3
Modelo conceitual e requisitos de privacidade

Neste capítulo, descrevemos um modelo conceitual e uma lista de requisitos de projeto que auxiliam os desenvolvedores a identificarem, compreenderem e priorizarem questões importantes ligadas ao projeto e implementação de um serviço de privacidade. O modelo conceitual apresenta, em linhas gerais, a integração de um serviço de privacidade com um outro serviço (i.e., provedor de contexto) responsável por processar e divulgar a localização dos usuários para aplicações LBS.

Algumas questões do modelo conceitual e dos requisitos de privacidade foram definidos a partir da nossa experiência, de trabalhos anteriores (29, 7, 9, 10, 14, 13) e derivados da análise dos resultados de uma pesquisa preliminar sobre as preferências de privacidade que realizamos com aproximadamente 120 usuários. Alguns resultados parciais dessa pesquisa estão disponíveis em (26, 27). No entanto, estamos cientes de que o modelo proposto não se aplica a determinados cenários (por exemplo, em redes *ad hoc* onde a inferência e a privacidade são tratadas de forma integrada) porque ele se baseia em uma abordagem centralizada e não atende a todos os possíveis requisitos de privacidade relacionados ao uso de aplicações LBS.

A seguir, descrevemos o modelo conceitual que especifica os papéis e o padrão de interação entre as entidades do sistema e discutimos algumas hipóteses consideradas no cenário de uso do serviço de privacidade proposto. Além disso, descrevemos alguns requisitos que devem ser considerados no projeto de um serviço de privacidade para tratar os principais desafios relacionados à configuração e à manutenção da política de privacidade do usuário.

3.1
Modelo conceitual

O modelo conceitual trata das questões de privacidade relacionadas ao acesso à informação de localização, apesar de também poder ser utilizado para gerenciar o acesso a outras informações de contexto (e.g., contexto computacional e pessoal do usuário). No modelo, cada usuário possui uma localização, representada por regiões simbólicas (organizadas hierarquicamen-

te), que pode variar no tempo. A informação de localização é inferida pelo serviço de contexto e repassada para as aplicações LBS. Essas aplicações usam essa informação para fornecer serviços ao próprio usuário ou a terceiros.

O modelo do serviço de privacidade proposto é formado por várias entidades cujos papéis são descritos como segue:

- *Sujeito (Subject)* é o usuário que tem a sua localização inferida pelo serviço de contexto;
- *Requisitante (Requester)* (um usuário intermediado por uma aplicação LBS) é a entidade que, após devidamente autenticada, solicita acesso à informação de localização de um Subject divulgada por um serviço de contexto;
- *Definidor da Política (PolicyMaker)* é o usuário responsável por definir (ou redefinir, caso já exista) a política de privacidade. Esse pode ou não ser o próprio Subject, pois o modelo proposto permite que tanto o usuário Subject quanto o administrador do sistema definam as políticas de privacidade;
- *Serviço de contexto* é a entidade responsável por processar as requisições dos Requesters, inferir e compartilhar a informação de localização do Subject mediante a autorização avaliada 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 através da qual o Subject controla e monitora o acesso a sua informação de localização no escopo das concessões e restrições da política de privacidade definida pelo PolicyMaker.

3.2 Padrão de interação

A Figura 3.1 ilustra o padrão de interação entre as entidades do modelo do serviço de privacidade.

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. A autenticidade da identidade do Requester deve ser garantida por algum serviço de autenticação da rede. Quando a requisição de acesso à informação de localização é recebida pelo serviço de contexto (3), ela é processada e repassada

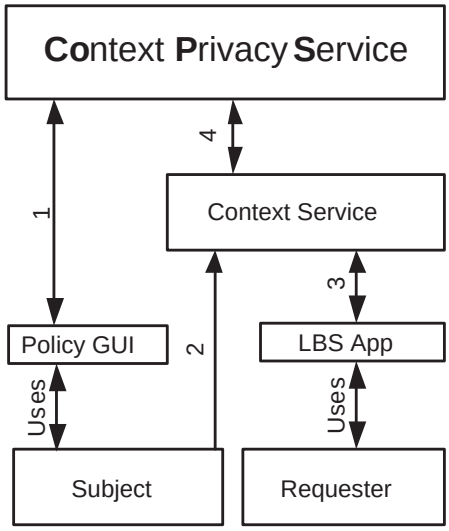

Figura 3.1: Padrão de interação

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" (4).

3.3 Hipóteses do modelo

Todo modelo é uma abstração da realidade que, para ser consistente e definir bem o seu escopo, precisa estar fundamentado em algumas hipóteses sobre as entidades do sistema. A seguir, enunciamos e discutimos as principais hipóteses adotadas no modelo.

- O Requester, Subject e o PolicyMaker possuem uma única identidade não forjável;
- O serviço de privacidade não trata das possíveis implicações do uso da informação de localização fora do seu propósito e contexto previsto;
- O Subject e o Requester são potenciais colaboradores e estão cientes dos benefícios e dos riscos relacionados à divulgação de sua informação de localização;
- Existe uma relação de confiança irrestrita entre os serviços que fazem parte do modelo conceitual;
- O serviço de privacidade deve ser utilizado em 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 departamento, ou por simplesmente se conhecerem pessoalmente.

Dentro do cenário de uso do serviço de privacidade, a autenticação do Requester deve ser realizada por um serviço de autenticação da organização. Por exemplo, um controlador de domínio da rede que pode usar uma PKI (*Public Key Infrastructure*) para tal propósito. Assume-se nesse cenário que o serviço de autenticação é capaz de garantir que cada usuário tenha uma identidade não forjável.

Conforme discutido em (8), *Grudin* destaca que o risco de privacidade não está ligado somente ao controle de acesso à informação de localização, mas também, na forma pela qual essa informação é armazenada, utilizada e divulgada pela rede. Uma vez que, após ter a sua localização divulgada, o usuário não tem mais controle sobre a mesma, ou seja, se ela será ou não divulgada pela rede, para quem será divulgada, por quanto tempo ela será armazenada em um meio digital, dentre outras questões. Nesse último caso, o usuário requisitante poderia usar a localização persistida como uma prova (e.g., em uma ação judicial) de que uma dada pessoa esteve em determinado lugar, em determinado momento. Além disso, a não-volatilidade da informação armazenada e a rapidez da sua difusão pela rede podem gerar danos irreparáveis ou inesperados com relação à maneira com que essa será interpretada fora do contexto em que foi gerada.

A justificativa para a restrição do modelo a um grupo cujos membros se conhecem mutuamente fora do ambiente computacional está baseada nos seguintes fatores:

1. Privacidade e segurança costumam confundir-se em alguns casos ou terem implicações recíprocas bastante fortes (por exemplo, alguns casos jurídicos utilizam a "escuta telefônica", já que a quebra de privacidade neste caso se justifica por valores maiores associados à segurança, como, por exemplo, a segurança pública).

2. O objetivo deste trabalho é tratar da questão da "privacidade" e não da questão da segurança (no sentido mencionado acima).

3. Os grupos de pessoas que se conhecem e se encontram freqüentemente são, em geral, formados por indivíduos que, em princípio, não representam, uns para os outros, qualquer ameaça de segurança. Portanto, podemos fatorar a questão de segurança e manter a questão de privacidade.

4. Mesmo em grupos de pessoas que se conhecem, a privacidade oferece algumas questões muito delicadas de se tratar - social ou psicologicamente. Portanto, a restrição em questão ainda mantém em pauta vários problemas importantes a serem resolvidos relacionados à privacidade.

Em nosso modelo, estamos considerando o uso do serviço de privacidade dentro de uma comunidade de usuários para tirar proveito da relação básica de confiança intrínseca ao ambiente social. Essa abordagem facilita a identificação dos possíveis tipos de requisitantes que devem ser considerados na definição da política de privacidade, pois, esses fazem parte da rede social de cada usuário. De acordo com o sociólogo Barry Wellman (86), comunidade é uma rede de ligações interpessoais que provê sociabilidade, auxílio, informação e identidade social. Dentro de uma comunidade existem referências pessoais diretas ou indiretas acerca dos membros participantes da mesma que permitem estabelecer um certo nível de confiança entre esses que pode, de certa forma, ser explorada no mundo digital. Conforme mostrado nos estudos feito por (10), dentro desse contexto no qual as pessoas se conhecem, por exemplo, por trabalharem/estudarem juntas, elas estão mais propensas a compartilhar mais informações pessoais e aumentar o nível de confiança das redes sociais. Além disso, a partir dos estudos descritos em (87), podemos concluir que o uso do serviço de privacidade dentro de uma comunidade de usuários em que as pessoas se conhecem pessoalmente e as suas identidades não podem ser forjadas, simplifica significativamente a definição e o gerenciamento da política de privacidade. Nesses estudos, mostrou-se que os usuários (e.g., Subjects) apresentaram uma maior predisposição para divulgar e ajustar a precisão da sua informação em função da identidade do Requester do que das circunstâncias em que a requisição foi recebida.

3.4 Cenários de aplicações LBS

Para ilustrar os tipos de aplicações atendidas pelo modelo conceitual do serviço de privacidade, são descritos a seguir dois cenários de uso de aplicações LBS e algumas questões de privacidade associadas ao uso das mesmas.

O primeiro cenário considera o uso de uma aplicação, conhecida como *People Finder*, através da qual o Requester solicita explicitamente a localização de um dado usuário para algum propósito específico, como, por exemplo, saber o local da reunião de um grupo de estudo do qual ambos fazem parte. No entanto, os usuários deste tipo de aplicação (i.e., os Subjects) podem ter certas preocupações com relação a invasão de sua privacidade. Por exemplo, a dificuldade de manter-se oculto à observação de terceiros, pois os Requesters, através da localização, poderiam deduzir certas informações sobre o padrão de comportamento dos Subjects. Por exemplo, a razão do seu atraso para uma reunião, o porquê do não comparecimento à aula, onde geralmente almoça, etc.

O segundo cenário ilustra o uso de aplicações LBS do tipo *Mural*

Virtual[1] (6) baseado em localização. Através dessa aplicação, usuários, por exemplo, professores e alunos, podem postar mensagens para determinados lugares geográficos representados como regiões simbólicas (e.g., Sala de aula 511, Corredor Sul do prédio RDC, Auditório 5, etc.) cadastradas no serviço de localização. Por exemplo, um professor poderia postar uma mensagem para seus alunos em uma dada sala de aula informando que chegará 15 minutos atrasado. Para entregar essa mensagem aos usuários presentes (ou que entrarem) na sala de aula, o servidor dessa aplicação solicita periodicamente a localização de todos os usuários registrados. Ao contrário do cenário de uso da aplicação *People Finder*, esta aplicação requisita ao serviço de localização, sem que seja necessária uma requisição explícita de um usuário, a informação de localização para desempenhar suas funções.

No entanto, tal funcionamento introduz certas preocupações de privacidade no que diz respeito ao uso da informação de localização obtida periodicamente. Após ter a sua localização divulgada sob as restrições da sua política de privacidade, o Subject perde completamente o controle sobre a mesma. Ou seja, ele não sabe como e por quanto tempo a sua informação de localização persistirá no servidor da aplicação, se esse mantém o histórico da mesma ou, até mesmo, se esse servidor divulgará tal informação pela rede. Além disso, existem outras preocupações relacionadas ao funcionamento da aplicação LBS que abrem caminho para uma invasão de privacidade. Por exemplo, o usuário da aplicação *Mural Virtual* poderia receber mensagens *SPAM* que não são do seu interesse. Contudo, ele não poderia especificar em sua política de privacidade que tipo de mensagens ele gostaria de receber, de quem, quando, com que periodicidade, etc., pois essas propriedades fazem parte da lógica de funcionamento da aplicação. Nessa situação, cabe ao administrador da aplicação moderar o conteúdo das mensagens postadas pelos usuários.

3.5 Requisitos do serviço de privacidade

A partir dos cenários discutidos na seção anterior, fica evidente a necessidade do serviço de privacidade contemplar funcionalidades que possibilitem aos usuários permitir, omitir ou negar acesso à sua localização em função da identidade do requisitante, do momento da requisição, do contexto corrente, da granularidade da informação requisitada, dentre outros. Nesta seção, são discutidos alguns requisitos de controle de privacidade que atendem a tais questões e que auxiliam os usuários a definirem e refinarem a sua política de priva-

[1]De fato, uma aplicação desse tipo foi implementada em nosso grupo.

cidade gradativamente, de acordo com as suas necessidades. Esses requisitos delinearam as decisões de projeto e implementação do CoPS.

3.5.1 Configuração da política de privacidade

Para atender às necessidades de privacidade de ambientes organizacionais e/ou de indivíduos específicos, o serviço de privacidade deve organizar as políticas de privacidade em uma hierarquia de três níveis: política da organização, política do usuário e política padrão. A política no nível da organização é definida pelo administrador do sistema e tem maior precedência sobre as demais. Essa política é utilizada pela corporação para impor certas práticas 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), independentemente se a política definida pelo usuário está negando acesso à mesma. Para aumentar o nível de transparência e confiança entre os usuários e a organização, o serviço de privacidade deve permitir que usuários visualizem as regras definidas pela organização. Além disso, essa política é facultativa, pois nem sempre é necessário ou desejável impor uma política de privacidade da organização. A política no nível de usuário é definida pelo próprio Subject e tem uma maior precedência em relação à política padrão definida pelo administrador do sistema.

Através da política padrão, que consiste de um *template* de regras que é associado a cada novo usuário do sistema, a organização pode determinar uma política de privacidade inicial que contempla as principais necessidades de privacidade dos usuários com o objetivo de minimizar os esforços na configuração inicial da política de privacidade. Em (12, 10) são apresentados resultados que demonstram que a 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.

No entanto, não existe um *template* padrão e único. Acreditamos que cada comunidade de usuários e indivíduos tem percepções diferentes sobre como as questões de privacidade devem ser tratadas. Sendo assim, cabe ao administrador do sistema identificar tais questões dentro do domínio em que o serviço de privacidade deve ser configurado, 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 artigo

(88) discute um modelo de propósito geral para identificação de riscos de privacidade que pode auxiliar o administrador do sistema nessa tarefa.

A fim de facilitar a definição da política de privacidade pelo usuário, o serviço de privacidade deve oferecer três políticas básicas de controle de acesso à informação de contexto: Reservado, Liberal e Sob-Demanda. No modo Reservado, por definição, todas as requisições são negadas, exceto aquelas que satisfazem alguma regra definida pelo usuário que libera o acesso. No controle de acesso Liberal, por definição, todas as requisições são aceitas, exceto aquelas que satisfazem alguma regra especificada pelo usuário 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. Essas três políticas básicas são apropriadas por refletirem as três atitudes fundamentais assumidas pelos usuários.

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 divulgadas. O PolicyMaker poderá mudar a sua política de controle de acesso corrente através da interface gráfica de configuração de regras. Tais políticas oferecem certas flexibilidades que amenizam o ônus da configuração da política de privacidade, pois após escolher a política de acesso Reservado ou Liberal, o PolicyMaker terá somente que especificar regras com um dos seguintes resultados: "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, interativamente, através da política Sob-Demanda, configurar a sua política de privacidade. As regras de privacidade definidas interativamente poderão também ser reaproveitadas para as outras duas políticas de acesso. Por exemplo, quando o Subject mudar a sua política de controle de acesso de Sob-Demanda para a política Reservado, as regras definidas interativamente que permitem determinados acessos (i.e., regras com resultados "Grant") podem ser reutilizadas nessa política mais conservadora. O mesmo se aplica quando ele mudar da política de acesso Sob-Demanda para a política Liberal, as regras definidas com resultado "Deny" podem ser reaproveitadas. As regras definidas interativamente com resultado "Not Available" e "Ask Me" podem ser reaproveitadas tanto para a política no modo "Reservado" quanto "Liberal".

O resultado "Not Available" que pode ser definido para algumas regras satisfaz o requisito de *plausible deniability* (89, 9). O objetivo desse tipo de resposta é negar o acesso à informação sem que o requisitante perceba que o acesso foi negado de forma proposital. Ao receber como resposta uma mensagem "Not Available", o requisitante não saberá se a resposta esperada

não foi obtida por causa de uma falha técnica do sistema, de um problema de comunicação, se a localização não pode ser inferida, ou se o Subject, de fato, negou acesso à mesma. O resultado "Ask Me" de uma regra de privacidade faz com que o serviço envie uma consulta de autorização de acesso ao Subject. Ao contrário da política Sob-Demanda, o resultado "Ask Me" pode ser utilizado em uma regra específica para configurar um controle de acesso interativo, no qual, o Subject deseja decidir de forma pontual, e a partir da situação e da informação sobre o Requester, se vai ou não divulgar a sua informação de localização.

Vale ressaltar que a configuração de uma nova regra de privacidade oferece ao Subject o bônus da privacidade da informação controlada e, por outro lado, o ônus de ter que se lembrar de desfazê-la ou removê-la quando a regra em questão não satisfaz mais as suas necessidades correntes. Por exemplo, um Professor pode definir uma regra que nega o acesso à sua localização aos seus alunos de Doutorado durante um determinado período. Provavelmente, ele deseja desfazê-la em algum momento seguinte. No entanto, tal regra só será anulada/removida pelo Professor quando ele se lembrar que adicionou uma regra que bloqueia tal acesso, ou quando um dos seus alunos comentar que não está conseguindo enviar uma mensagem para ele através da aplicação Mural Virtual, citada anteriormente. Com objetivo de amenizar o ônus da reconfiguração da política de privacidade, o serviço de privacidade deve permitir que o PolicyMaker defina regras temporárias que são automaticamente desabilitadas e removidas após um determinado período.

Segundo os resultados da pesquisa publicada em (10), a maioria dos usuários envolvidos nas entrevistas escolheu configurar suas permissões de privacidade usando grupos de usuários. Esses oferecem uma maior flexibilidade para controlar o acesso às informações pessoais e diminui consideravelmente o esforço envolvido na configuração das regras. De certa forma, essa funcionalidade também oferece uma maior transparência para os usuários estabelecerem um certo nível de confiança para com os possíveis requisitantes (e.g., Família, Colegas de trabalho). Sendo assim, para usufruir de tais benefícios, o serviço de privacidade deve oferecer suporte a grupos de usuários na configuração das regras de privacidade.

3.5.2 Refinamento e manutenção da política de privacidade

As questões relacionadas à definição e manutenção da política de privacidade representam os maiores desafios a serem atendidos pelos serviços de privacidade. Em (13) são discutidos alguns desafios em relação a essas questões

segundo o ponto de vista do psicólogo social Irwin Altman (33). Ao invés de compreender privacidade como um estado do retrocesso social, Altman a interpreta como sendo um processo de ajuste das fronteiras dialéticas e dinâmicas do comportamento social, das informações, etc. Como um processo dialético, o ajuste da privacidade está condicionado pela nossa expectativa e experiência, e condicionado pela expectativa e experiência daqueles com os quais nós interagimos. Como um processo dinâmico, privacidade requer uma negociação e gerenciamento contínuo das fronteiras que distinguem o que é privativo daquilo que é público de acordo com as circunstâncias/o contexto. Sendo assim, podemos concluir que os usuários, no dia a dia, necessitam freqüentemente refinar as suas políticas para revelar as informações adequadas para as pessoas certas nos momentos certos.

Com intuito de atender a tais necessidades, o serviço de privacidade deve oferecer as seguintes funcionalidades para auxiliar a tarefa de refinamento e manutenção da política de privacidade: notificações de requisições de acesso ao contexto (i.e., acesso à localização), relatório estatístico de acesso, controle de acesso interativo e regras temporárias. Essas foram definidas a partir da pesquisa preliminar com usuários e a partir dos resultados de pesquisa apresentados por outros grupos de trabalho (7, 89, 9).

Durante a configuração de uma regra, o PolicyMaker deve poder especificar o tipo de notificação (e.g., e-mail, mensagem SMS) a ser enviada ao Subject quando uma tentativa de acesso à sua localização for recebida. Nós acreditamos que tal funcionalidade aumenta o nível de transparência sobre quem está tentando acessar o quê e com que periodicidade e, conseqüentemente, pode ser utilizada como um parâmetro de decisão para a atualização das regras de privacidade. Além disso, essa funcionalidade cria, implicitamente, um protocolo social entre os usuários da comunidade que pode evitar determinadas ações maliciosas. O fato dos Requesters estarem cientes de que o Subject pode estar sendo notificado a cada tentativa de acesso pode inibir certas atitudes que caracterizam uma invasão de privacidade. Por exemplo, considerando a aplicação *People Finder*, um Requester (e.g., o orientador de João) poderia se sentir inibido a fazer repetidas consultas à localização de João para não criar uma situação embaraçosa/constrangedora entre eles.

Além das notificações, o serviço de privacidade também deve oferecer ao Subject relatórios de acesso à informação de localização representados hierarquicamente pela granularidade dos acessos no ano, meses, semanas e dias. Através destes, é possível obter informações estatísticas dos acessos bem ou mal sucedidos de um Requester específico (ou de grupos de Requesters) através das estatísticas de acesso do ano (raiz da hierarquia), meses, semanas e dias (folha).

Além disso, para facilitar a manutenção da política de privacidade, o Subject pode visualizar nos relatórios a regra que permitiu ou bloqueou uma dada tentativa de acesso. O Subject também pode configurar em suas preferências a periodicidade com a qual ele gostaria de receber (por exemplo, via e-mail) um relatório com as estatísticas de acesso de um período específico (e.g., última semana, último mês, ...). Nós acreditamos que tais informações aumentam o nível de controle e confiança do usuário para com o sistema e aumentam o nível de transparência sobre quem conseguiu ou não conseguiu acessar quais informações, com que periodicidade tais tentativas ocorreram, etc. Além disto, essas informações revelam a variação (aumento ou decréscimo) do número de tentativas de acesso em certo período como, por exemplo, entre dias, semanas, ou meses diferentes, dentre outros. A partir dessas informações, o Subject pode modificar, se necessário, as regras da sua política de privacidade.

Além das funcionalidades supracitadas, acreditamos que a política de acesso Sob-Demanda e a opção de resultado "Ask Me" também facilitam o processo de manutenção da política do usuário. Através dessas, o Subject pode implementar um controle de acesso interativo, através do qual ele pode determinar gradativamente o que deve ser permitido ou negado a determinados grupos de usuários ou indivíduos específicos. Além disso, conforme explicado anteriormente, as regras temporárias também diminuem os esforços de gerenciamento da política de privacidade.

3.5.3 Controle de acesso

Com o intuito de oferecer um controle de acesso flexível, o serviço de privacidade deve permitir ao Subject ajustar 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 da aplicação *People Finder*. No entanto, João pode não se sentir confortável em compartilhar 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 am). 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 alguns minutos atrás deve ser divulgada. Cabe ao serviço de contexto

divulgar a localização do usuário com a precisão informada em sua política de privacidade. Para tanto, o serviço de contexto deve manter um histórico da informação a ser divulgada.

De acordo com os trabalhos de Goffman em (90), as pessoas incorporam/assumem diferentes papéis no convívio em sociedade que, por sua vez, revelam a nossa face ou aspectos diferentes sobre nós mesmos. Por exemplo, muitas pessoas assumem e mantêm diferentes posturas e estereótipos no relacionamento com os seus subordinados ou superiores dentro do ambiente de trabalho, e que geralmente difere do estado descontraído e/ou brincalhão assumido com os amigos mais íntimos ou familiares. Isso nos leva a acreditar que, para o controle da privacidade, alguns usuários desejam definir a sua política de privacidade em função do papel específico que estão desempenhando a cada momento. Alguns desses estados, por exemplo, "Descansando", "Em Reunião", "Ocupado", dentre outros, podem representar papéis/situações comuns de um usuário, mas que somente ele próprio pode determinar. E, para cada papel/situação, provavelmente, o usuário tenha necessidade de definir uma política de privacidade específica e adequada à situação.

Para satisfazer esse requisito, o serviço de privacidade deve permitir ao PolicyMaker criar *Perfis de privacidade*, nos quais ele seja capaz de definir políticas de acesso específicas em função do papel/situação em que o Subject pode estar engajado. Ou seja, ao selecionar manualmente o perfil "Em Reunião", somente as regras que regem a política de privacidade do usuário nessa situação (ou durante essa atividade) serão aplicadas ao controle de acesso ao contexto. De uma certa forma, além de modularizar a política de privacidade facilitando a sua definição/configuração, essa funcionalidade também auxilia os usuários a terem uma visão/percepção mais clara do que está sendo permitido ou negado em cada papel/situação. Por exemplo, após selecionar um determinado perfil, digamos, "Descansando", João estaria ciente de que a única pessoa que poderia localizá-lo, através da aplicação *People Finder*, seria a sua esposa.

Além dos perfis de privacidade, o serviço de privacidade deve permitir que um usuário fique "invisível" para requisições de terceiros. Para tanto, o serviço deve oferecer uma funcionalidade, chamada *"Modo Invisível"*, a partir da qual, o sistema negará qualquer acesso à localização do usuário retornando uma mensagem "Not Available" aos requisitantes, para tirar proveito das vantagens da *plausible deniability*.

Nos estudos reportados em (11) sobre violação de privacidade em sistemas de comunicação multimídia, é ressaltada a preocupação dos usuários em relação ao uso da informação divulgada. A partir das avaliações realizadas com

um grupo de usuários, foi identificado que a maioria gostaria de saber para que fim a sua informação está sendo coletada, qual é o risco *versus* o benefício envolvido na divulgação da informação, etc. Diante de tais questões, o serviço de privacidade deve implementar uma funcionalidade, conhecida por "Contrato de uso de contexto", que torna explícito para quê o Requester deseja obter a localização do Subject e o que será feito com a mesma. Essa funcionalidade é extremamente útil para aplicações semelhantes ao *LBS Mural Virtual*. Como descrito anteriormente, essa aplicação monitora a localização dos usuários com o objetivo de postar mensagens para os mesmos sempre que esses entrem em uma determinada área lógica.

A fim de esclarecer as questões de privacidade relacionadas ao uso da aplicação *Mural Virtual* discutidas na Seção 3.4, no modelo proposto, o serviço de privacidade deve permitir que a aplicação envie ao Subject a descrição do "Contrato de uso do contexto". Este pode apresentar ao usuário uma descrição clara dos riscos/benefícios em divulgar a informação de localização em diferentes granularidades, explicitando para quê tal informação será utilizada, por quanto tempo será armazenada, se será divulgada para terceiros, dentre outros. Cabe então ao Subject deferir o resultado final da consulta liberando ou não o acesso à sua localização a aplicação. Naturalmente, nesse cenário, configura-se uma relação de confiança do usuário em relação à aplicação, pois aquele não saberá se essa honrará o contrato pré-estabelecido entre eles. Cabe ao administrador do sistema identificar potenciais problemas deste tipo e adotar medidas preventivas ao uso de aplicações maliciosas que possam desrespeitar tais contratos.

Para oferecer uma maior flexibilidade no controle de acesso, o serviço de privacidade deve permitir que os usuários definam regras gerais e regras mais específicas. Naturalmente, as regras mais específicas devem ter maior precedência sobre as regras gerais que se aplicam a uma mesma requisição. Por isto, necessita-se de um algoritmo de especificidade que seleciona dentre todas as regras que se aplicam a uma requisição, aquela que seja mais específica. Com esse controle mais flexível e de granularidade fina, o usuário pode especificar para cada regra um tipo de notificação diferente, ajustar a granularidade da informação a ser revelada, restringir o acesso a um grupo específico em um período/horário predeterminado, etc.

3.6 Discussões

Neste capítulo, descrevemos o modelo conceitual de um serviço de privacidade integrado a uma infra-estrutura de provisão de contexto (e.g.,

localização) centralizada, e descrevemos algumas hipóteses que devem ser consideradas ou tratadas em um serviço do gênero. Além disso, com base em estudos de trabalhos relacionados e a partir da nossa experiência em questões relacionadas à privacidade de aplicações LBS, derivamos uma série de requisitos relativos à definição, manutenção da política de privacidade e mecanismos de controle de acesso que podem ser utilizados como base para o projeto e implementação de um serviço de privacidade.

O modelo conceitual e os requisitos de privacidade têm o propósito de refinar as discussões conceituais abstratas de privacidade em possíveis soluções concretas para tratar de privacidade no uso de aplicações LBS. No entanto, estamos cientes de que parte do projeto do modelo conceitual proposto atende somente a determinados tipos de sistemas, por exemplo, a definição dos papéis e a interação entre as entidades do modelo conceitual são específicas para um serviço de privacidade centralizado. Além disso, os requisitos levantados não contemplam ou tratam todas as possíveis questões a serem consideradas no projeto de um serviço de privacidade. Entretanto, esses servem como guia para os desenvolvedores refletirem sobre o impacto social e organizacional da privacidade no uso de aplicações sensíveis a localização e, na medida do possível, projetarem e implementarem soluções adequadas aos problemas discutidos. No próximo capítulo, descrevemos a arquitetura e implementação do serviço de privacidade proposto.