UNITED STATES PATENT APPLICATION

For

METHOD OF DETECTING END-USER PRIVATE DATA LEAKAGE

INVENTORS:

JOHN C. BAHR
AUSTIN RALPH PAHL
ERIC WINKELMAN
JEREMY G. DIAMOND
JOHN MORGAN FELAND, III
RICHARD D. TERPSTRA
SCOTT L. CARUSO
STEPHEN ARENDT
STEPHEN GLENNON
THOMAS MARDIS
THOMAS HOLTZMAN WILLIAMS
ZACKARY FOREMAN

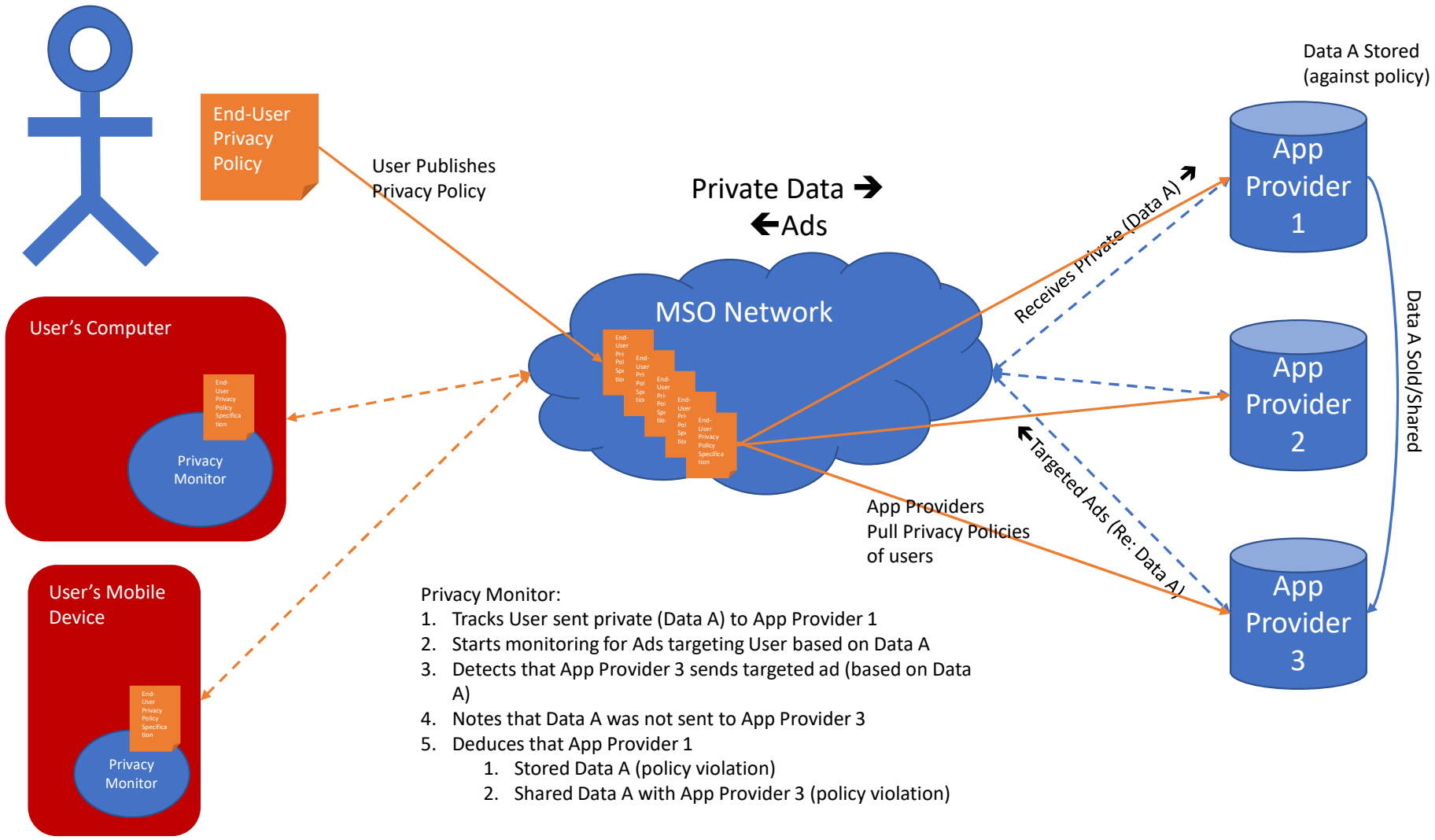
Description

MSOs can detect private data leakage/storage and determine if this storage is against an end-user's policy by:

- Monitoring which private data the user may be sending to each App Provider via a browser plugin
- Monitoring ads that show up in the end-user's browser sessions (via a browser plugin doing OCR of images/videos or scraping HTML), and on a user's mobile device (via screen monitoring app).
- Comparing ad content with end-user's published privacy policy
- Determining which Application provider leaked the data and compiling a data-trail for evidence
- Using data fuzzing (or data watermarking?) to figure out who is leaking what data by comparing the fuzzed data to ads that show up after the fuzzed data is supplied to an application provider.

Background

End-users may be able to specify their privacy preferences (e.g., CableLabs project: User-Centric Privacy - D5102) but figuring out if an entity is violating those preferences is extremely difficult. This is challenging because traffic between and end-user's computer or mobile device is encrypted at the application-layer (e.g., HTTP (SSL)) and tracking what private information is transmitted to which application provider.



Privacy Monitor:

1. Tracks User sent private (Data A) to App Provider 1
2. Starts monitoring for Ads targeting User based on Data A
3. Detects that App Provider 3 sends targeted ad (based on Data A)
4. Notes that Data A was not sent to App Provider 3
5. Deduces that App Provider 1
    1. Stored Data A (policy violation)
    2. Shared Data A with App Provider 3 (policy violation)