Um serviço flexível para a configuração e manutenção da política de privacidade de usuários de aplicações LBS

Vagner Sacramento[1], **Markus Endler**[2], **Clarisse de Souza**[2]

[1]Instituto de Informática – Universidade Federal de Goiás (UFG)
Caixa Postal 131 – CEP 74001-970 – Goiânia/GO

[2]Departamento de Informática – PUC-Rio
Rua Marquês de São Vicente – 225 RDC – CEP 22453-900 – Gávea – Rio de Janeiro/RJ

vagner@inf.ufg.br, {endler,clarisse}@inf.puc-rio.br

Abstract. *The potential loss of privacy due to the use of location based applications may be one of the greatest limitation of their acceptance. Nevertheless, most research in privacy does not consider the complexity in the utilization of a location based application that deals with privacy issues. In this article, we propose a privacy service that aims to help users maintain their privacy policy in a flexible way. Based on a qualitative evaluation study, we exemplify several challenges that should be handled in the design of such a service.*

Resumo. *A potencial perda de privacidade na utilização de aplicações baseadas em localização pode ser um dos maiores empecilhos para a sua aceitação. No entanto, a maioria das pesquisas sobre privacidade não considera a complexidade de utilização de uma aplicação baseada em localização que trata das questões de privacidade. Neste artigo, estamos propondo um serviço que visa a auxiliar o usuário a manter a sua política de privacidade de forma flexível. Através de uma avaliação qualitativa, exemplificamos vários desafios que devem ser tratados no projeto de um serviço do gênero.*

1. Introdução

A disseminação de dispositivos GPS e a existência de vários serviços de middleware que realizam a inferência da localização do usuário [MoCATeam 2005], têm motivado cada vez mais o desenvolvimento de aplicações baseadas em localização (também conhecidas como LBS - *Location Based Services*). Essas aplicações usam a informação de localização para oferecer serviços customizados ou mais adequados ao usuário final. Por exemplo, permitir o envio de mensagens baseado na localização ou na proximidade entre os usuários, facilitar a coordenação e a movimentação de equipes de busca, etc.

Entretanto, esses serviços e aplicações introduzem novos riscos e ameaças à privacidade do usuário. Segundo Harper [Harper 1996], as preocupações dos usuários com a sua privacidade podem ser um grande empecilho para a aceitação dessas aplicações que coletam, processam e utilizam suas informações.

Essas preocupações apontam para a necessidade de aplicações LBS que tratem das questões de privacidade relacionadas à sua utilização. No entanto, a maioria dos trabalhos relacionados não considera a real complexidade de utilização de uma aplicação

LBS sensível à privacidade. Vários tratam somente de certos aspectos básicos da privacidade, como, por exemplo, o anonimato [Myles et al. 2003, Beresford and Stajano 2003] ou a autenticação [Hengartner and Steenkiste 2004] de acesso à informação do usuário, não oferecendo flexibilidade para os casos em que o usuário deseja também divulgar as suas informações (e.g., localização) para tirar proveito dos serviços disponíveis para colaboração e comunicação [Hong and Landay 2004].

Com o intuito de oferecer um serviço de privacidade com tal flexibilidade, estamos propondo um serviço, chamado CoPS - **Co**ntext **P**rivacy **S**ervice, através do qual os usuários podem definir e gerenciar a sua política de privacidade gradativamente, durante o uso de uma aplicação LBS. Este serviço foi integrado à arquitetura MoCA - *Mobile Collaboration Architecture* [Sacramento et al. 2004, MoCATeam 2005] para que pudéssemos desenvolver aplicações sensíveis ao contexto que tratem das questões de privacidade.

Com base nas discussões de Westin [Westin 1967] e Altman [Altman 1977], concluímos que o conceito de privacidade e a forma de exercê-la e defendê-la variam fortemente de um indivíduo para outro, de maneira que somente os próprios usuários de um serviço de privacidade estão aptos a decidir sobre o que pode ou não ser disponibilizado, pois só eles são capazes de analisar, de acordo com a situação, qual é o risco *versus* o benefício de divulgar a informação de localização. Sendo assim, o principal desafio no projeto de um serviço de privacidade não é simplesmente implementar o controle de acesso à informação do usuário, mas, sim, oferecer recursos que o auxiliem a definir e manter sua política de privacidade de forma gradativa e flexível. Em função disto, a principal questão que norteou a nossa pesquisa foi: Como fornecer um conjunto significativo de controles de privacidade que ofereça flexibilidade e amenize a complexidade da configuração e manutenção da política de privacidade do usuário?

Para tratar essa questão, realizamos uma pesquisa preliminar com usuários para identificar algumas necessidades básicas de gerenciamento de privacidade (Seção 2). O resultado dessa pesquisa e o estudo sistemático de outros trabalhos que discutem questões gerais de privacidade envolvidas no projeto e uso de tecnologias mediadas pelo usuário serviram de base para o projeto do serviço de privacidade proposto (Seção 3). A partir deste, fizemos um estudo qualitativo com usuários para identificar como estes utilizariam alguns dos controles de privacidade oferecidos pelo CoPS (Seção 4). Os resultados obtidos nos permitiram comparar a nossa abordagem com a de outros trabalhos relacionados (Seção 5) e derivar uma série de conclusões e reflexões (Seção 6) sobre algumas questões fundamentais sobre o benefício e o risco de perda de privacidade decorrente do uso de serviços LBS e, principalmente, como estes podem ou devem tratar estas questões.

2. Pesquisa preliminar com usuários

Para identificar as expectativas e preocupações dos usuários com respeito a algumas questões de privacidade, nós realizamos um estudo *preliminar* com *120 usuários* familiarizados com tecnologias de informação. O estudo foi baseado em um questionário que descrevia em termos não-técnicos, a existência de uma tecnologia hipotética capaz de coletar, processar e divulgar os dados de contexto induzindo a localização dos usuários, e seria utilizada para oferecer novas aplicações para comunicação e colaboração entre eles.

Com base nos resultados desta pesquisa [Sacramento 2006], e a partir dos resultados reportados em trabalhos relacionados [Harper 1996, Grudin 2001,

Hong and Landay 2004, Patil and Lai 2005], identificamos, inicialmente, os seguintes requisitos desejáveis para um serviço de privacidade.

Flexibilidade: os usuários devem ser capazes de definir suas preferências de privacidade com diferentes níveis de detalhe para diferentes grupos de requisitantes;

Notificação das tentativas de acesso: os usuários devem poder ser notificados sobre, ou poderem rastrear, qualquer tentativa de acesso às suas informações de contexto;

Negação Aceitável: os usuários devem poder negar o acesso aos requisitantes sem que eles tenham conhecimento;

Controle de Precisão: os usuários devem poder ajustar a precisão temporal e espacial de suas informações de contexto;

Controle de Acesso: a qualquer momento, os usuários devem poder bloquear o acesso a qualquer das suas informação de contexto;

Exceções em Emergências: os usuários devem poder definir regras de exceção que tenham precedência maior do que qualquer outra política de privacidade;

Simplicidade: não deve ser difícil nem demorado, para os usuários, configurarem suas preferências de privacidade;

Eficiência: o tratamento das questões de privacidade não deve causar um atraso significativo na comunicação da aplicação LBS.

3. Arquitetura do CoPS

A arquitetura do CoPS, ilustrada na Figura 1, oferece um controle de acesso de granularidade fina e flexível que permite ao usuário, através de uma interface adequada, definir e gerenciar a sua política de privacidade, gradativamente, durante o uso de uma aplicação LBS. O serviço proposto tem como público-alvo uma comunidade de usuários na qual as pessoas têm uma certa relação de confiança entre si, por exemplo, por trabalharem juntas ou estarem associadas diretamente à mesma organização, ou por simplesmente se conhecerem pessoalmente.

Além dos requisitos gerais discutidos na Seção 2, nós identificamos alguns requisitos de projeto que podem ser utilizados como base para o desenvolvimento de um serviço de privacidade que visa a auxiliar os usuários a definirem e refinarem as suas políticas gradativamente, de acordo com as suas necessidades. Dada a limitação de espaço, não discutiremos as justificativas que embasaram a proposta de cada requisito. No entanto, a descrição completa do modelo conceitual e de tais requisitos pode ser encontrada em [Sacramento et al. 2006]. De fato, esses delinearam as decisões de projeto e implementação do CoPS [Sacramento 2006] o qual descrevemos a seguir.

O serviço de privacidade proposto está baseado em um modelo que é formado por várias entidades cujos papéis são descritos como segue:

- *Subject* é o usuário que tem a sua localização inferida pelo serviço de contexto;
- *Requester* é a entidade que, após devidamente autenticada, solicita acesso à informação de localização de um Subject divulgada por um serviço de contexto;
- *PolicyMaker* é o responsável por definir a política de privacidade. Este pode ser tanto o Subject, quanto o administrador do sistema;
- *Serviço de contexto* é a entidade responsável por processar as requisições dos Requesters, inferir e divulgar a informação de localização do Subject mediante a autorização concedida por um serviço de privacidade;

- *Aplicação LBS* é o meio de interação/comunicação através do qual o Requester requisita o acesso à informação de localização do Subject;
- *Serviço de privacidade* é a ferramenta que controla e monitora o acesso a informação de localização do Subject no escopo das concessões e restrições da política de privacidade definida pelo PolicyMaker.

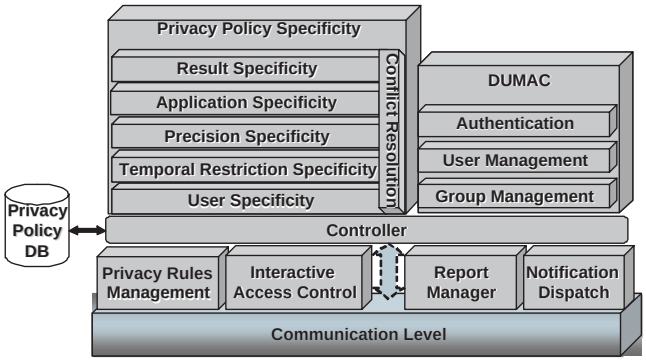

Figura 1. Arquitetura geral do CoPS

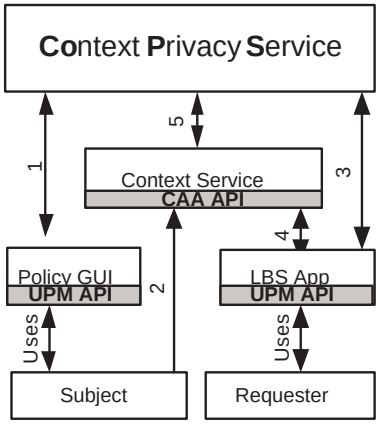

Figura 2. Interação entre cliente e servidor

3.1. Interação entre as entidades do serviço

A interação entre as entidades que usam o CoPS, ilustrada na Figura 2, segue o padrão de interação definido no modelo conceitual [Sacramento et al. 2006]. Inicialmente, o PolicyMaker (Subject ou Administrador) define a política de privacidade através da interface de gerenciamento de políticas/regras (1). Em paralelo, o serviço de contexto recebe periodicamente dados de sensores para inferir a localização do Subject (2). Entretanto, a sua localização somente será divulgada mediante as restrições impostas pela sua política de privacidade. O Requester autentica-se junto ao CoPS para validar a sua identidade (3). Quando a requisição de acesso à informação de localização é recebida pelo serviço de contexto (4), ela é processada e repassada para o serviço de privacidade. Se a requisição do Requester é aceita, o serviço de privacidade responde com uma mensagem "Grant", caso contrário responde com um resultado "Deny" ou "Not Available" (5).

3.2. Visão Geral dos Componentes da Arquitetura

Uma visão geral dos componentes da arquitetura é ilustrada na Figura 1. Conforme mostrado nesta figura, as requisições recebidas pelo *Communication Level* são repassadas para o componente *Controller*, que por sua vez, interpreta o tipo de requisição recebida e interage com os demais componentes da arquitetura para desempenhar a ação solicitada.

Para atender às necessidades de privacidade de ambientes organizacionais e/ou de indivíduos específicos, o componente *Privacy Rules Management* organiza as *políticas de privacidade em uma hierarquia de três níveis*: política da organização, do usuário e política padrão. A política em nível da organização é definida pelo administrador do sistema e tem maior precedência sobre as demais. Essa política é utilizada pela corporação para impor-se perante as políticas dos usuários por alguma necessidade específica, por exemplo, exigir que a localização dos mesmos esteja sempre disponível para

uma aplicação de controle de situações emergenciais (e.g., incêndios). A política em nível de usuário é definida pelo próprio Subject e tem uma maior precedência em relação à política padrão definida pelo administrador do sistema.

A política padrão consiste de um *template* de regras que é associado a cada novo usuário do sistema. Em [Patil and Lai 2005] são apresentados resultados que demonstram que a grande maioria dos usuários não muda a configuração padrão do sistema e das aplicações. Sendo assim, a política padrão pode ser muito útil, principalmente, na fase inicial de uso de uma aplicação LBS, pois os usuários não precisarão, de antemão, configurar a sua própria política para ter o mínimo de privacidade desejável. Dado que não existe um *template* padrão e único, cabe ao administrador do sistema identificar e definir um modelo de risco de privacidade que contemple um conjunto de regras padrão que represente as principais necessidades de privacidade da maioria dos usuários.

O componente *Privacy Rules Management* também implementa três *políticas de controle de acesso*: Reservado, Liberal e Sob-Demanda. No modo Reservado, por definição, todas as requisições são negadas, exceto aquelas que casam com alguma regra que libera o acesso. No controle de acesso Liberal, por definição, todas as requisições são aceitas, exceto aquelas que casam com alguma regra que explicitamente nega o acesso. No controle de acesso Sob-Demanda, o resultado a ser aplicado às requisições é obtido interativamente, a partir de uma consulta ao Subject.

Para cada tipo de política de controle de acesso, o PolicyMaker pode definir um conjunto de regras que determinará sob quais condições as informações do Subject serão reveladas. Para tanto, o PolicyMaker poderá escolher um dos serguintes resultados a ser aplicado a uma requisição: “Grant” ou “Deny” (mas não ambos), “Not Available” ou “Ask me”. Além disso, o PolicyMaker (i.e., o Subject) tem a opção de não definir nenhuma regra inicialmente e, gradativamente, através da política Sob-Demanda, configurar a sua política de privacidade interativamente.

A notificação sobre as tentativas de acesso enviada pelo *Notification Dispatch* cria, implicitamente, um protocolo social entre os usuários que pode evitar certas ações maliciosas. O fato do Requester saber que o Subject pode estar sendo notificado a cada tentativa de acesso, pode inibir certas atitudes que caracterizam uma invasão de privacidade.

Quando um Subject tiver escolhido uma política de controle de acesso tipo “Sob-Demanda”, ou quando a ação associada à regra selecionada para avaliar uma requisição for “Ask Me”, o componente *Interactive Access Control* interage com o Subject para consultá-lo sobre o resultado a ser aplicado às requisições recebidas do serviço de contexto. Quando consultado, o Subject deve informar o resultado (e.g., *Grant/Deny*) a ser aplicado à requisição e, na resposta, ele pode informar se a avaliação deferida deve ou não ser armazenada em sua política de privacidade para evitar futuras consultas desnecessárias.

Para amenizar o ônus de ter que se lembrar de remover uma regra de privacidade que não se aplica mais à suas necessidades, o PolicyMaker pode definir *regras temporárias* que são automaticamente removidas após um determinado período.

3.3. Propriedades de controle de acesso flexível

Com o intuito de oferecer um controle de acesso flexível, o componente *Privacy Policy Specificity* permite que o Subject ajuste a *granularidade temporal*, *espacial* e a *precisão*

da informação a ser revelada. Por exemplo, considere um cenário em que o usuário João pretende compartilhar sua localização com seus colegas de sala de aula para que eles possam se coordenar através de uma aplicação *Friend Finder*. No entanto, João pode não se sentir confortável em divulgar a sua localização exata. Neste caso, ele poderia ajustar a granularidade espacial da sua informação de localização revelando que está no prédio "RDC" da PUC-Rio ao invés da "Sala 512". João também poderia implementar uma restrição temporal limitando o acesso a sua localização a um grupo específico de requisitantes somente em um determinado horário (e.g., de segunda à sexta, entre 9:00 e 12:00). E, se necessário, ele também pode especificar a precisão (*freshness*) da informação a ser revelada, determinando que ao invés da sua localização corrente, somente a localização conhecida de 30 minutos atrás deve ser divulgada.

3.4. Estrutura das regras de privacidade

Toda regra de privacidade está associada a uma política de acesso padrão (e.g., Reservado, Liberal ou Sob-Demanda). Os campos das regras de privacidade e seus significados são:

- *Policy Maker*: Usuário que define/configura a regra de privacidade (pode ou não ser o próprio Subject);
- *Subject*: Usuário ou entidade cuja informação de contexto (e.g., localização) é controlada pela regra de privacidade;
- *Requester*: Usuário ou componente de software que requisita acesso à localização do Subject;
- *Context Variable*: Informação de contexto requisitada pelo Requester (e.g., localização do Subject);
- *Application*: Lista de nomes das aplicações que podem ser utilizadas pelo Requester para acessar a variável de contexto;
- *Precision*: Especifica a precisão do valor da variável de contexto a ser divulgada (e.g., este campo poderia ter os seguintes valores: Prédio, Andar, Sala, etc.);
- *Temporal Restriction*: Restrições de hora e data para divulgar a informação de contexto (e.g., dias da semana, das 9:00 às 14:00);
- *Freshness*: Especifica quão recente deve ser a informação de contexto a ser divulgada para um dado Requester (e.g., revelar somente a localização inferida há 15 minutos atrás, ou revelar a localização corrente);
- *Timestamp*: Horário em que a regra de privacidade foi criada ou atualizada;
- *AccessPolicy*: Representa a política de acesso (Reservado, Liberal ou Sob-Demanda) com a qual a regra de privacidade está associada;
- *Policy Level*: Nível da hierarquia da regra de privacidade. O CoPS oferece suporte às seguintes hierarquias: "Organization", "Individual" ou "Default" (com este grau de precedência);
- *Result*: Resultado a ser aplicado à requisição de acesso à informação de contexto. Os possíveis valores são: "Not Available", "Ask Me", "Grant" e "Deny";
- *Notify Me*: Tipo de notificação a ser enviada para o Subject quando uma requisição é avaliada pela regra. Por exemplo, "NoNotification", "E-Mail" ou "SMS".

3.5. Avaliação da política de privacidade

A avaliação da política de privacidade é uma das principais questões a ser tratada pelo serviço de privacidade para oferecer um controle de acesso efetivo e de granularidade fina

na avaliação das requisições. No CoPS, o componente *Privacy Policy Specificity* avalia as requisições de autorização de acesso à informação de localização. Em linhas gerais, o algoritmo de especificidade funciona da seguinte forma. A partir de um conjunto de regras selecionado previamente para avaliar uma requisição, o algoritmo identifica a regra mais específica desse conjunto comparando os campos das estruturas das regras na seguinte ordem de prioridade: *Subject*, *Requester*, *Temporal Restriction*, *Precision*, *Application* e *Result*. Ao comparar as regras com relação a um determinado campo, somente aquelas com o valor mais específico neste campo são selecionadas para a análise de especificidade posterior, enquanto que as demais regras não são consideradas na avaliação seguinte. Desta forma, mesmo se duas ou mais regras têm diferentes especificidades relativas (i.e., elas diferem em dois ou mais campos), o algoritmo pode identificar a regra mais específica analisando esses campos de acordo com suas prioridades.

Para a especificidade dos campos "*Subject*" e "*Requester*", as regras de privacidade que contêm o nome de um usuário específico (e.g., "Alice") são mais específicas do que as regras contendo um grupo definido pelo usuário (e.g., "MyFriend"), que por sua vez, são mais específicas do que as regras com grupos criados pelos administradores. A especificidade destes últimos segue a interpretação de uma hierarquia: grupos no nível mais baixo da hierarquia são mais específicos do que grupos no nível mais alto (e.g., "puc.employee.prof.cs" é mais específico do que o grupo "puc.employee.prof").

O mesmo critério de especificidade aplicado aos grupos hierárquicos definidos pelo administrador é utilizado também para o campo *Precision*. Na comparação das regras relacionadas à informação de localização, as regras mais específicas são aquelas onde o campo *Precision* contém o nível mais baixo na hierarquia dessa informação, por exemplo, a hierarquia "campus.predio.andar.sala" (nível 4) é mais específica do que "campus.predio.andar" (nível 3). Duas ou mais regras de privacidade podem estar no nível mais alto da especificidade com relação ao campo *Precision* se elas contêm o valor mais específico e estão no mesmo nível na hierarquia. Quando isto acontece, o próximo campo (de acordo com a ordem de prioridade de avaliação) dessas regras é comparado para identificar a regra mais específica.

A especificidade para o campo *Temporal Restriction* é processada em três fases: (1) seleciona as regras que combinam com o horário e data da requisição; (2) identifica a regra com o maior intervalo de tempo e verifica se os intervalos de tempo das demais regras selecionadas são seu subconjunto próprio (e.g., a restrição "Feb 5, 10:30am-2:00pm" é um subconjunto próprio de "Feb 5, 10:00am-6:00pm"). As regras estarão no mesmo nível de especificidade em relação a esse campo se elas têm intervalos de tempo idênticos, ou se o intervalo de tempo de uma delas não é um subconjunto próprio da regra selecionada com o maior intervalo de tempo; (3) seleciona a regra com o menor intervalo de tempo, caso as regras selecionadas não estejam no mesmo nível de especificidade.

Com relação ao campo *Application*, a especificidade tem somente dois níveis possíveis: qualquer aplicação (representada por "*") e uma lista de aplicações. Finalmente, se todos os campos considerados anteriormente estão no mesmo nível de especificidade, o campo *Result* é utilizado para selecionar a regra mais específica para avaliar a requisição. Os possíveis valores para este campo são: "Not Available", "Ask Me" e "Grant" (ou "Deny"). O resultado "Not Available" tem uma maior precedência que "Ask Me", que por sua vez, tem maior precedência que os outros ("Grant" e "Deny"). A razão

é que “Not Available” implicitamente significa “Negar acesso” e “não deixar o requester ter ciência disso”, enquanto o “Ask Me” pode ser interpretado como “Deny” ou “Grant” dependendo da intenção do usuário no momento da consulta.

4. Estudo qualitativo com usuários

Dado que privacidade representa um conceito subjetivo e pessoal, realizamos um estudo para avaliar como um grupo de usuários típicos (dentro de seu contexto social e cultural) expostos a situações que suscitam questões de privacidade interpretam e manejam os controles de privacidade do CoPS. O objetivo do estudo era entender em maior profundidade o problema, e não prever e generalizar como “a maioria” dos usuários interpretarão as questões de privacidade e usarão a tecnologia. Como já discutido neste artigo, esta generalização não faz sentido quando o assunto é privacidade.

Os experimentos envolveram, portanto, 5 (cinco) usuários que realizaram entrevistas e testes em um simulador de um jogo fictício. Nosso intuito foi avaliar se esses usuários têm percepções que convergem ou divergem de algumas hipóteses de usabilidade do CoPS. Os experimentos realizados visaram especificamente descobrir como os mecanismos de controle de privacidade do CoPS podem ser interpretados, se são vistos como efetivos (i.e., funcionam) e úteis (i.e., atendem às expectativas dos usuários) para os usuários “gerenciarem” a sua privacidade ao usarem uma aplicação sensível à localização.

4.1. Discussão sobre a metodologia de avaliação

Como privacidade é um conceito fortemente individual, o uso de métodos quantitativos de pesquisa (que visam embasar a “generalização” de resultados) não fazia sentido. Por isto, realizamos experimentos que expuseram nossas hipóteses ou expectativas (no sentido qualitativo) sobre a efetividade e a utilidade das funcionalidades do CoPS à refutação. As hipóteses avaliadas são descritas sucintamente a seguir, no entanto, elas estão mais detalhadas e elaboradas em [Sacramento 2006].

Hipótese 1: Há situações em que o usuário deseja manter um compromisso entre sociabilidade e privacidade, disponibilizando a sua localização em diferentes granularidades em função do dia/horário e dos usuários/grupos de requisitantes.

Hipótese 2: Há usuários que não querem se ater a detalhes de configuração da política de privacidade para usar uma aplicação LBS. No entanto, eles desejam saber quais informações pessoais a seu respeito estão sendo divulgadas, como e para quem.

Hipótese 3: Há usuários que não se preocupam se a sua localização é divulgada ou não.

Hipótese 4: Há usuários que desejam criar, a priori, perfis de privacidade para diferentes papéis sociais que desempenham com a mediação, necessária ou opcional, de uma tecnologia sensível a privacidade (e.g., professor, aluno, orientador, amigo).

Hipótese 5: Há situações em que, para não prejudicar o seu relacionamento social, o usuário deseja negar acesso à sua localização, em um período pré-determinado, sem que os requisitantes tenham conhecimento de tal atitude.

Estruturamos o processo de avaliação da seguinte forma: (a) enunciamos as hipóteses de usabilidade e efetividade do CoPS; (b) associamos a cada hipótese um cenário de avaliação possível; (c) elaboramos um teste em que pessoas “representativas” do público-alvo ao qual a tecnologia deve servir possam, por intermédio de sua ação, adotar atitudes e produzir julgamentos alinhados ou desalinhados com as nossas hipóteses.

4.1.1. Descrição dos testes com o simulador do jogo

Os testes realizados com os usuários através de um simulador do jogo consistiram da análise de alguns cenários específicos que fazem parte de um jogo fictício em que duas equipes concorrentes usam as suas informações de localização para se coordenarem na busca de alguns equipamentos perdidos no Campus da PUC-Rio. No jogo, os membros de cada equipe adotavam diferentes estratégias para vencer a equipe adversária e/ou acomodar suas atividades e objetivos pessoais no contexto da competição que se desenrolava.

O único meio de contato do usuário com os demais participantes era através do simulador. Através dele, o usuário podia também controlar e monitorar o acesso de outros à sua localização, bem como (tentar) obter a localização dos demais participantes de uma e outra equipe.

4.1.2. Metodologia de avaliação

Os experimentos foram realizados com cada usuário separadamente, em quatro etapas, seguindo duas técnicas comuns em IHC (Interação Humano-Computador): entrevistas abertas e experimentos do tipo "Mágico de Oz" [Kelley 1984] (simulação conceitualmente fidedigna de aspectos relevantes de uma tecnologia que ainda não está em produção). Essas etapas foram organizadas da seguinte forma:

- Primeiro, fizemos uma entrevista cujo objetivo foi determinar como os usuários lidam com as questões de privacidade presentes em aplicações de bate-papo (e.g., *Instant Messaging*) e telefones celulares;
- Segundo, averiguamos como os usuários acham que gerenciariam a privacidade da informação de localização em alguns cenários do jogo. As opiniões dos usuários obtidas nessa etapa foram contrastadas com suas ações desempenhadas através do simulador. Isso nos permitiu avaliar o quanto as opiniões dos usuários obtidas na entrevista divergem de suas ações desempenhadas no simulador;
- Terceiro, realizamos testes com os usuários através do simulador do jogo, confrontando-os com cenários específicos através dos quais eles poderiam reforçar ou enfraquecer algumas hipóteses de usabilidade do CoPS; e
- Por fim, realizamos uma segunda entrevista para investigar se o usuário conseguiu manejar o simulador, se os controles de privacidade foram úteis, quais foram as principais dificuldades encontradas, quão difícil seria utilizar os mecanismos de controle de privacidade em uma situação real do cotidiano, dentre outros.

Nos experimentos realizados através do simulador, o usuário desempenhava o papel de um dos personagens do jogo em 7 cenários distintos. Em cada cenário, ele recebia uma mensagem do sistema estimulando-o a desempenhar uma determinada tarefa, por exemplo, obter a localização de um outro usuário do mesmo grupo ou do grupo oponente, alterar a política de privacidade ou interagir com outros usuários. Exemplo de uma mensagem: *Você está cansado de procurar e precisa descansar um pouco, mas já combinou com seus colegas de grupo que vai procurar os brindes nas salas do Prédio RDC. Por um lado, você quer mostrar para os seus colegas que você continua seguindo o plano determinado, mas, por outro lado, não deseja deixar explícito para eles que você vai ficar "parado" por um certo tempo.* O administrador do simulador do jogo desempenhava o papel dos usuários do grupo adversário e fazia consultas à localização do usuário

entrevistado. Assim, os participantes eram motivados a alterar as suas preferências de privacidade, analisar as notificações e relatórios de acesso.

4.2. Principais conclusões dos experimentos

Nas entrevistas realizadas nas duas primeiras etapas, *os usuários relataram que se preocupam com privacidade "on-line" em relação ao acesso a seus dados pessoais ou em situações em que terceiros podem derivar conclusões a seu respeito.* Por exemplo, deduzirem que estão no trabalho, ou descansando, namorando, etc. Entretanto, em alguns cenários do jogo, houve usuário que, apesar de afirmar que se preocupa com a sua privacidade, não restringiu o acesso a sua localização para o grupo adversário, mesmo em situações em que os seus adversários pudessem inferir as suas ações. Esta é uma evidência real que demonstra que nem sempre as pessoas *reagem* em certas circunstâncias (e.g., dentro do contexto do jogo) como elas *acham que reageriam* fora delas (e.g., fora do jogo).

No geral, *os usuários controlaram o acesso e a visibilidade à sua informação de localização*, reforçando o fundamento da Hipótese 1. Também identificamos que *os usuários disponibilizaram a sua localização exata para os membros do seu próprio grupo e se preocuparam em restringir o acesso a esta informação somente para os membros do grupo oponente.* Isso nos leva a crer que em cenários reais a relação pessoal, social e profissional entre os usuários pode determinar quais informações e em que condições os usuários as divulgariam.

Os participantes dos experimentos alegaram que seria muito difícil manter as suas preferências de privacidade atualizadas em função das inúmeras opções de controles de privacidade que podem ser re-configuradas e das diferentes situações que podem requerer essas atualizações. Como uma solução paliativa, a maioria dos entrevistados disse que o uso de perfil de privacidade (e.g., Em Reunião, Descansando, ...) facilitaria o gerenciamento da política de privacidade, principalmente se a seleção dos perfis fosse realizada de forma automática e eles pudessem alterar as exceções quando fosse necessário. Como um dos entrevistados reportou, *"Eu gostaria de criar perfis para gerenciar a política de privacidade. Controlar as propriedades de privacidade individualmente pode fazer com que o usuário cometa erros e divulgue a sua localização indevidamente"*. Isto vai ao encontro do que expressa a Hipótese 4.

A partir dos experimentos realizados, constatamos que a maioria dos usuários nos forneceu elementos que enfraquecem a Hipótese 5, pois, mesmo diante de cenários que induziam à necessidade de uso da funcionalidade "Negação Aceitável", eles não a utilizaram na maioria das vezes. Nas entrevistas feitas após os experimentos, os usuários disseram que não se lembraram ou não entenderam essa funcionalidade no sistema. Porém, isto também pode ter ocorrido por causa de algum problema da interface ou por causa da falta de expressividade ou importância dessa funcionalidade no contexto do jogo, o que aponta para a necessidade de fazermos pesquisas mais profundas sobre este item.

Também identificamos em algumas etapas dos experimentos que os usuários podem expressar percepções que enfraquecem e reforçam várias das hipóteses de usabilidade do CoPS, dependendo da situação. Por exemplo, se o participante considera que o momento não representa muito risco, ele divulga a sua localização e acompanha os relatórios de acesso e notificações (convergindo para as Hipóteses 2 e 3, e divergindo da Hipótese 1). Em uma situação oposta, ele bloqueia explicitamente o acesso e controla o

nível de visibilidade da localização a ser disponibilizada (convergindo para a Hipótese 1 e divergindo das Hipóteses 2 e 3).

Essas evidências nos sugeriram que assim como para esses usuários, para um grupo muito maior de pessoas as questões de privacidade são extrema e complicadamente dependentes do contexto em que se encontram. Sendo assim, não podemos partir para soluções generalizantes. E se partirmos para uma variedade de controles de privacidade em que as pessoas podem escolher usá-los ou não de acordo com o contexto, temos de estar atentos para o fato de que este contexto pode mudar muito e, portanto, o leque de opções utilizadas a cada momento pode também variar na mesma proporção. Com isto, os controles e as interfaces das aplicações LBS e da aplicação de gerenciamento da política de privacidade constituirão, provavelmente, um desafio não trivial de interação.

Além disto, identificamos que os usuários apresentaram certas opiniões ou atitudes que de certa forma "desperdiçam" os reais benefícios do projeto de uma tecnologia. Por exemplo, considerando a quantidade de opções oferecidas para o controle de privacidade em uma ferramenta de comunicação (e.g., status de visibilidade, gerenciamento de grupos), às vezes, os usuários esquecem de utilizá-las. No entanto, muitos expressaram o desejo de ter ainda mais controles disponíveis. Isto nos leva a crer que a *atitude* das pessoas em relação às ofertas tecnológicas pode ser *ambígua* - elas *podem dizer* que querem um determinado recurso, que preferem *de uma forma* ou *de outra*, mas quando expostas à necessidade de uso das funcionalidades deparam-se com as implicações imprevistas de todos estes desejos e preferências, e acabam por não usar o que disseram que queriam.

5. Trabalhos relacionados

Há inúmeros outros trabalhos que tratam das questões de privacidade relacionadas ao anonimato [Hoh and Gruteser 2005], confidencialidade dos dados (através de mecanismos de criptografia) [Hengartner and Steenkiste 2004], controle de acesso [Ferraiolo and Kuhn 1992], serviço e arquitetura de privacidade para a Web [Ishitani 2003], dentre outros. Entretanto, nos preocupamos em fazer uma comparação com trabalhos que propõem uma abordagem, um serviço ou uma arquitetura para tratar das questões de privacidade de aplicações sensíveis ao contexto, principalmente aqueles que se referem a localização.

A Context Fabric (Confab) [Hong and Landay 2004] é uma arquitetura para provisão de informação de localização que trata do controle de privacidade. O projeto da arquitetura da Confab apresenta uma série de requisitos de privacidade que oferecem flexibilidade no uso de uma aplicação sensível a privacidade, tais como o modo invisível, o controle de acesso interativo, a notificação de acesso. Alguns de seus requisitos de projeto (e.g., modo invisível, notificação de acesso) e resultados do estudo com usuários serviram de base para o nosso trabalho. No entanto, definimos novos princípios de projeto (e.g., controle de acesso de granularidade fina, desacoplamento do sistema de privacidade da aplicação sensível ao contexto) e incorporamos novas funcionalidades de controle de privacidade ao CoPS que oferecem maior flexibilidade no gerenciamento da política de privacidade do usuário ou da organização. Como, por exemplo, políticas de controle de acesso, relatórios de acesso, *templates* de regras, perfis de privacidade, dentre outros. Além disto, fizemos uma pesquisa com usuários que descreve a complexidade e os desafios que devemos estar atentos no projeto de um serviço de privacidade.

Ao contrário do CoPS, as arquiteturas CoBrA (*Context Broker Architecture*) [Chen 2005] e *pawS* (*Privacy Awareness System*) [Langheinrich 2002] usam a informação de localização do requisitante para determinar quais restrições de acesso devem ser impostas sobre a divulgação de cada tipo específico de informação de contexto. No entanto, os autores desses trabalhos não discutem como os sistemas deles se comportam na ausência da informação de localização utilizada no controle de acesso. Além disso, eles não discutem questões práticas sobre a complexidade e dificuldade (sob o ponto de vista do usuário) da utilização dos sistemas propostos.

Em [Myles et al. 2003] é proposto um *framework* de componentes para controle de privacidade. Este foi integrado ao serviço de localização *LocServ (Location Service)*. Através dos componentes *Validators*, o *LocServ* avalia se a localização de um dado usuário requisitada por um terceiro pode ser divulgada ou não. O sistema presume que uma organização confiável definirá um conjunto de *Validators* na tentativa de não sobrecarregar o usuário. Para as situações atípicas em que a política de privacidade padrão implementada pelos *Validators* não é apropriada, os usuários podem criar novos *Validators* através de ferramentas, consideradas pelos autores, "simples" e "intuitivas". O CoPS apresenta algumas semelhanças a esse projeto. Por exemplo, ambos restringem o acesso em função do tempo, utilizam grupos, *templates* de regras. Entretanto, no projeto do CoPS, definimos uma abordagem mais concreta e viável para tratar os desafios envolvidos na definição da política de privacidade dos usuários. Pois, acreditar que os administradores do sistema podem prever as necessidades de privacidade geral dos usuários e que existem ferramentas "simples" para tratar das exceções é uma abordagem simplista tendo em vista a complexidade e a quantidade de desafios relacionados a tal problema.

Um diferencial da nossa pesquisa comparada a outros trabalhos [Cuellar et al. 2002, Hengartner and Steenkiste 2004, Chen 2005, Langheinrich 2002, Myles et al. 2003], é que o serviço de privacidade proposto oferece ao usuário um conjunto de mecanismos de controle de privacidade mais abrangentes e efetivos que o auxilia na definição e manutenção de sua política de privacidade. A partir dos experimentos realizados, percebemos que os usuários, tacitamente, têm certas expectativas com relação à garantia e manutenção da sua privacidade. Eles esperam que os controles necessários estejam sendo implementados pelo sistema e que eles possam alterar suas políticas de forma flexível e gradativa. Para tanto, o serviço de privacidade e a interface de gerenciamento de regras devem ser projetados para atender à demanda daqueles que vão em última instância decretar o valor e a relevância da tecnologia - os usuários.

6. Conclusão

A partir dos experimentos realizados, pudemos identificar opiniões e atitudes dos usuários que reforçam a viabilidade de usabilidade do CoPS, uma vez que foi expresso o desejo de manter um compromisso entre sociabilidade e privacidade, disponibilizando a localização com diferentes granularidades para diferentes grupos de requisitante. De acordo com os usuários, as aplicações LBS podem ser muito úteis, entretanto, sem os controles de privacidade que lhes permitam gerenciar o acesso e a visibilidade da sua localização, essas aplicações apresentariam riscos à perda de privacidade que poderiam ser mais evidentes e impactantes do que os seus benefícios.

A noção de privacidade é individual, havendo substancial variação na atitude que

as pessoas têm em relação à privacidade como um todo. Sendo assim, há usuários pouco ou muito preocupados com questões de privacidade. Em função disto, acreditamos que para atender as necessidades dos usuários, o serviço de privacidade deve fornecer um conjunto significativo de recursos de controle de privacidade flexíveis. Estes devem permitir os usuários adotar uma postura mais conservadora, por exemplo, negar o acesso à sua localização ou, uma postura liberal (porém, moderada), por exemplo, divulgar sua localização e monitorar os acessos para identificar e inibir os eventuais abusos.

Conforme descrito nos resultados das entrevistas e dos experimentos, *os usuários não devem ser sobrecarregados com a configuração das suas preferências de privacidade*. Esta conclusão nos estimulou a identificarmos e trabalharmos em um dos principais desafios relacionados ao projeto do CoPS, que envolve: Flexibilidade *versus* Complexidade no gerenciamento da política de privacidade. Através do CoPS, o usuário não precisa definir logo de imediato uma política de privacidade, pois ele pode usufruir das regras da política *Padrão*. No entanto, a medida que ele define novas regras, gradativamente, interagindo com o sistema através da política Sob-Demanda ou de regras com resultado "Ask Me", ele customiza e define sua própria política pessoal. Além disso, o usuário pode adotar a política "Liberal" e identificar eventuais abusos/intrusões através das notificações ou relatório das tentativas de acesso. Ou, adotar uma postura conservadora através da política "Pessimista". O usuário também poderá configurar regras temporárias ou configurar perfis de privacidade que o auxilie a mudar de política corrente de acordo com as circunstâncias, dentre outros.

Vale ressaltar que, conforme discutido em [Rotenberg and Laurant 2004], não existe uma solução única e completa que assegure a privacidade dos usuários. Para alcançarmos o nível de privacidade o mais próximo do desejado, devemos levar em conta a combinação de diversos meios, tais como legislações com punições bem definidas para as possíveis infrações, normas sociais, normas corporativas, soluções tecnológicas e, por fim, acreditar na boa conduta dos usuários e empresas que diante de tais mecanismos, se sintam intimidados e sigam o protocolo social estabelecido na sociedade.

Referências

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, 33(3):66–84.

Beresford, A. R. and Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1):46–55.

Chen, H. L. (2005). *An intelligent broker architecture for context-aware systems*. Unpublished phd thesis, University of Maryland, Department of Computer Science and Electrical Engineering.

Cuellar, J., Morris, J. B., and Mulligan, D. (2002). Ietf geopriv requirements.

Ferraiolo, D. and Kuhn, R. (1992). Role-based access controls. In *15th NIST National Institute of Standards and Technology - NCSC National Computer Security Conference*, pages 554–563.

Grudin, J. (2001). Desituating action: Digital representation of context. In *HCI '01: Human-Computer Interaction*, pages 269–286.

Harper, R. H. R. (1996). Why people do and don't wear active badges: a case study. *Comput. Supported Coop. Work*, 4(4):297–318.

Hengartner, U. and Steenkiste, P. (2004). Implementing access control to people location information. In *SACMAT '04: Proceedings of the ninth ACM symposium on Access control models and technologies*, pages 11–20, New York, NY, USA. ACM Press.

Hoh, B. and Gruteser, M. (2005). Location privacy through path confusion. In *SecureComm '2005: Proc. of the First IEEE/CreatNet International Conference on Security and Privacy for Emerging Areas in Communication Networks*. IEEE Computer Society Press.

Hong, J. I. and Landay, J. A. (2004). An architecture for privacy-sensitive ubiquitous computing. In *MobiSYS '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 177–189. ACM Press.

Ishitani, L. (2003). *Uma Arquitetura para Controle de Privacidade na Web*. Tese de doutorado, Universidade Federal de Minas Gerais.

Kelley, J. F. (1984). An iterative design methodology for user-friendly natural language office information applications. *ACM Trans. Inf. Syst.*, 2(1):26–41.

Langheinrich, M. (2002). A privacy awareness system for ubiquitous computing environments. In *UbiComp '02: Proceedings of the 4th international conference on Ubiquitous Computing*, pages 237–245, London, UK. Springer-Verlag.

MoCATeam (2005). Moca home page. http://www.lac.inf.puc-rio.br/moca (Last visited: April 2006).

Myles, G., Friday, A., and Davies, N. (2003). Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, 2(1):56–64.

Patil, S. and Lai, J. (2005). Who gets to know what when: configuring privacy permissions in an awareness application. In *CHI '05: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 101–110, New York, NY, USA. ACM Press.

Rotenberg, M. and Laurant, C. (2004). Privacy for human rights 2004: An internation survey of privacy laws and development. Electronic Privacy Information Center, Washington D.C.

Sacramento, V. (2006). *Gerência de Privacidade para Aplicações Sensíveis ao Contexto em Redes Móveis*. Tese de doutorado, Pontifícia Universidade Católica do Rio de Janeiro/PUC-Rio, Departamento de Informática.

Sacramento, V., Endler, M., Rubinsztejn, H. K., Lima, L. S., Goncalves, K., Nascimento, F. N., and Bueno, G. A. (2004). Moca: A middleware for developing collaborative applications for mobile users. *IEEE Distributed Systems Online*, 5(10):2.

Sacramento, V., Endler, M., and Souza, C. (2006). Modelo conceitual e requisitos de projeto de um serviço de privacidade para aplicações baseadas em localização. In *SBSeg '2006: Anais do VI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*.

Westin, A. F. (1967). Privacy and freedom. In *New York: Atheneum*.