Supporting privacy preferences when sharing personal content

Patricia Charlton and Jonathan Teh

Motorola Labs

Patricia.charlton@motorola.com

Jonathan.teh@motorola.com

Overview of the presentation

- Privacy and Digital Content
- Digital content management and sharing
- Privacy Preferences, Policies and Tools
- Some findings and challenges going forward

User results when using mobile devices to create and share content

- Easy sharing (open) between known social groups
- Prevention of content misuse when sharing or providing access to anonymous environments
- DRM too complicated and not well received
- Default rules required and those proposed were thought to be useful
- Flexibility required to deal with granularity of content management
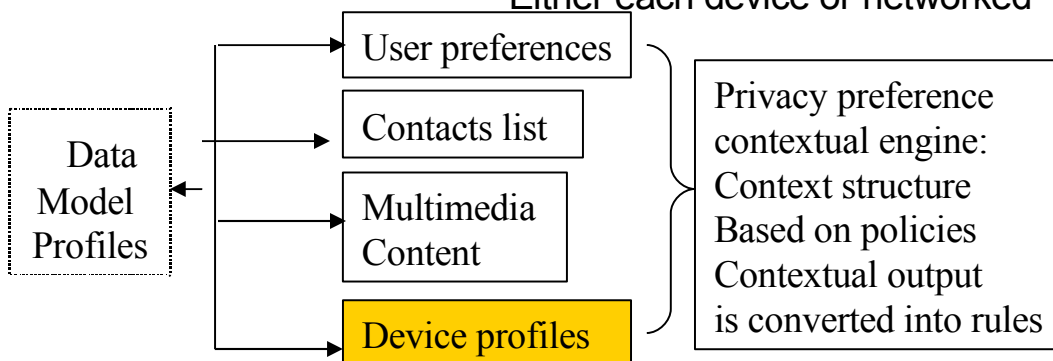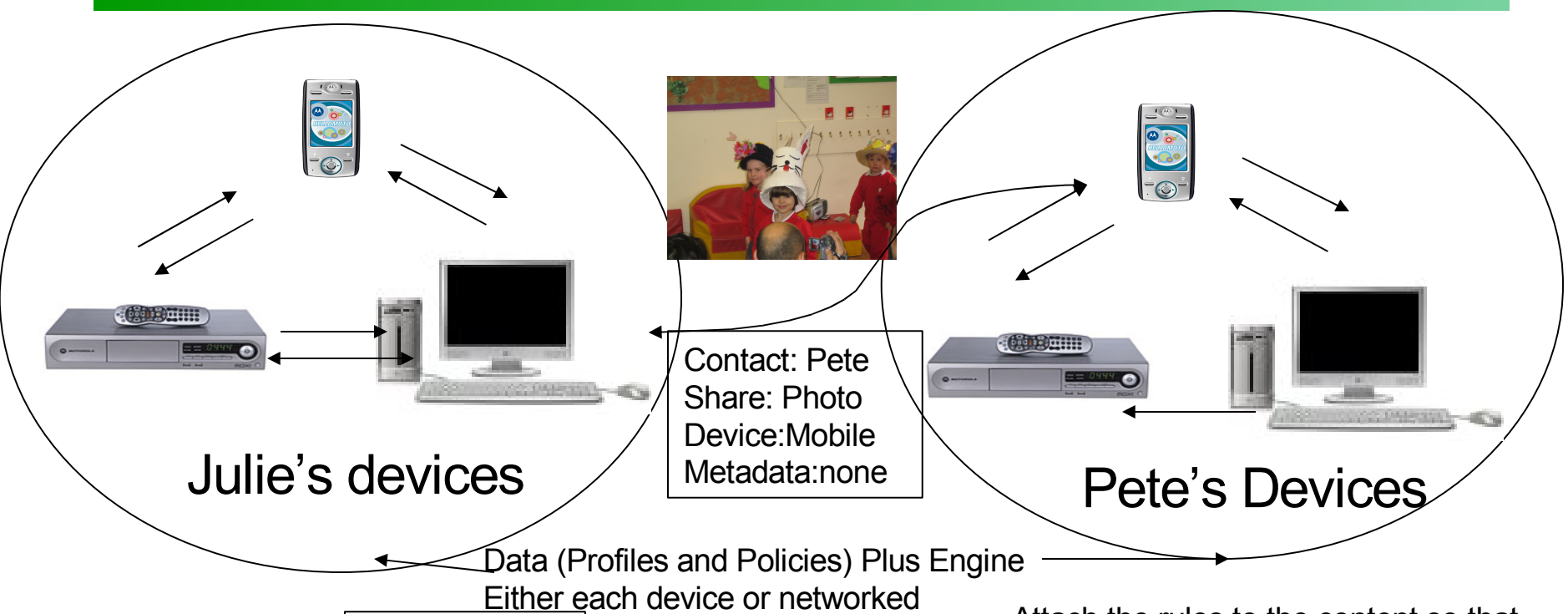- Access preferences should be with the content when the content leaves the owner's environment/device

User privacy priorities when sharing content (scale of 1 to 5)

Uncontrolled distribution/misuse of content	Main concern: 5
Declaring access rights when sharing with individual or known groups	Concern about further distribution: 3
Declaring access rights when sharing with anonymous community	More concerned but they filter: 4
Declaring access rights for environments, location	More concerned about devices: 3
Declaring access rights on a specific piece of content	More concerned about compromising situations:3
Declaring access rights about specific content in a location	Implications of content in different locations: 3
Person identity via media analysis	Not concerned about this: 2
Declaring access rights about automatic metadata	Not concerned: 1
Declaring access rights about personal metadata	More concerned when manual metadata is being used: 4

Profiles, Preferences and Policies

- ◆ Profiles for configuring devices and applications:
  - ◆ Profile about a device e.g. memory size, ring tone style
  - ◆ Profile about user e.g. age, address
- ◆ Preference for customising an application possibly at run-time
  - ◆ User declares preferences
    - ◆ *e.g. I prefer to listen to the radio than watch TV, I prefer films to news etc.*
    - ◆ *E.g. I prefer my mum to receive weekly photo updates of my cat. I prefer all my photos to be centrally stored on my home server*
- ◆ Policies declare explicit actions, taking contextual cues from profiles and preferences
  - ◆ E.g. a preference "never share this content" is declared in a policy with an action "grant no access rights" to this content
  - ◆ E.g. a preference "share my holiday photos with my family" is declared as a policy with contextual cues which are "holiday photos and family" (group contacts) with an action "grant access rights" to this content

Preference and Device Content Management

Contact: Pete
Share: Photo
Device:Mobile
Metadata:none

Julie's devices

Pete's Devices

Data (Profiles and Policies) Plus Engine
Either each device or networked

Data Model Profiles

User preferences

Contacts list

Multimedia Content

Device profiles

Privacy preference contextual engine:
Context structure
Based on policies
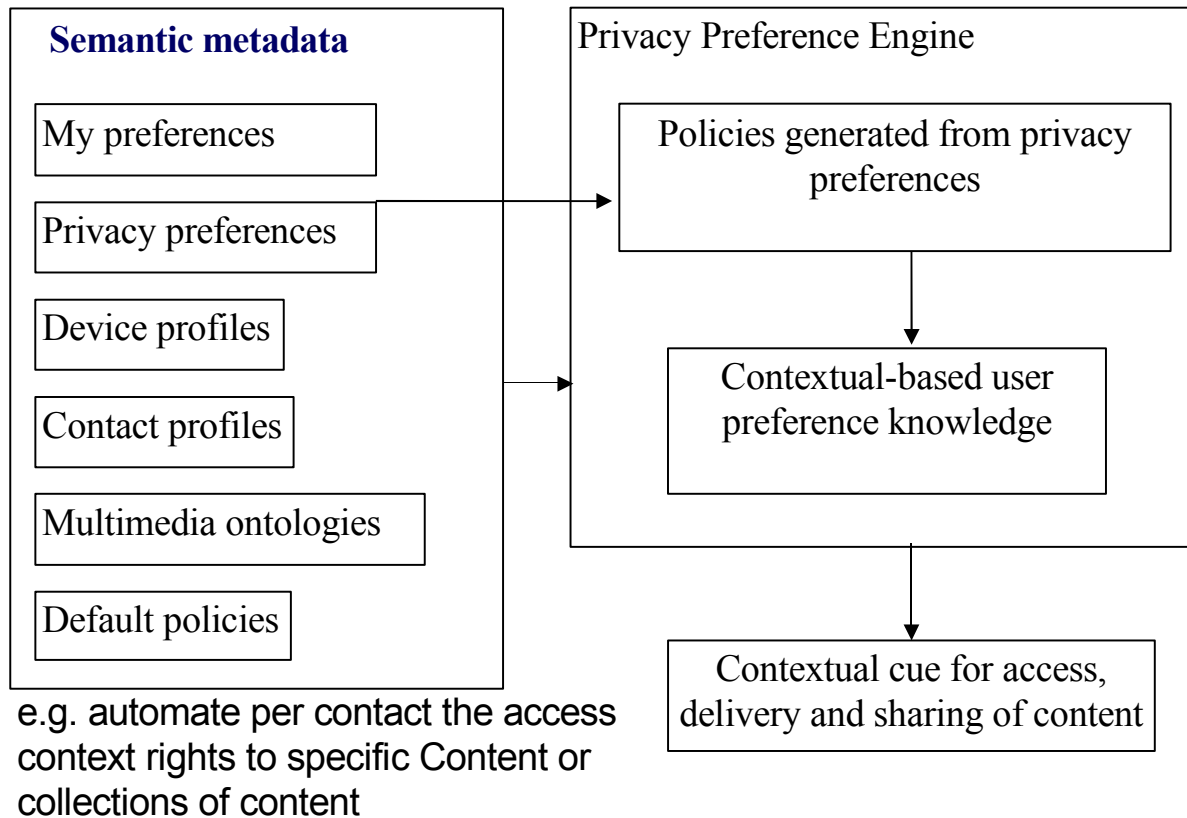Contextual output
is converted into rules

Attach the rules to the content so that the rules manage the content wherever it Is. Only the rules needed go with the content which are executable code

Example default Rules
• Ownership to remain with originator
• Close friends to view and copy
• No anonymous viewing

Privacy Preference Engine

Semantic metadata

My preferences

Privacy preferences

Device profiles

Contact profiles

Multimedia ontologies

Default policies

e.g. automate per contact the access context rights to specific Content or collections of content

Privacy Preference Engine

Policies generated from privacy preferences

Contextual-based user preference knowledge

Contextual cue for access, delivery and sharing of content

Creating and adding personal content access rights as rules

♦ Create (From user) or use default policies: Preferences and policies applied to content, metadata and contacts (family, friends, colleagues etc.): Done by *privacy reasoner*

♦ Share content: The reasoner creates a new modified content collection for each contact adding appropriate access rights (uses simplified rights from DRM) based on user policies: Done by *privacy reasoner*

♦ Generate the rules to be attached to content: Done by *rule generator*

♦ Execute rules when receiver wants access to content: Done by *self-governing reasoner*

Key Findings

♦ Privacy model to meet social networking and content sharing applications

♦ Social networking and personal metadata

♦ Semantic attacks: Ontologies, personal metadata and autonomous systems

♦ Many types of knowledge required but only small amount of facts used

♦ REI: Complexity, meta-policies, granting rights, scalability-linked to the type of applications

The right to decide

- Policies and users: What and how

- Terminology: Is it a profile or a policy or a preference?

- "test-bed":

  - Semantics of policy languages,

  - appropriate application set that the approach targets (guidelines),

  - Flexibility and ease of use required ,

  - Policy enforcement methods

The Knowledge Connection

Me & Myself	Family & Friends	People I work with	External Commercial world
Scenario I would like to take my holiday photo Collection with me	Scenario I want to always share the best photos of my family with close friends and family	Scenario I need some good slides for aceMedia review	Scenario I want to follow my favourite football team and be kept up to date
Preference Engine (applied to policy inference system) Pack and go, target appropriate form factor	Privacy Preference Engine (applied to policy inference system) Sends the photo to mum and dad – the family group	Privacy Preference Engine (applied to policy inference system) Finds work colleagues, checks rights, creates collections with automated annotation	Privacy Preference Engine (applied to policy inference system) Purchases the latest exciting moments, annotate , prepares the film clip for watching
Scenario I would like to see an automated showing of my birthday party photos	Scenario To send holiday video and pictures with some personal annotations and create a group collection	Scenario I wonder where the meeting docs and notes are for the next meeting?	Scenario I would like to enhance my collection with music
Privacy Preference Engine (applied to policy inference system) Knows my preferences of presentation and device, configures and plays content	Privacy Preference Engine (applied to policy inference system) Check rights of content, Apply personal content ownership, Preference, target individual Device,	Privacy Preference Engine (applied to policy inference system) Pack and go to appropriate form factor, provides a summary.	Privacy Preference Engine (applied to policy inference system) Finds appropriate music content, purchase the content, proposes an organisation

aceMedia

Thank you!