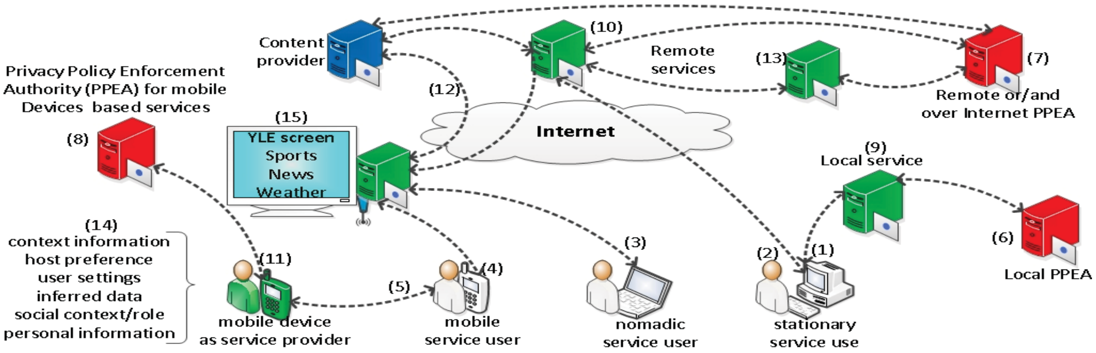
Enforcing Privacy Policies in Mobile Context-Aware Services

Were Oyomno, Pekka Jäppinen, Esa Kerttula
Lappeenranta University of Technology
Lappeenranta, Finland.
{were.oyomno, pekka.jappinen, esa.kerttula}@lut.fi

Abstract

Transparent context-aware services leverage miniaturised mobile devices to expose new service models. Inexpensive mobile devices have positioned most domestic and business users as potential service consumers. However, the inconveniences of small screens, compact keyboards and limited attention span, reinforce the proliferation of transparently ubiquitous services. As services become more transparent and ubiquitous requiring less user intervention, the more they demand personal and context data of their users' for customisation and automation. Deeper personal and context data facilitates better individualised and adapted services preferred/perceived by many users as useful. Unfortunately, transparently and seamlessly soliciting, acquiring and handling of personalisation, authentication, credentials and payment data legitimises privacy concerns. We propose privacy policy enforcement authority to safeguard privacy concerns regarding personal data and monitors adherence to stipulated privacy policies. Concerns regard disclosures, retention, re-use and re-purposement of personal data.



Depicted service landscape distinguishes five (*1, 2, 3, 3, 4, 5*) service uses based on provider characteristics. Service providers may be local (*9*), remote (*10*), third-party (*13*) or ad-hoc/mobile (*11*). These providers exposed services that could be displayed on hosts device screens (*1, 2, 3*) or provider's real estate (*15*). Assurance over personal data (*14*) handling and policy compliance are facilitated by privacy policy and enforcement authority systems. Enforcement systems verify solicitations to be within defined privacy threshold. Retrieved data are weighted against prior defined enforcements and certified privacy policies. Data solicits are subject compliance monitoring by bound enforcement authorities. This binding of enforcement authority, certifying authority, services and policies serves to: (1) notify of data retrieval, (2) scope the data retrieved, (3) disambiguate data use and purpose, (4) expose avenues for complaint and redress in-case of non-compliance and (5) discourages malice by services. Privacy policy enforcement authority can be implementable at the local (*6*), remote (*7*) and ad-hoc/mobile arenas (*8*).

Index Terms:Privacy, Policy, Enforcement, Personal information, Context, Service.