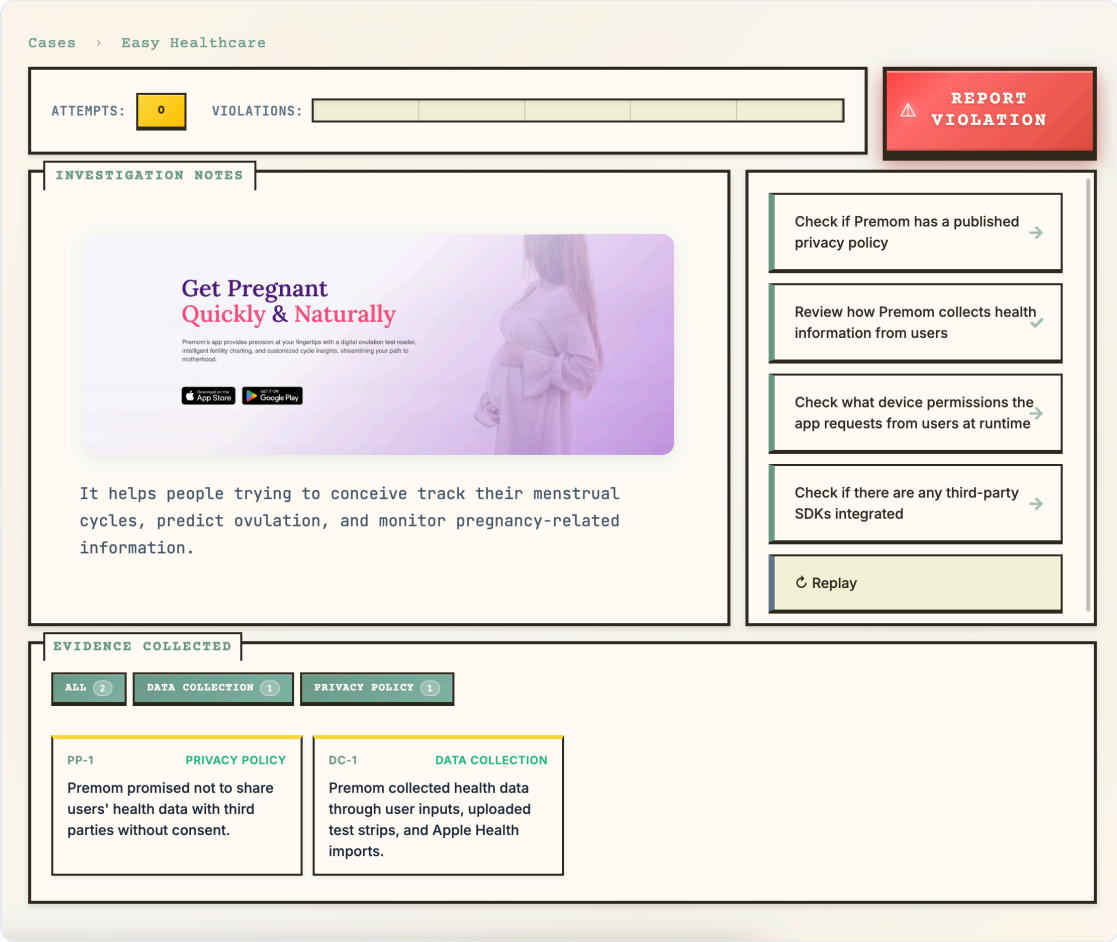
Privacy Jury

A global registry of real privacy enforcement decisions



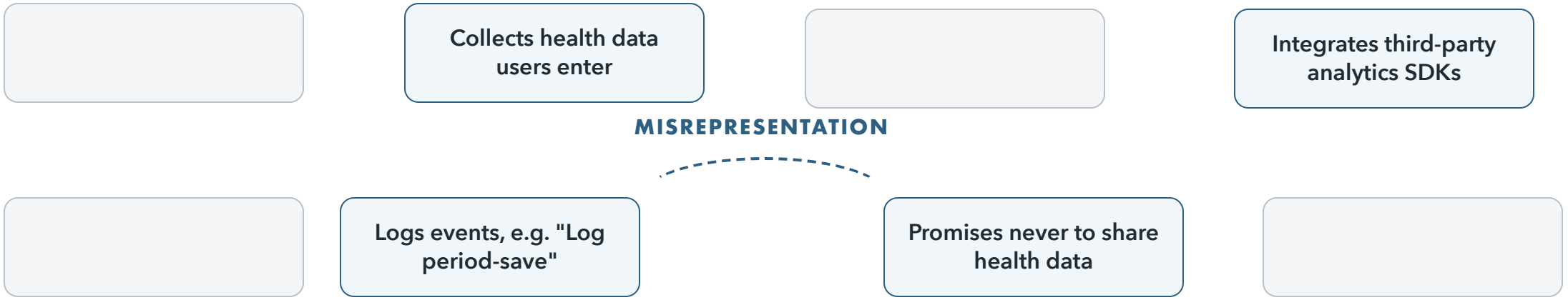
- 1,135 enforcement decisions
- 7 jurisdictions
- $533.3M+ in fines

Privacy Detective



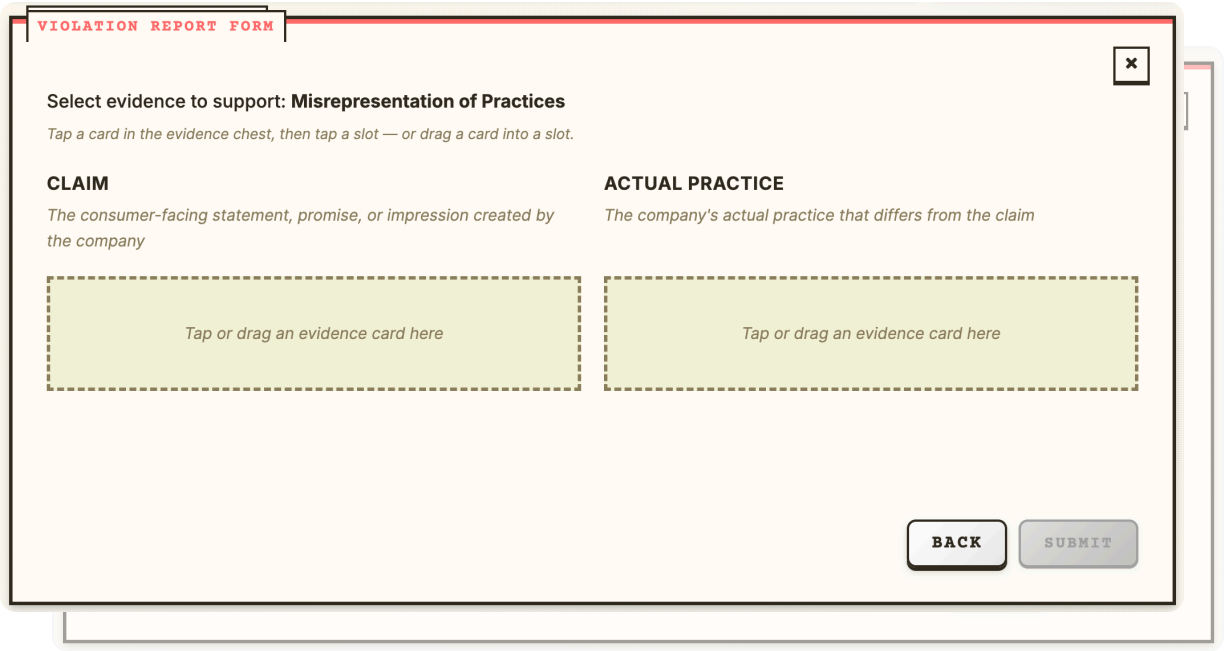
1. A detective game
2. Guided reasoning
3. Real enforcement cases

Detective game



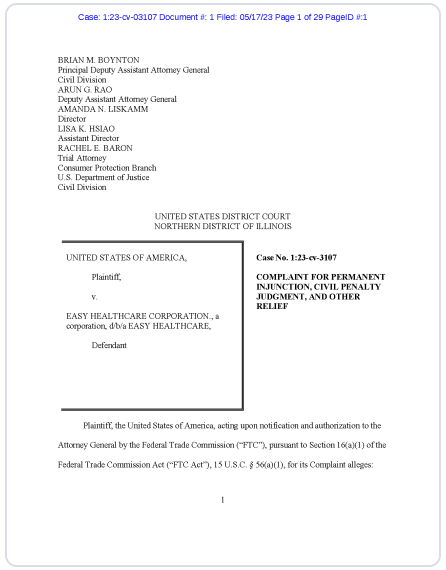
1. Selective attention
2. Longer attention window

Guided reasoning



1. Explain > recognize
2. Auto-gradable → immediate feedback

Real enforcement cases



Case: 1:23-cv-03107 Document #: 1 Filed: 05/17/23 Page 1 of 29 PageID #:1

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
Civil Division
ARUN G. RAO
Deputy Assistant Attorney General
AMANDA N. LISKAMM
Director
LISA K. HSIAO
Assistant Director
RACHEL E. BARON
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
Civil Division

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

UNITED STATES OF AMERICA,

Plaintiff,

v.

EASY HEALTHCARE CORPORATION , a corporation, d/b/a EASY HEALTHCARE,

Defendant

Case No. 1:23-cv-3107

COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC"), pursuant to Section 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 56(a)(1), for its Complaint alleges:

1

¶19

"WE PROMISE WE WILL **NEVER SHARE** YOUR EXACT AGE OR ANY DATA RELATED TO YOUR **HEALTH** WITH ANY THIRD PARTIES WITHOUT YOUR CONSENT OR KNOWLEDGE."

¶28

… when a user logs and saves information related to her period, Defendant records the Custom App Event as "**Log period-save.**"

1 Contextualized, concrete scenarios

2 Calibrated sensitivity

From document to game level

THE COMPLAINT

THE IN-GAME REPORT

COUNT I · cites ¶19, ¶28

Privacy misrepresentation — disclosing health data to third parties

→ **REPORT TEMPLATE**
Misrepresentation of Practices

¶19

"WE PROMISE WE WILL **NEVER SHARE** … ANY DATA RELATED TO YOUR **HEALTH** …"

→ **CLAIM**

Premom promised never to share health data.

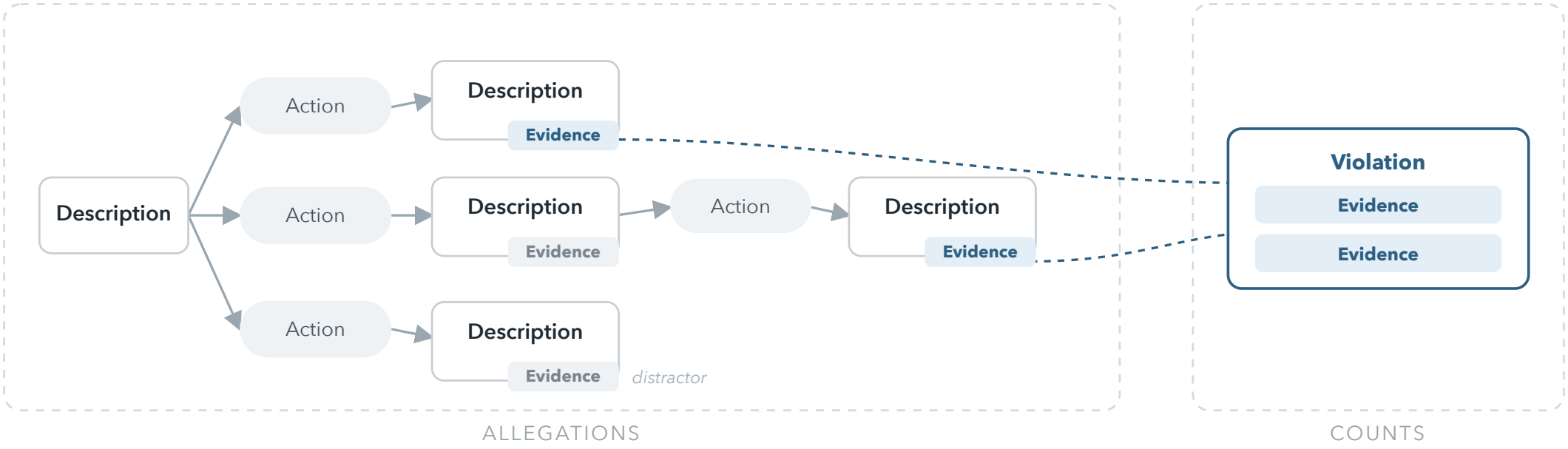
¶28

records the event "**Log period-save,**" sent to Google

→ **ACTUAL PRACTICE**

Premom sent "Log period-save" to Google.

Assemble into a playable search tree



- Clustered into actions
- Distractors
- Playable in any order

User study

PARTICIPANTS

24 student developers

TASK

Identify & explain privacy violations in a scenario → Play the game / read complaint + press release → Identify & explain privacy violations in a new scenario

ANALYSIS

Measure improvement, before vs. after learning

Metrics

METRIC 1

Recall

Of the violations the FTC actually found, how many did they catch?

IN THE CASE

- ✓ Misrepresentation — shared health data
- ✓ Failure to disclose — location use
- ✗ Health-breach notification (missed)

METRIC 2

Reasoning completeness

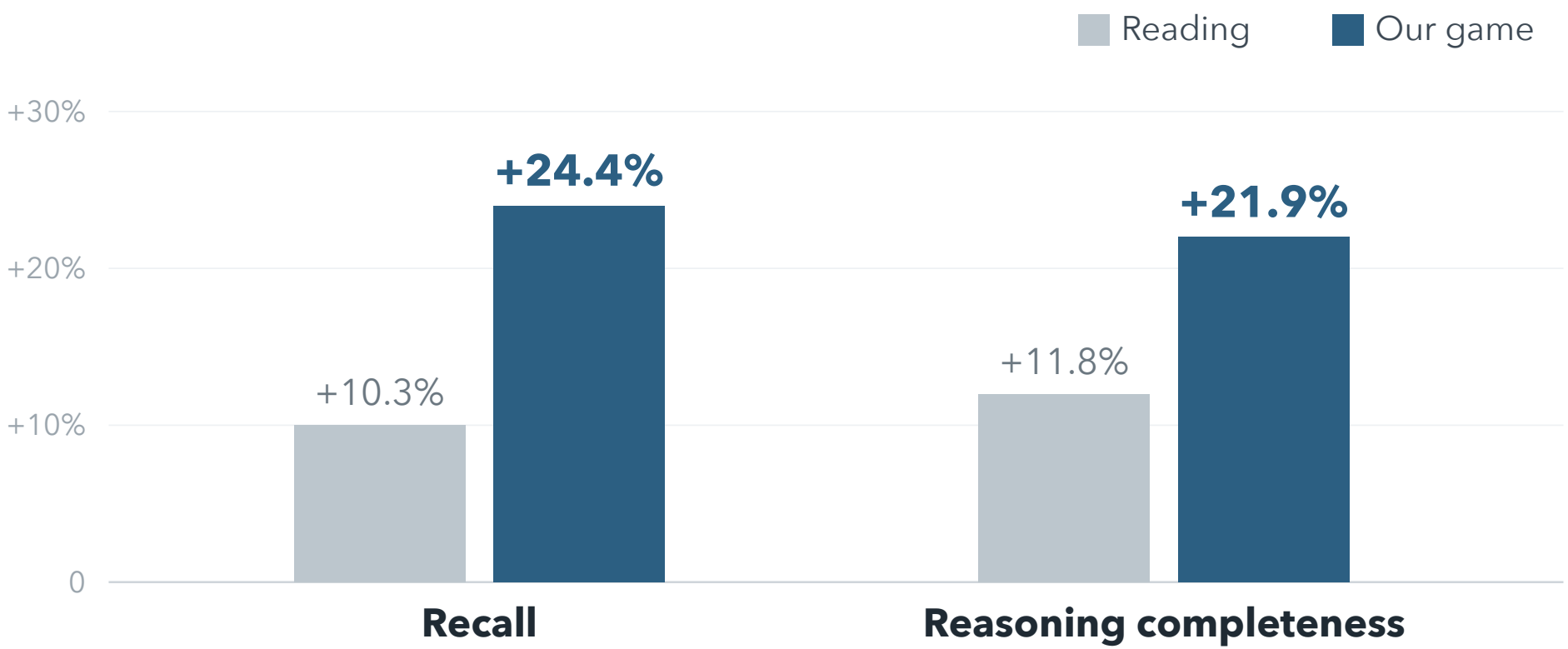
For a violation they caught, did they give the full argument?

A COMPLETE MISREPRESENTATION

the promise made +

the practice that broke it

Results


Reading
Our game
+30%
+20%
+10%
0
+10.3%
+24.4%
+11.8%
+21.9%
Recall
Reasoning completeness

Developers' privacy education

Privacy Detective

https://privacy-detective.vercel.app

Privacy Jury – led by Viki Shi

https://jury.privacydev.org

Panopticon

https://github.com/AISmithLab/Panopticon

Contact:

shaoyuchu@ucsd.edu