7
Conclusões

Os riscos de privacidade podem ser um empecilho para a evolução e aceitação das tecnologias sensíveis ao contexto, em especial, daquelas que usam a informação de localização. Muitos usuários não se importariam em divulgar a sua localização se pudessem usufruir de certos serviços, como, por exemplo, serem capazes de encontrar outras pessoas co-localizadas que tivessem interesses, afinidades ou *hobbies* similares, ou que pudessem esclarecer uma dúvida sobre um trabalho, etc. No entanto, que riscos esses usuários estão dispostos a assumir para usufruir de tais serviços? O que esses usuários achariam desses serviços se soubessem que poderiam ser lesados financeiramente ou fisicamente (e.g., serem assaltados) pelo simples fato de estarem divulgando sua localização ou outra informação contextual para outras pessoas?

Apesar dos benefícios que podem ser obtidos a partir de aplicações sensíveis ao contexto, as questões de privacidade devem ser investigadas e tratadas cuidadosamente. Deve-se permitir que o usuário seja capaz de controlar a sua privacidade a fim de limitar os possíveis riscos envolvidos na divulgação da informação contextual. Com esse propósito, definimos e implementamos um serviço de privacidade através do qual os usuários podem controlar o quê, quando, com que precisão e para quem as suas informações de contexto (e.g., localização) podem ser divulgadas.

Nesta tese, analisamos e identificamos vários requisitos que devem ser atendidos por um serviço de privacidade para aplicações sensíveis ao contexto, em particular para aplicações baseadas em localização. A partir do modelo e dos requisitos discutidos no Capítulo 3, da implementação de um serviço de privacidade descrita no Capítulo 4 e da avaliação das funcionalidades deste serviço realizada no Capítulo 5, nós mostramos que é possível usufruir dos benefícios oferecidos pelas aplicações sensíveis ao contexto sem abrir mão de um controle maior da privacidade. De fato, um controle total da privacidade não pode ser garantido. Como discutido no Capítulo 1, a localização do usuário pode ser inferida de diferentes maneiras em diferentes granularidades: por um serviço de localização, pelo endereço IP do seu dispositivo registrado nos arquivos de *log* de um serviço, por uma câmera de segurança de um prédio, etc.

Entretanto, cada tecnologia deve (ou deveria) tratar as questões de privacidade envolvidas na sua utilização para garantir a privacidade dos usuários. Conforme postulado por Mark Weiser (118), a tecnologia deve estar condicionada às necessidades dos usuários, e não o contrário.

Com intuito de tratar as questões de privacidade relacionadas à divulgação da informação fornecida por um serviço de localização, projetamos um serviço de privacidade (chamado CoPS) que ajuda o usuário a definir e gerenciar a política de privacidade da sua informação de localização.

As duas principais questões com as quais nos deparamos em relação ao projeto do CoPS foram: Dado que privacidade é um conceito abstrato, subjetivo e fortemente dependente das circunstâncias em que é considerada, como poderemos identificar um conjunto de requisitos de privacidade relevantes para os usuários? Não menos importante, como poderemos oferecer mecanismos eficientes e flexíveis de gerenciamento da política de privacidade dos usuários, e ao mesmo tempo reduzir a complexidade envolvida neste gerenciamento?

Nós desempenhamos duas atividades para estabelecer os requisitos relevantes para os usuários: primeiro, fizemos um estudo aprofundado de outros trabalhos que discutem questões gerais de privacidade envolvidas no projeto e uso de tecnologias mediadas pelo usuário. Segundo, fizemos uma pesquisa preliminar com 120 usuários para identificar as suas expectativas e preocupações em relação a algumas questões de privacidade (27) associadas ao uso de aplicações LBS. Conforme mostrado na Seção 1.3, uma das conclusões deste experimento foi: *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. No CoPS, uma das nossas principais preocupações foi a de oferecer um serviço que permita ao usuário usufruir dos mecanismos de controle de privacidade sem precisar lidar com as complexidades de configuração e manutenção da política de privacidade.

A flexibilidade mencionada diz respeito às opções de controle de privacidade que permitem ao usuário disponibilizar suas informações de contexto quando desejado e, ao mesmo tempo, usufruir de mecanismos que lhe auxiliem a identificar e inibir eventuais abusos ou ações consideradas intrusivas. No Capítulo 3, definimos um modelo conceitual e um conjunto de requisitos de privacidade com o intuito de refinar as discussões conceituais abstratas de privacidade em possíveis soluções concretas. O modelo e os requisitos auxiliam o projeto e o desenvolvimento de um serviço de privacidade para aplicações sensíveis ao contexto que ofereça tal flexibilidade.

Para amenizar a complexidade envolvida na configuração e manutenção da política de privacidade, o modelo e os requisitos propostos oferecem diversos recursos que permitem ao usuário configurar e refinar a sua política de privacidade gradativa - interativamente.

No entanto, estamos cientes de que o modelo conceitual proposto atende somente a determinados tipos de infra-estruturas de localização. Por exemplo, a definição dos papéis e da interação entre as entidades do modelo conceitual são específicas para um serviço de privacidade centralizado. Além disso, os requisitos definidos não contemplam todas as possíveis questões a serem consideradas no projeto de um serviço de privacidade. Isso decorre do fato de tais requisitos serem intrinsecamente dependentes das necessidades dos usuários. Logo, conforme argumentado na Seção 1.1, inferir as reais necessidades de todos os usuários é praticamente impossível.

Um diferencial do CoPS, comparado a outros serviços de privacidade (30, 93, 94), é o gerenciamento de granularidade fina das políticas de privacidade dos usuários implementado pelo algoritmo de especificidade. Este algoritmo permite que os usuários possam configurar diferentes tipos de notificações de acesso ao contexto e diferentes níveis da precisão da localização divulgada para cada grupo de requisitante. Por exemplo, um usuário poderia configurar em suas preferências que, durante o horário de trabalho os membros do grupo "Colegas de trabalho" podem saber em que prédio ele se encontra, e os membros do grupo "Amigos" podem obter a sua localização exata após o expediente de trabalho e nos fins de semana. Caso exista algum membro comum aos dois grupos, o algoritmo de especificidade identifica e resolve possíveis conflitos a fim de escolher uma única regra definida pelo usuário que determinará o que deve ser divulgado.

Para avaliar algumas hipóteses de usabilidade do CoPS, fizemos uma avaliação qualitativa através de experimentos com usuários. Estes experimentos visaram a descobrir se os mecanismos de controle de privacidade deste serviço são considerados efetivos e úteis atendendo às expectativas dos usuários no controle de sua privacidade no uso de uma aplicação LBS. Mais especificamente, nesses experimentos avaliamos como um conjunto de usuários (dentro de seus contextos social e cultural) usam os controles de privacidade do CoPS quando são expostos a situações que suscitam questões de privacidade.

A partir dos experimentos realizados, pudemos identificar opiniões e atitudes dos usuários que reforçam as hipóteses de usabilidade do CoPS: *os usuários expressaram o desejo de manter um compromisso entre sociabilidade e privacidade, disponibilizando a sua localização com diferentes granularidades para diferentes grupos de requisitantes.* Além disso, conforme discutido no

Capítulo 5, os usuários afirmaram que a aceitabilidade das aplicações LBS depende da existência e da eficácia dos mecanismos de controle de privacidade.

Outra conclusão interessante obtida nos experimentos com usuários foi a diferença entre aquilo que eles expressaram fora do contexto (i.e., nas entrevistas) e o que eles efetivamente fizeram no contexto (i.e., no jogo). Por exemplo, durante as entrevistas alguns usuários afirmaram que não bloqueariam o acesso à informação de sua localização para o grupo adversário, mas, durante o jogo simulado, diante do mesmo cenário exposto na entrevista, eles bloquearam. Além disto, identificamos que os usuários apresentaram certas opiniões ou atitudes opostas aos reais benefícios do projeto de uma funcionalidade 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 expressam 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 uma determinada coisa, que preferem *de uma forma* ou *de outra*, mas quando expostas à necessidade concreta de uso das funcionalidades deparam-se com as implicações de todos estes desejos e preferências. As complicações (e.g., complexidade de uso) envolvidas são muitas e, de fato, acarretam inúmeros problemas, na maioria das vezes, imprevistos.

Com base nos estudos de trabalhos relacionados e nos experimentos e entrevistas realizadas com usuários, verificamos que as questões de privacidade não se restringem apenas a desafios técnicos. É importante que a pesquisa sobre a proteção e controle de privacidade leve em consideração as necessidades dos diferentes domínios e comunidades de usuário, estudando, por exemplo, regras sociais, a cultura e o grau de aceitação de inovações tecnológicas, etc. Assim, fica evidente que tal pesquisa requer um trabalho interdisciplinar.

Além do estudo sobre privacidade, trabalhamos na definição e projeto de uma arquitetura de provisão de contexto chamada MoCA, e no projeto e implementação dos serviços e das APIs de comunicação que constituem o núcleo desta arquitetura. Estes serviços foram propostos com o intuito de auxiliar o desenvolvimento de aplicações sensíveis ao contexto e, de fato, têm sido utilizados como base para o desenvolvimento de várias dessas aplicações (4) e de novos serviços de provisão de contexto (5, 85).

Durante o projeto e implementação da MoCA, nós nos deparamos com vários desafios no desenvolvimento dos serviços de provisão de contexto. Alguns desses desafios estão relacionados à complexidade de implementação do Monitor para diferentes plataformas e sistemas operacionais, ao número limitado de

dispositivos portáteis que nos permitissem testar (em um cenário real) a escalabilidade dos serviços e o esforço despendido com a implementação das APIs de comunicação e do serviço de provisão de contexto (CIS).

O CoPS foi integrado aos serviços de contexto da MoCA com o intuito de adicionar à arquitetura um controle de privacidade para aplicações sensíveis ao contexto. Como foi mostrado no Capítulo 6, a maioria das arquiteturas de provisão de contexto não lidam com questões de privacidade, ou oferecem uma solução parcial e pouco efetiva.

7.1 Contribuições

As principais contribuições desta tese são: i) a definição de um modelo conceitual e de um conjunto de requisitos para o projeto de serviços de privacidade, ii) a implementação de um serviço de privacidade; iii) o projeto de um algoritmo de especificidade para análise de regras de privacidade; iv) a instanciação de um conjunto de métodos de avaliação qualitativa de usuários; v) o projeto de uma arquitetura de provisão de contexto e a implementação de alguns serviços que constituem o núcleo desta arquitetura.

Modelo conceitual e requisitos para um serviço de privacidade: A pesquisa preliminar com usuários e o estudo de outros trabalhos relacionados a nossa pesquisa nos possibilitaram definir um modelo conceitual e identificar alguns requisitos essenciais para o projeto de um serviço de privacidade. Esses requisitos sugerem que o projetista deva oferecer flexibilidade e reduzir a complexidade e o esforço da configuração e manutenção da política de privacidade.

Os requisitos e as discussões sobre privacidade também podem ser utilizados por outros trabalhos que desejem tratar as questões de privacidade no projeto e utilização de uma aplicação sensível ao contexto. Em particular se esta aplicação tem como objetivo servir aqueles que vão, em última instância, decretar o seu valor e a sua relevância - os usuários.

Serviço de privacidade: O modelo conceitual e os requisitos de privacidade delinearam a implementação do serviço de privacidade proposto - o CoPS. Este, por sua vez, foi integrado à arquitetura MoCA para oferecer um controle de privacidade para aplicações sensíveis ao contexto. Nós projetamos o CoPS para ajudar o usuário a definir e redefinir a sua política de privacidade dinamicamente durante o uso da aplicação, não requerendo que ele conheça, a priori, todas as possíveis situações em que gostaria de negar ou disponibilizar uma dada informação de contexto.

Algoritmo de especificidade: O CoPS oferece ao usuário vários mecanismos de controle de privacidade que o ajudam a definir e manter a sua política de privacidade. Dentre esses, está a configuração de políticas de privacidade usando grupos de requisitantes. No entanto, o uso de grupos implica que mais de uma regra de privacidade pode ser selecionada para avaliar uma dada requisição de acesso ao contexto. Para resolver o conflito entre essas regras, definimos um algoritmo de especificidade para selecionar a regra mais específica definida pelo usuário que se aplica à requisição.

Instanciação de métodos de avaliação qualitativa de usuários: Nós realizamos uma avaliação qualitativa das hipóteses de usabilidade do CoPS através de experimentos com usuários. Um dos principais desafios com os quais nos deparamos foi a forma de coletar e interpretar as evidências sobre as opiniões dos usuários a respeito dos controles de privacidade do CoPS. Em função disso, acreditamos que a metodologia de avaliação definida e discutida no Capítulo 5 pode ser seguida por outros trabalhos para avaliar uma tecnologia em que a percepção de utilidade e efetividade de suas funcionalidades dependam diretamente da opinião dos usuários.

Os experimentos com usuários também identificaram alguns desafios na área de IHC relacionados ao projeto de interfaces para aplicações sensíveis à privacidade que devem ser levados em conta pelo projetista. Por exemplo, considerando que a percepção e o desejo por privacidade é estritamente dependente do usuário e do contexto, surgem inúmeros desafios sobre a maneira de expor as funcionalidades do serviço para o usuário final de uma forma simples e não-intrusiva. Devemos estar atentos para o fato de que as circunstâncias em que o usuário deseja alterar a sua política de privacidade pode mudar muito. Portanto, o leque de opções de controle de privacidade utilizadas a cada momento pode também variar na mesma proporção, e, isto, pode representar um grande desafio para o projeto da interface de interação com o usuário. Algumas sugestões dos usuários para a interface de gerenciamento de regras incluem a implementação de uma abstração da apresentação das notificações (e.g., notificar o usuário somente se houver "várias" tentativas de acesso do mesmo requisitante) e a seleção de perfis de privacidade baseada na localização do usuário.

Arquitetura de provisão de contexto: Nós projetamos e implementamos a arquitetura MoCA, cujo objetivo é auxiliar o desenvolvimento de aplicações sensíveis ao contexto. Além de ser utilizada para ganharmos experiência no desenvolvimento de tais aplicações, esta arquitetura também serviu de base

para o desenvolvimento de outras pesquisas de mestrado (5, 85, 84) e de doutorado (74, 109) realizadas no laboratório LAC e em outros grupos de pesquisa (82, 83). Além disto, nos últimos dois anos, os serviços da MoCA têm sido utilizados pelos alunos da disciplina de computação móvel ministrada no DI/PUC-Rio para desenvolver aplicações e serviços sensíveis ao contexto. A partir de questionários respondidos pelos alunos pudemos evidenciar o quanto a arquitetura pode facilitar e agilizar o desenvolvimento de novas aplicações.

7.2 Trabalhos futuros

Inicialmente, trabalharemos no projeto de uma interface de gerenciamento de políticas de privacidade. Dada a importância desta interface para o uso do CoPS, faremos uma análise dos seus requisitos desejáveis a partir das discussões descritas nesta tese e investigaremos outros trabalhos que apresentam sugestões para o projeto de interfaces do gênero (119, 120). Em seguida, pretendemos estender as aplicações LBS implementadas (4) para tratar das questões de privacidade discutidas.

Além disso, pretendemos fazer uma nova pesquisa com usuários a partir das aplicações implementadas para contrastar os resultados dos experimentos realizados a partir do simulador do jogo com os resultados obtidos em um experimento com aplicações implantadas em um cenário real, como, por exemplo, em um Campus universitário.

Embora as funcionalidades providas pelo CoPS visem a auxiliar o Subject a manter a sua privacidade, estamos cientes que o uso das mesmas, se mal projetadas, podem ser um meio a partir do qual os Requesters possam deduzir o comportamento do Subject, violando assim a sua privacidade. Por exemplo, a partir das informações implícitas ao funcionamento do sistema, o Requester pode inferir que a resposta foi analisada e processada pelo serviço de privacidade (via algoritmo de especificidade), caso ela tenha sido recebida imediatamente após a requisição; ou pode deduzir que ela foi enviada pelo Subject que está utilizando a política de acesso Sob-Demanda se o tempo de resposta exceder o tempo usual de uma consulta processada diretamente pelo CoPS. Dessa forma, ao receber um "Not Available", um dado Requester poderia concluir que o Subject não deseja disponibilizar a sua localização para ele. Isso vai contra os princípios e benefícios da *plausible deniability* e pode gerar sérios problemas sociais entre os usuários em uma comunidade que socialmente preza pela confiança mútua. Para tratar essas questões pretendemos projetar um protocolo que emprega um padrão de envio de resposta randômico, independente do estado de configuração da política do Subject. Além disso, pre-

tendemos averiguar a partir do uso de aplicações LBS outros possíveis canais escondidos/ocultos que podem revelar o comportamento do usuário.

Apesar de não termos incorporado no CoPS mecanismos que garantam o anonimato na comunicação, pretendemos investigar como alguns dos mecanismos de anonimato existentes (20, 19) podem ser integrados à sua arquitetura para que os usuários possam ocultar suas identificações, quando necessário.

A versão preliminar do CoPS implementa alguns dos requisitos de privacidade discutidos tais como algoritmo de especificidade, restrições espacial e temporal, dentre outros. No entanto, pretendemos aprimorar o projeto inicial do CoPS a partir das seguintes atividades futuras:

- Especificar a estrutura das regras de privacidade de acordo com o padrão P3P - *Platform for Privacy Preferences* (115), melhorando assim, a extensibilidade e a facilidade de integração com outros serviços;
- Implementar a abordagem de controle de acesso interativo requerido pelas regras de privacidade com resultado "Ask Me";
- Oferecer uma funcionalidade de pré-configuração de perfis de privacidade através da qual o usuário possa automatizar a seleção de seus perfis de acordo com a sua localização;
- Avaliar os desafios de como implantar e configurar o serviço de privacidade em um cenário real. Investigar e experimentar como devem ser tratadas as questões de autenticação, mobilidade do usuário, comunicação intermitente, configuração inicial do serviço, etc.;

Além das questões de coleta e de difusão da informação, as arquiteturas de provisão de contexto também precisam lidar com outros desafios inerentes às redes sem fio, entre eles, mobilidade dos usuários, comunicação intermitente e limitação dos recursos computacionais. Alguns desses desafios estão relacionados ao gerenciamento de mobilidade, à descoberta dinâmica de serviços, à transferência do estado da comunicação nas operações de *roaming*, implementação e gerenciamento de *caching* local para tratar das operações desconectadas, etc. A MoCA ainda não oferece soluções para esses problemas, no entanto, a longo prazo, pretendemos tratar essas questões nos trabalhos futuros.

Alguns trabalhos futuros relacionados aos serviços de provisão de contexto da MoCA que pretendemos solucionar a curto prazo são listadas a seguir:

- Desenvolver aplicações sensíveis ao contexto e à privacidade;
- Incentivar o uso de aplicações LBS para a comunidade de uma universidade;

- Implementar ferramentas para depuração e rastreamento de falhas na comunicação distribuída entre os serviços;
- Desenvolver um gerenciador de instalação dos serviços da MoCA.