

Who am I?



Travis Breaux
Assistant Professor
Carnegie Mellon
University

- Ph.D. in Computer Science from North Carolina State University
- Research Interests:
 - Impact of laws, regulations and policies on software systems (NSF CAREER)
- Mixed-Methods
 - Grounded theory
 - Judgment and decision-making
 - Formal methods (logic)
 - Natural language processing
- Teaching
 - Software Design Methods
 - Engineering Privacy

Balancing utility and risk

Maximize Data Utility

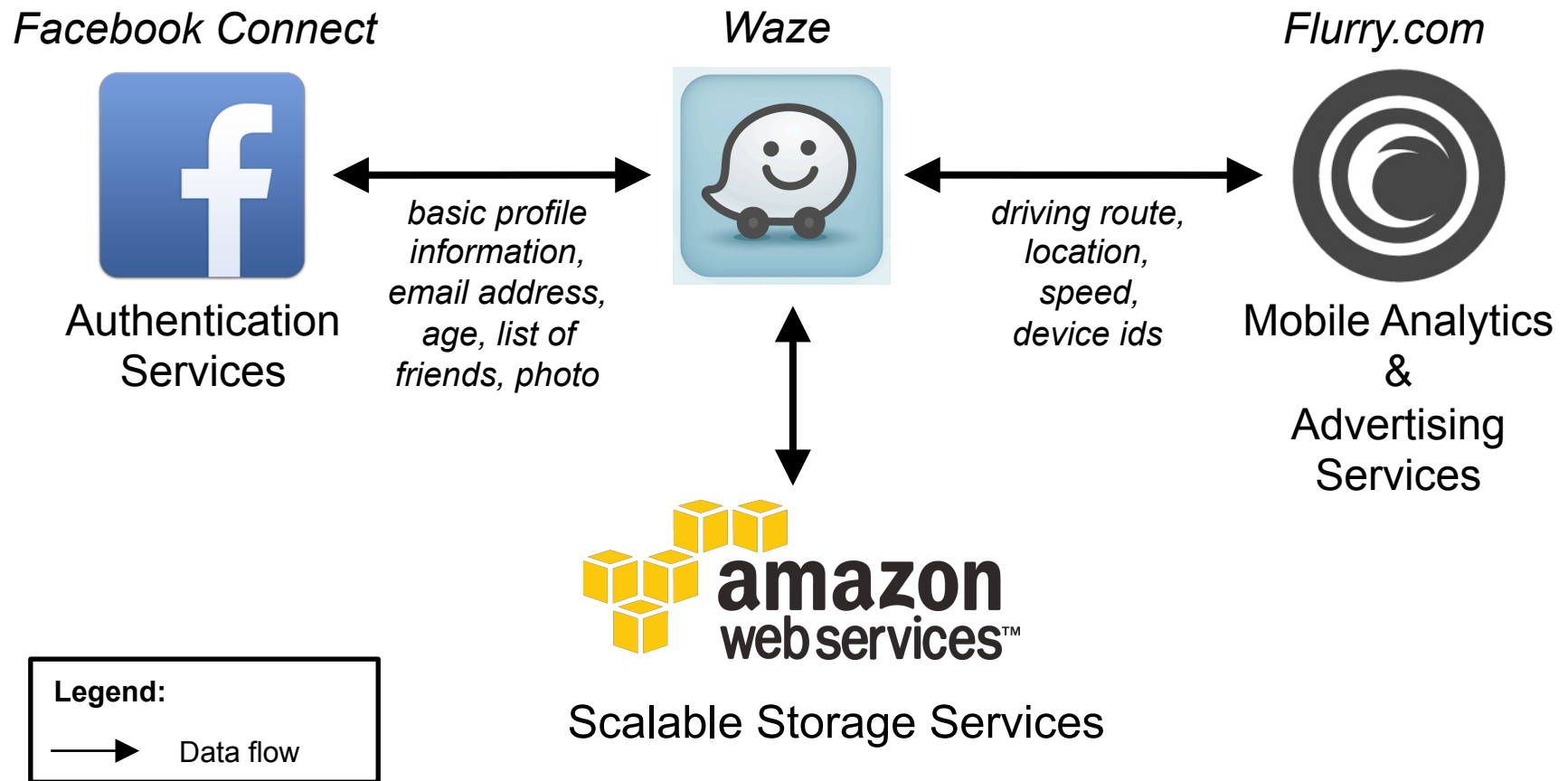
- Collect everything, value is realized later
- Ensure open access; this drives innovation
- Disclose to leverage third-party value
- Retain as long as practical (longitudinal/behavioral)
- Avoid destruction

Minimize Privacy Risk

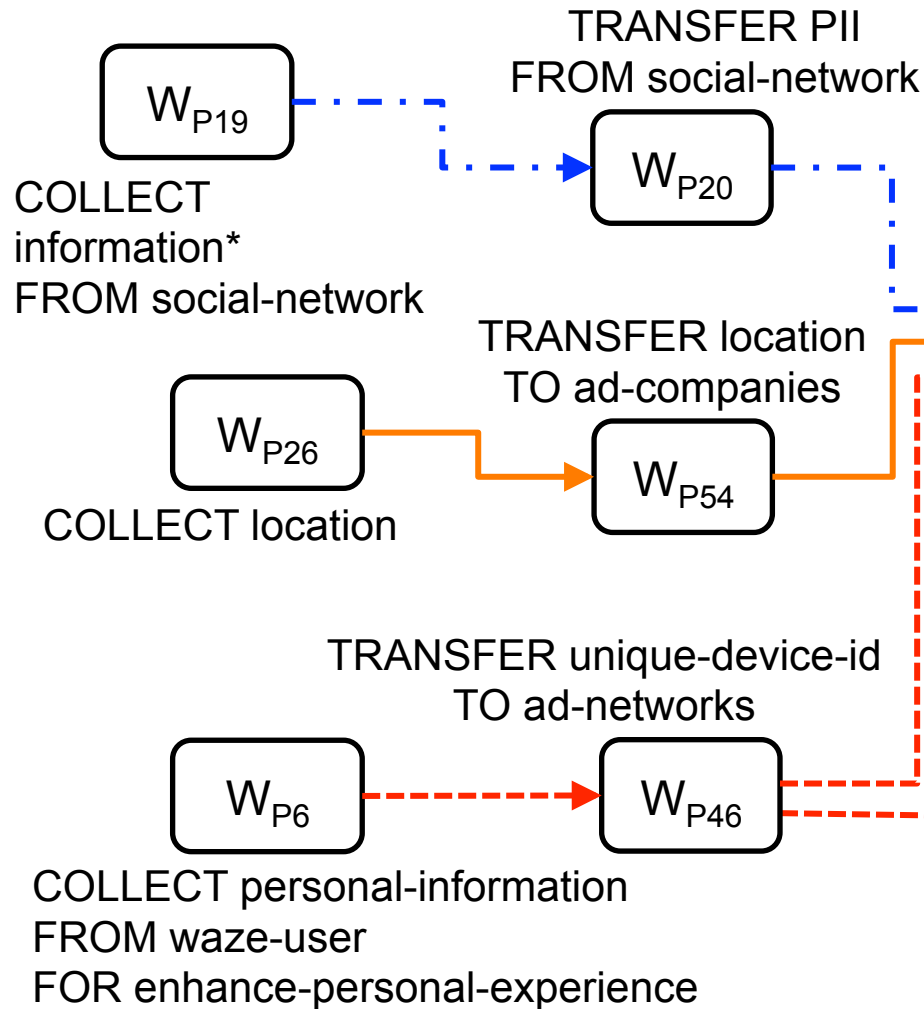
- Limit collection based on stated needs
- Limit access, obtain consent for new uses
- Limit disclosure and third-party uses
- Destroy when no longer needed
- Embrace destruction

Example Service Integration

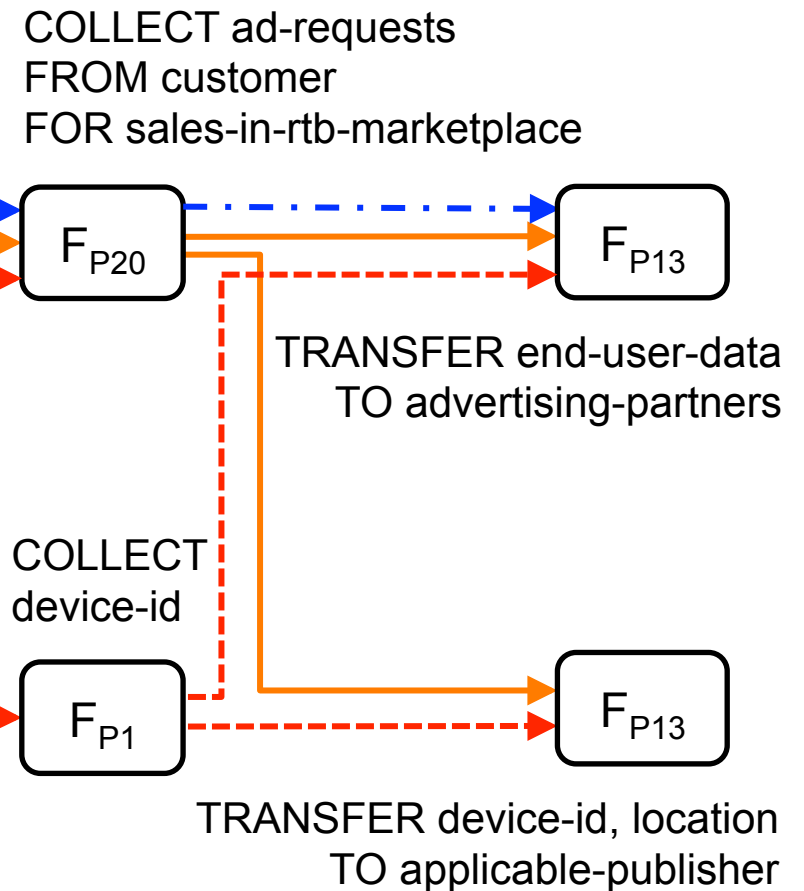
IEEE RE 2013 / RE 2015



Waze Collections & Transfers



Flurry Collections & Transfers



- Legend:**
- Blue dashed arrow: User's social network information, including name, age, gender
 - Orange solid arrow: User's mobile device location
 - Red dashed arrow: User's mobile device unique identifier

Beyond Data Minimization

- Privacy risk is exogenous, contextual and anthropic; how to collect and assess risks at design and run time?
- How to propagate privacy requirements across systems and components?
- How to detect sensitive uses at design or run time and reverse propagate real time consent mechanisms?

References

- Travis D. Breaux, Daniel Smullen, Hanan Hibshi. "Detecting Repurposing and Over-collection in Multi-Party Privacy Requirements Specifications." *IEEE 23rd International Requirements Engineering Conference (RE'15)*, Ottawa, Canada, pp. 166-175, Sep. 2015.
- Hanan Hibshi, Travis D. Breaux, Stephen B. Broomell, "Assessment of Risk Perception in Security Requirements Composition." *IEEE 23rd International Requirements Engineering Conference (RE'15)*, pp. 146-155, 2015.
- Travis D. Breaux, Hanan Hibshi, Ashwini Rao. "Eddy, A Formal Language for Specifying and Analyzing Data Flow Specifications for Conflicting Privacy Requirements." *Requirements Engineering Journal*, 19(3): 281-307, 2014.