

Privacy Preservation in Mobile Online Social Networks

Position Statement for the NSF/EU Workshop on
Pervasive Computing and Social Networking

Ramón Cáceres
AT&T Labs

21 March 2010

Mobile Online Social Networks are becoming popular

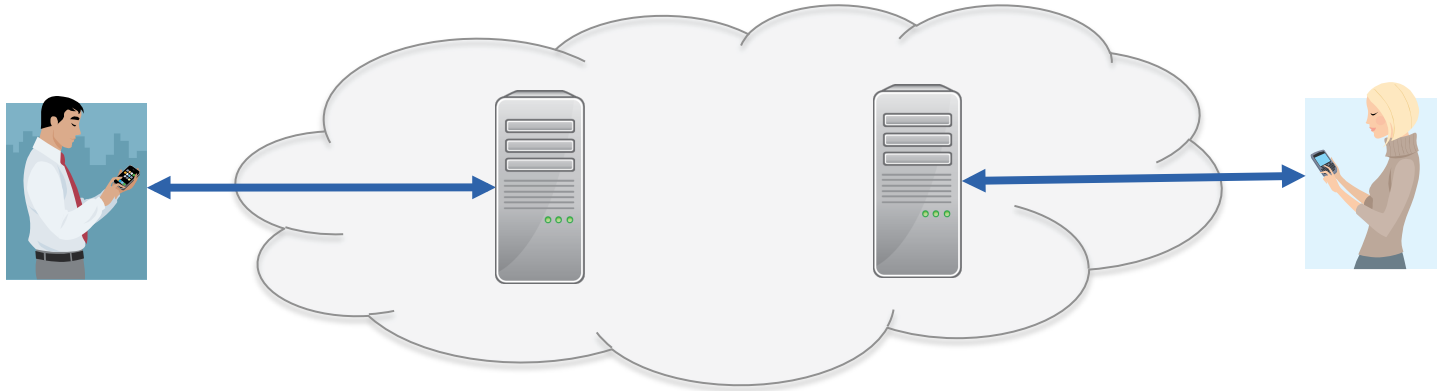


Focused on the sharing of location and other personal information generated and consumed on mobile devices

MOSNs raise important privacy issues

- Services are centralized
 - Hold data for many users under a single administrative domain
 - Vulnerable to large-scale privacy breaches
- Terms of service often grant providers rights to user data
 - Provider may display and distribute data in any way it sees fit
 - Advertising-driven business models create incentives to share data with third parties in ways that may diminish user privacy
- Prominent privacy violations have already been seen
- Public awareness of privacy issues is growing

Virtual Individual Servers can help



- Individuals would be better served by uploading their personal information to a machine they themselves own
- A VIS is a personal machine that stores sensitive data
- Preferred instantiation is a virtual machine running in a paid cloud computing infrastructure
- Data is distributed across many administrative domains
- Individuals maintain rights to their data

Vis-à-Vis enables decentralized MOSNs

- Vis-à-Vis is a distributed OSN framework based on VISs
- Mobile devices send sensitive data to their owners' VISs
- VISs self-organize into overlay networks, one per social group
- VISs arbitrate requests for their owners' data
- Mimics privacy expectations and trust relationships of offline social networks

