Privacy Policies Through the Lens of Contextual Integrity

Yan Shvartzshnaider\textsuperscript{1,2}, Noah Apthorpe\textsuperscript{2}, Nick Feamster\textsuperscript{2}, Helen Nissenbaum\textsuperscript{3}
NYU\textsuperscript{1}, Princeton CITP\textsuperscript{2}, Cornell Tech\textsuperscript{3}

This research was funded by Princeton IoT Consortium grant and NSA and NSF grants.
Do these services respect our privacy?
Let’s Check the Privacy Policy

- We can infer that *claimed* practices respect our privacy if they conform to our expectations of the resulted information flows.
Privacy as Contextual Integrity

- Users come to services with privacy expectations in mind.
- We can describe information flows using CI in terms of 5 key parameters.
All 5 CI Parameters Matter!

Transmission principle (e.g., with permission)

Attribute (e.g., medical record)
Using CI to Capture Norms

- **Actors**
  - Who is the Sender? Recipient? Subject?
- **Attribute**
  - What type of information?
- **Transmission Principle**
  - Under what condition? For what purpose?
Methodology

- Use the CI framework to annotate policy statements that describe contextual information exchanges.

We reveal only the last four digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.
Detecting Policy Ambiguities

- Identifying statements that omit contextual information (Incomplete flows)
- Recognizing complex statements (CI Parameter Bloating)
- Comparing privacy policy versions
- Diagnosing vague statements
Facebook Case Study

- Annotate previous and updated versions of Facebook’s privacy policy
- Increase in the number of information flows and parameters
- More information flows does not mean more clarity!
Incomplete Information Flows

- Previous policy
  - 47% (25/53) of flows are missing one or more parameters.

- Updated policy
  - 55% (42/76) of flows are missing one or more parameters.

- Failing to specify parameters introduces ambiguity, leaving consumers uninformed about company behavior.
Advertisers, app developers and publishers\textsuperscript{senders} can send \textit{us} \textit{recipient} information through Facebook Business Tools that they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs or the Facebook pixel\textsuperscript{TP}. These partners provide information about your\textit{subject} activities off Facebook including information about your device, websites you visit, purchases you make, the ads you see and how you use their services\textit{attributes} whether or not you have a Facebook account or are logged in to Facebook.\textsuperscript{TP}
CI Parameter Bloating: 1 to N Flows
Crowdsourcing Annotations

- Constructed CI annotation as an Amazon Mechanical Turk task
  - Promising results (high precision)
  - **Future goal**: produce a large corpus of privacy policies annotations to discover trends in within and across industries
Takeaways

- Privacy practices should conform with privacy expectations
- Policies that omit contextual information are ambiguous and misleading
- CI Parameter Bloating generates complexity beyond human cognition and memory
Thank You

@privaci_way

http://privaci.info