1
Introdução

A difusão dos dispositivos portáteis (e.g., *Palmtops* e *Laptops*), das tecnologias de rede sem fio e de localização (e.g., RFID, GPS) tem impulsionado e motivado o desenvolvimento de aplicações sensíveis ao contexto e à localização. Normalmente, estas aplicações usam o contexto computacional (e.g., nível de energia, largura de banda), pessoal (e.g., perfil, localização do usuário) ou físico (e.g., temperatura, umidade) 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 a partir da informação de localização, adaptar o comportamento da aplicação de acordo com as limitações dos dispositivos (e.g., nível de energia da bateria) ou da rede (e.g., largura de banda), etc. De fato, são muitas as suas possibilidades.

Entretanto, apesar das informações contextuais oferecerem uma grande variedade de novas possibilidades para implementar aplicações colaborativas (distribuídas), a provisão destas informações ainda apresenta vários desafios por causa da complexidade envolvida na sua coleta e no seu processamento. A diversidade de informações de contexto que podem ser exploradas e a abundância de tecnologias de sensoriamento tornam cada vez mais complexo o desenvolvimento e a implantação de sistemas sensíveis ao contexto (1). Sendo assim, é necessário desacoplar a lógica da aplicação do *software* e *hardware* responsáveis pelo sensoriamento/coleta de contexto por dois motivos principais: i) por causa da sobrecarga de desenvolvimento requerida na interação com os sensores para realizar a coleta; e ii) por causa da sobrecarga no processamento da informação coletada. Essas razões se justificam ainda mais se considerarmos que as aplicações sensíveis ao contexto podem estar executando em dispositivos móveis com capacidade e recursos computacionais limitados. Além disto, o desacoplamento é importante para permitir o compartilhamento do sistema de provisão de contexto para várias aplicações.

Com o intuito de oferecer uma infra-estrutura que auxiliasse o desenvolvimento de tais aplicações, trabalhamos na definição e no projeto de uma arquitetura de provisão de contexto chamada **M**obile **C**ollaboration **A**rchitecture

- MoCA (2, 3). Além disso, implementamos alguns serviços que constituem o núcleo desta arquitetura. Estes realizam a coleta, o processamento e a divulgação do contexto computacional dos dispositivos móveis e da rede sem fio IEEE 802.11. Esses serviços têm sido utilizados como base para o desenvolvimento de várias aplicações sensíveis ao contexto (4) e de novos serviços que manipulam informações de contexto mais básicas para derivar outras de mais alto nível. Por exemplo, o serviço de localização integrado à MoCA, LIS - *Location Inference Service* (5), utiliza as informações de RSSI (*Received Signal Strength Indicator*) dos pontos de acesso fornecidas pelo serviço de contexto para inferir e divulgar a informação de localização de um usuário em uma rede sem fio IEEE 802.11.

As aplicações desenvolvidas através da MoCA nos ajudaram a avaliar e testar os serviços de provisão de contexto e, dentre estas, podemos destacar aquelas que usam a informação de localização de um usuário para desempenhar as suas funções (também conhecidas como aplicações LBS - *Location-Based Services*). Por exemplo, através da aplicação LBS chamada NITA - *Notes In the Air* (6), um usuário poderia criar murais virtuais que o permitissem postar mensagens a serem entregues a todos os usuários localizados em uma determinada área/região.

De fato, o avanço da tecnologia e a nova geração de serviços e aplicações sensíveis ao contexto oferecem inúmeros benefícios para a sociedade em geral. Entretanto, essas mesmas tecnologias introduzem novos riscos e ameaças à nossa privacidade. Por exemplo, através de uma aplicação *Friend Finder*, um professor poderia ficar ciente de que um de seus alunos não compareceu à reunião por que ele estava no *coffee-break* de um evento (previamente anunciado a todos). Esta situação poderia gerar um problema social (gravíssimo) se este aluno disser para o seu orientador que não pode comparecer à reunião porque ficou preso no trânsito.

Com base nos argumentos descritos em (7), acreditamos que 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, como, por exemplo, preferências pessoais, localização, atividade corrente, etc. Vários artigos (7, 8, 9, 10, 11, 12, 13, 14, 15) e livros (16, 17), discutem questões relacionadas à perda de privacidade e destacam a preocupação dos usuários em determinar como as suas informações serão armazenadas, divulgadas e usadas por terceiros.

Essas preocupações apontam para a necessidade de serviços e aplicações sensíveis ao contexto que tratem das questões de privacidade relacionadas ao seu funcionamento. No entanto, poucos trabalhos apresentam uma proposta

concreta para lidar com essas questões no desenvolvimento de tais aplicações. Outros tratam somente de alguns aspectos básicos da privacidade, como, por exemplo, o anonimato (18, 19, 20, 21) ou a autenticação (22, 23) de acesso à informação do usuário, não oferecendo flexibilidade para os casos em que o usuário deseja também divulgar as suas informações (e.g., identidade pessoal, localização, perfil) para tirar proveito dos serviços disponíveis para colaboração e comunicação. A flexibilidade mencionada diz respeito aos recursos tecnológicos que permitem ao usuário disponibilizar suas informações quando desejado e, ao mesmo tempo, usufruir de mecanismos que lhes permitam identificar e inibir eventuais abusos ou ações consideradas intrusivas.

Com o intuito de oferecer um serviço de privacidade com tal flexibilidade, estamos propondo, como uma das principais contribuições deste trabalho, o CoPS - **Co**ntext **P**rivacy **S**ervice. Através deste serviço, os usuários podem definir e gerenciar a sua política de privacidade para controlar o acesso à sua informação de localização, mas também pode ser utilizado para controlar o acesso a outras informações de contexto fornecidas pela MoCA e por outras arquiteturas, como, por exemplo, o nível de bateria do dispositivo, o endereço IP e a lista de pontos de acesso. Nós concentramos o nosso estudo nas questões de privacidade associadas à informação de localização porque esta informação evidencia as necessidades de controle de privacidade dos usuários. Além disso, localização é um dos aspectos de contexto mais explorado no momento (24) e provavelmente será a forma de computação sensível ao contexto mais comum (25). Outras razões que nos motivaram a considerar a informação de localização como principal estudo de caso para o controle de privacidade são discutidas no Capítulo 2.

Para identificar alguns requisitos de privacidade relevantes para os usuários, realizamos uma pesquisa *preliminar* (discutida na Seção 1.3) com pessoas com diferentes idades e graus de conhecimento tecnológico. Os resultados dessa pesquisa (26, 27), como também as experiências reportadas por outros grupos (7, 8, 28, 29, 30, 10, 31, 11, 12) nos ajudaram a identificar alguns requisitos de privacidade para aplicações sensíveis ao contexto, que, por sua vez, nos auxiliaram no projeto de um serviço de privacidade mais flexível no que diz respeito ao gerenciamento da política de privacidade do usuário. Através do CoPS, os usuários podem compartilhar seus dados de contexto com as pessoas e serviços certos, com a precisão adequada e no momento apropriado.

1.1 Conceitos e discussões sobre privacidade

O conceito de privacidade está ligado intrinsecamente à percepção de cada indivíduo sobre o que representa uma ameaça à sua propriedade pessoal ou integridade física ou moral. Sendo assim, podemos deduzir que a definição de privacidade é algo muito abstrato e subjetivo que toma forma nas mais diversas necessidades particulares de cada indivíduo. Tais necessidades não são homogêneas e podem ser dependentes tanto de aspectos culturais como religião, tradição, costumes, educação ou política, como de questões mais subjetivas ligadas à intimidade do usuário ou ao seu contexto corrente, tais como idade, estado de saúde, função no trabalho, humor, atividade, etc. Em função disso podemos concluir que o controle da privacidade é algo que transcende a nossa capacidade de identificar as reais necessidades de todos os usuários, sendo estes os mais aptos a decidir sobre o que pode ou não ser disponibilizado, pois só eles são capazes de analisar, de acordo com o contexto corrente, o custo *versus* o benefício do compartilhamento da informação.

Dessa forma, podemos ver que privacidade é um conceito abrangente e complexo ligado às reais necessidades circunstanciais de cada indivíduo. Existem diversas outras definições sobre esse tema que atestam essa afirmação, como, por exemplo, a teoria de privacidade de Altman (32, 33) que descreve que o ajuste do controle da privacidade não pode ser estático e nem estritamente baseado em regras. Ele também afirma que a metodologia existente do mundo tecnológico que requer que as pessoas definam parâmetros de configuração e vivam condicionadas a eles, simplesmente não funciona. Já a teoria de privacidade definida por Westin em (34) diz que "indivíduos, grupos e instituições reivindicam a necessidade de poderem determinar quando, como e para que as suas informações são compartilhadas/disponibilizadas para outros usuários".

De acordo com (35, 36), o conceito de privacidade pode ser descrito através de quatro dimensões: social, física, informacional e psicológica. Privacidade social tem uma forte conotação cultural que se refere à capacidade do indivíduo de controlar o acesso às suas informações de acordo com o seu meio. A dimensão física preocupa-se com a amplitude do espaço pessoal e territorial disponibilizado para outras pessoas. Já a dimensão informacional refere-se à capacidade de um indivíduo determinar como, quando e quanto sobre si mesmo pode ser revelado para outra pessoa ou organização. Por fim, a dimensão psicológica compreende o grau em que o indivíduo é capaz de "controlar os aspectos cognitivos e afetivos para formar valores que irão auxiliá-lo a tomar as decisões corretas para determinar com quem e em quais circunstâncias

ele deve compartilhar suas intenções ou revelar informações íntimas" (35).

Diante dessas discussões, surgem algumas questões: Será que as empresas estão respeitando e dando o direito aos usuários de controlarem as dimensões física, informacional? Por outro lado, o quanto os usuários se importam com essas questões de privacidade? Alguns pesquisadores (37, 14) relataram como resultado de suas pesquisas que os usuários entrevistados não se importariam em divulgar a sua localização se eles achassem que os benefícios obtidos superam os riscos envolvidos. No entanto, estes usuários poderiam expressar uma opinião diferente se lhes fossem apresentado um cenário em que eles pudessem ser lesados ou prejudicados em função da divulgação da sua localização, como, por exemplo, a possibilidade de ser roubado ou seqüestrado. Ou seja, as opiniões dos usuários estão intimamente ligadas à visão dos riscos e benefícios percebidos, e, estes, podem mudar de acordo com as circunstâncias.

Já certas empresas não poupam esforços para obter as informações pessoais dos usuários. Elas usam o histórico e perfil de compra, o histórico de uso do cartão de crédito, a freqüência de viagens, etc., para explorar estas informações economicamente. Para elas, as informações dos usuários são como petróleo, elas as "mineram", refinam e depois vendem ou exploram diretamente em seus negócios. Atualmente, esta é uma das atividades mais rentáveis do *Google* para vender anúncios sensíveis ao contexto. Conforme declarado em sua política de privacidade (38), esta empresa afirma que, para fornecer serviços (e.g., anúncios) mais direcionados ao perfil de cada usuário, ela pode combinar e analisar as informações obtidas a partir de suas ferramentas/aplicações. Sendo assim, acreditamos que, para atingir os seus objetivos, esta empresa poderia registrar e fazer o cruzamento de dados sobre tudo que os usuários procuram na Internet, analisar o que e com quem se comunicam via *Gmail* e *GoogleTalk*, analisar as informações privativas do usuário através do *Google Desktop*, estar ciente da agenda e dos relacionamentos (pessoais, de negócios) dos usuários via *Google Calendar*, etc. No entanto, nem sempre estas questões estão evidentes para a maioria dos usuários e, mesmo cientes disto, não sabemos o que eles fazem com essas informações. Será que só as utilizam em benefício próprio ou também as vendem para terceiros? Será que essas informações não poderão ser usadas contra nós em algum momento no futuro (já que elas são armazenadas nos bancos de dados indeterminadamente)? Apesar dos benefícios providos por essas ferramentas, os usuários devem ter o direito de saber a que riscos estão expostos (i.e., transparência da tecnologia), e terem o direito de optar em disponibilizar ou não suas informações diante dos riscos evidenciados.

Apesar dessas questões representarem uma demanda da sociedade, elas ainda não são tratadas apropriadamente, pois não vão ao encontro dos inte-

resses econômicos do mercado. Nós acreditamos que as tecnologias em geral devem considerar, desde a sua fase de projeto, como as questões de privacidade serão tratadas. Ou seja, melhorar a transparência em relação à coleção, uso e divulgação das informações pessoais e fornecer níveis de controle sobre o uso e divulgação da informação. Esta já é uma preocupação no centro de desenvolvimento de *software* de grandes empresas (39) e, talvez, futuramente, possa vir a ser um diferencial determinante na escolha entre uma ou outra ferramenta que ofereça o mesmo serviço.

Vale ressaltar que as questões de privacidade estão estritamente relacionadas às questões de "sociabilidade" dos usuários, uma vez que as tecnologias onde a privacidade se torna uma questão crucial são, tipicamente, tecnologias usadas para socialização ou para interações de outra ordem, onde o componente social é muito importante (por exemplo, no trabalho colaborativo, no comércio eletrônico, etc.). Decorre disto, que determinadas atitudes em relação a privacidade são controladas para fins de "manter as aparências" sociais (40).

1.1.1 Leis de privacidade

As necessidades e preocupações com a privacidade dos dados pessoais dos usuários, por exemplo, em um serviço de *roaming* global para telefones móveis, incentivaram, em alguns países, a criação de uma política legislativa com foco na privacidade pessoal. A *European Union Directive on Data Protection* (41) compreende o conjunto de leis de privacidade mais completo na atualidade. Essa diretiva inclui vários princípios de privacidade da informação que determinam como a privacidade dos dados pessoais deve ser tratada, apesar de que cada país, de maneira geral, pode acrescentar algumas particularidades que aprimorem a proteção da privacidade dos usuários. Os dados pessoais dos usuários nos países sob a *European Union Directive* estão sujeitos aos seguintes princípios de privacidade (35, 42):

- devem ser obtidos de forma correta e dentro das condições impostas pela lei;
- devem ser usados somente para o propósito original especificado;
- devem ser requisitados de forma adequada e relevante ao propósito original, ou seja, a precisão da informação requerida não deve ser mais específica do que o necessário para atender a necessidade do requisitante;
- devem ser mantidos de forma segura;
- devem estar acessíveis ao dono da informação; e
- devem ser destruídos depois que o seu propósito de uso foi alcançado.

As principais legislações propostas ou em vigor, em vários países do mundo, que visam a garantir os direitos de privacidade pessoal de cada indivíduo, são descritas em (43, 44). Em especial no Brasil, algumas legislações propostas ou em atividade que asseguraram o direito de privacidade dos usuários dizem essencialmente o seguinte:

Leis em vigor:

- A lei sobre telecomunicação, homologada em 1997, afirma que tem como parte do seu princípio de funcionamento garantir que usuários de serviços de telecomunicações tenham o direito de ter sua privacidade respeitada quanto ao uso de seus dados pessoais (45);
- Existem algumas leis que não tratam diretamente dos direitos de privacidade e proteção dos dados, mas têm certas implicações relacionadas à garantia de privacidade. Por exemplo, a política nacional brasileira sobre o acesso às informações do governo (46) garante a todas as pessoas o direito de receber informações de interesse pessoal ou geral. Entretanto, o direito é limitado pela privacidade pessoal de cada indivíduo: "a intimidade inviolável, a vida privada, a honra e a imagem das pessoas".

Leis propostas:

- Foi proposto no senado em 1996 um projeto de lei que está parcialmente em conformidade com as normas propostas pela *OECD* (*Organisation for Economic Co-operation and Development*) (47). Esse projeto determina que: "Nenhuma informação ou dado pessoal deve ser disponibilizado, comunicado ou transmitido para propósitos diferentes daqueles que serviram de base para o registro e obtenção dos dados, sem a devida autorização do proprietário, exceto em caso de ordem judicial ou para propósitos de uma investigação criminal. Além disso, é proibido reunir, registrar, arquivar, processar e transmitir dados pessoais de terceiros relativos a: origem étnica, crenças religiosas e políticas, saúde mental e física, vida sexual, registros penal e policial, assuntos familiares, estado civil, etc. Todo cidadão tem o direito de, sem qualquer empecilho, acessar seus dados pessoais armazenados nas bases de dados, alterá-los, ou eliminá-los, e ser informado pelo gerente da base de dados da existência de todo e qualquer dado referente à sua pessoa" (48);
- Em 2000, foi proposta uma lei (49) que afirma que os dados pessoais só podem ser coletados com aviso prévio, sob a permissão expressa do sujeito dono da informação, e usado somente para os propósitos para os quais eles foram coletados;

- Em abril de 2003, a lei de privacidade (50) foi proposta para estabelecer sanções criminais referente à coleta e distribuição não autorizada de informações protegidas.

Apesar da existência dessas leis, as exigências não são devidamente cumpridas porque as leis não evoluem no mesmo ritmo das tecnologias e por causa da complexidade em controlar a difusão e uso das informações privativas dos usuários. Em função disso, nós achamos que, além das leis, faz-se necessário recursos tecnológicos que garantam ao usuário o direito de controlar o acesso às suas informações.

1.2 Ameaças à privacidade

Na computação móvel e sensível à localização, existem vários níveis de ameaças à privacidade da informação de localização do usuário. Essa pode ser comprometida tanto pelos protocolos quanto pelos serviços de contexto e aplicações LBS que inferem e fazem uso da informação de localização, respectivamente. Tais possibilidades tornam-se cada vez mais factíveis dadas as inúmeras ferramentas e agentes existentes que implementam ataques automatizados através da comunicação, observação e inferência de comportamento dos usuários (51).

No nível da comunicação, um agente malicioso poderia explorar vulnerabilidades ou facilidades dos protocolos e aplicações com o propósito de obter e revelar a localização do dispositivo do usuário na rede. Isso pode ser feito de diversas formas, como, por exemplo, explorando o comportamento dos sensores Bats e *Actives Badges* (52) que propagam a sua localização abertamente, ou das interfaces 802.11, que transmitem os seus endereços MAC por meio de *broadcast*. A partir desses identificadores e da identificação lógica do usuário (e.g., e-mail, nome do usuário) que está usando o equipamento é possível inferir a localização aproximada do mesmo.

Em alguns cenários, a identificação dos usuários também pode ser obtida de diversas formas, como, por exemplo, a partir do comportamento ingênuo e vulnerabilidades dos protocolos de rede. Por exemplo, um agente malicioso poderia identificar o nome do usuário proprietário de um laptop Windows através do protocolo de compartilhamento de arquivos *Netbios*. Em um outro cenário, um agente poderia explorar uma vulnerabilidade em telefones com *bluetooth* para obter uma cópia da agenda telefônica e o número do aparelho (53). Além disso, um agente malicioso remoto poderia inferir a localização aproximada (no nível do domínio de rede) de um usuário a partir do IP utilizado pelo seu dispositivo, ou a partir das propriedades de funcionamento de outros proto-

colos de comunicação. Tais riscos tornam-se ainda mais evidentes nos serviços de contexto que inferem a localização dos usuários ou nas aplicações LBS que fazem uso da mesma, pois esses lidam diretamente com a informação de localização e, em princípio, podem divulgá-la ou utilizarem-na de forma maliciosa e indevida.

Como podemos ver, as ameaças à privacidade de localização dos usuários podem estar presentes desde o nível de enlace até o nível de aplicação da pilha de protocolos de rede. Além disso, as tarefas de identificação da localização do usuário podem ser automatizadas e, por conseguinte, podem ser utilizadas para observar e inferir padrões de comportamento dos usuários, o que pode ter conseqüências desastrosas. Por exemplo, pacientes com determinada doença poderiam ser identificados pelo padrão de comparecimento rotineiro a um centro de tratamento.

Neste trabalho, o serviço de privacidade proposto não trata das questões de privacidade relacionadas à vulnerabilidade, fragilidade ou falha de configuração dos protocolos de rede. Ao invés disto, este serviço se limita a ajudar os usuários a controlarem o grau de privacidade desejado no nível da aplicação, ou seja, para determinar como, quando e para quem o serviço de contexto poderá divulgar a sua localização.

1.3 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 usuários de diferentes idades, formação educacional, áreas de trabalho, e familiaridade com tecnologias de comunicação e informação. O estudo foi baseado em um questionário que descrevia em termos não-técnicos, a existência de uma tecnologia hipotética que realizava a coleta, processamento e compartilhamento dos dados de contexto pessoal e computacional dos usuários móveis, e seria utilizada para oferecer novas aplicações e serviços para comunicação e colaboração espontânea entre os usuários. As questões avaliaram os seguintes aspectos de privacidade: o interesse ou o receio em utilizar tal tecnologia; os grupos de pessoas com os quais o usuário compartilharia seus dados de contexto; a demanda por anonimidade; as necessidades de controle de acesso; o uso de opções de notificação e identificação das tentativas de acesso ao contexto/à localização, dentre outros. O questionário foi respondido por aproximadamente 120 pessoas (54).

Os resultados mais relevantes do nosso estudo indicaram os seguintes fatos (com os respectivos percentuais de votos):

- uma atitude cautelosa com relação à aceitação da tecnologia. Por exemplo, 45% selecionariam as opções para desabilitar, seletivamente, o monitoramento de alguns dados (e.g., permitir a coleta do nível de energia da bateria, mas negar a coleta do endereço MAC/IP) e 16% recusariam a tecnologia;
- desejo dos usuários em saber quais informações de contexto foram coletadas;
- considerando que a comunicação e a descoberta mútua são mediadas por uma tecnologia desconhecida, 64% dos usuários utilizariam um apelido/pseudônimo ao invés de sua identidade real;
- 74% dos usuários somente compartilhariam as suas informações de contexto com pessoas que eles conhecem, tais como amigos, colegas, parentes;
- com relação ao controle de acesso, 76% dos usuários afirmaram que, *a priori*, todos os acessos seriam negados, e que eles gostariam de definir explicitamente quais tentativas de acesso seriam permitidas, e 66% gostariam de ser explicitamente consultados para deferir o resultado de uma tentativa de acesso;
- com relação às notificações e à identificação das tentativas de acesso, 57% gostariam de verificar em algum momento (e.g., em um relatório de acesso) quem requisitou o dado, quando e através de qual aplicação, e 29% desejariam ser notificados imediatamente, a cada requisição.

Com base nos resultados desta pesquisa com usuários, e a partir dos resultados reportados em trabalhos relacionados (7, 8, 28, 29, 30, 10, 31), nós 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 podem ser notificados sobre, ou estarem aptos a rastrear, qualquer tentativa de acesso às suas informações de contexto;

Negação Aceitável: além das opções de controle de acesso "Grant" e "Deny", uma terceira opção - "Not Available" - deve ser oferecida. A partir desta opção, os usuários podem negar o acesso sem que os requisitantes tenham conhecimento das suas ações. Este artifício também é conhecido como *plausible deniability* (7, 9);

Controle de Precisão: os usuários podem 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 (ou a todas) informação de contexto;

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

Simplicidade: os usuários não devem ser sobrecarregados com a configuração das suas preferências de privacidade;

Eficiência: o tratamento das questões de privacidade não deve causar um atraso significativo na comunicação ou uma carga de processamento excessiva para os serviços de provisão de contexto.

1.4 Requisitos gerais

Diferentemente do controle de acesso convencional implementado em um *firewall*, um serviço de privacidade não deve somente determinar o que é ou não é permitido. Esse serviço deve auxiliar o usuário a manter a sua privacidade o mais próxima do desejado, sem impedi-lo de desfrutar de novas experiências, como, por exemplo, iniciar uma colaboração com um desconhecido "de boa fé" que deseja obter a sua localização, e sem dificultar o uso dos serviços e aplicações existentes, quando o custo do risco de exposição é baixo se comparado ao benefício do serviço utilizado. Nesse cenário, somente o usuário pode determinar previamente ou dinamicamente o que melhor lhe convém. Com base nisto e nos resultados da pesquisa preliminar descrita na Seção 1.3, projetamos o CoPS para auxiliar 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.

A grande maioria dos usuários utiliza uma aplicação para um determinado fim, geralmente não se preocupando diretamente com as questões de segurança e privacidade, apesar de estas serem desejáveis. Na verdade, os usuários, tacitamente, têm certas expectativas com relação à manutenção da sua segurança e privacidade e esperam que essas funcionalidades estejam sendo fornecidas pelo sistema. Por exemplo, o usuário usa um cliente de e-mail com o objetivo de ler e enviar mensagens, no entanto, implicitamente, ele deseja

que os mecanismos de segurança adequados, como criptografia, sejam aplicados para garantir a confidencialidade da sua informação. O ideal seria se essa funcionalidade fosse ativada dinamicamente sem que o usuário tivesse que configurá-la explicitamente, não exigindo que ele conheça recursos de criptografia para enviar uma mensagem de forma segura. Com esse propósito, o CoPS deve auxiliar o usuário a definir e manter a sua privacidade através de uma série de recursos, como, por exemplo: hierarquia de regras de privacidade, a partir da qual poderia ser configurado um conjunto de regras modelo que atenda à necessidade de privacidade da maioria dos usuários, sendo essas, automaticamente associadas a cada novo usuário do sistema. Além disso, o CoPS deve oferecer recursos para notificação de acesso à informação, *logging*, relatórios de acesso a um dado tipo de contexto (e.g., localização), consultas ao usuário para determinar se a tentativa de acesso deve ser negada ou permitida, dentre outros, para que o usuário possa, na medida do possível, definir e refinar a sua política de privacidade gradativamente.

Conforme evidenciado na pesquisa preliminar com usuários, a usabilidade do serviço de privacidade está intimamente ligada à facilidade de configuração, bem como do refinamento da política de privacidade. O serviço e a interface de definição da política de privacidade devem facilitar ao máximo a definição da política do usuário. Dessa forma, o usuário pode especializar a sua política de privacidade à medida que ele vai ganhando experiência no controle e uso de uma aplicação sensível à privacidade.

Vale ressaltar que, conforme discutido em (43, 30), não existe uma solução única e completa que assegure a privacidade dos usuários. Para alcançarmos o nível de privacidade o mais próximo do desejado, nós devemos levar em conta a combinação de diversos meios, tais como legislações com punições bem definidas para as possíveis infrações, normas sociais, normas corporativas, tecnologias 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. O que estamos propondo nesse trabalho é mais um recurso tecnológico, através de um serviço de privacidade, que auxilie os desenvolvedores a incorporar nas aplicações sensíveis ao contexto mecanismos que permitam aos usuários controlarem como, para quem, e com que granularidade as suas informações de localização devem ser divulgadas.

1.5 Objetivos da tese

De uma forma geral, esta tese trata de dois desafios principais relacionados ao desenvolvimento e uso de aplicações sensíveis ao contexto: a comple-

xidade em desenvolver os serviços de provisão de contexto e a necessidade de controlar o grau de privacidade da informação de contexto (e.g., localização) do usuário. Com o intuito de tratar dessas questões, nós estruturamos a nossa pesquisa em duas partes.

Na primeira parte, propomos uma arquitetura cujo objetivo é auxiliar o desenvolvimento de aplicações sensíveis ao contexto. Esta infra-estrutura de *software* também serviu de base para o desenvolvimento da segunda parte da nossa pesquisa: o estudo de privacidade em aplicações LBS.

Na segunda parte, focamos a nossa pesquisa no objetivo principal desta tese, que é discutir e tratar as questões de privacidade nos serviços e aplicações sensíveis ao contexto, em especial, nas aplicações LBS. Há muitos trabalhos teóricos sobre o projeto de serviços de privacidade para aplicações baseadas em localização, mas poucos descrevem ferramentas práticas para auxiliar os desenvolvedores de tais serviços nessa tarefa. Em função disto, nesta tese, propomos um modelo conceitual e um conjunto de requisitos que visam a auxiliar o projeto de um serviço de privacidade a ser utilizado por aplicações sensíveis ao contexto. Como estudo de caso, pretendemos oferecer um serviço de privacidade que implemente o referido modelo e os requisitos de privacidade propostos. A principal questão que delineou a nossa pesquisa sobre privacidade 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?

1.6 Metodologia

Para realizar esta pesquisa, seguimos uma metodologia que envolveu as seguintes atividades:

- Primeiro, trabalhamos ativamente na definição e no projeto de uma arquitetura de provisão de contexto - chamada MoCA. Esta serviu de base para o desenvolvimento de aplicações sensíveis ao contexto que nos possibilitaram trabalhar nas questões de privacidade relacionadas ao uso de tais aplicações;
- Em seguida, realizamos uma pesquisa preliminar com usuários para identificar requisitos importantes para o projeto de um serviço de privacidade para aplicações sensíveis ao contexto, com enfoque para aplicações baseadas em localização;
- Depois fizemos uma pesquisa sistemática de outros trabalhos que discutem questões gerais de privacidade envolvidas no projeto e uso de tecnologias mediadas pelo usuário;

- Com base na pesquisa preliminar e no estudo de trabalhos relacionados, definimos um modelo conceitual e um conjunto de requisitos que podem ser utilizados para o projeto de um serviço de privacidade;
- Seguindo as diretrizes do modelo e dos requisitos definidos, implementamos um serviço de privacidade - o CoPS;
- Depois, definimos uma metodologia de avaliação qualitativa da usabilidade de algumas funcionalidades do CoPS;
- Posteriormente, avaliamos algumas funcionalidades do CoPS através de um estudo com usuários usando duas técnicas comuns em IHC: entrevistas abertas e experimentos do tipo "Mágico de Oz" (55, 56);
- Finalmente, integramos o CoPS à arquitetura MoCA.

1.7 Resumo das contribuições da tese

A seguir, apresentamos de forma objetiva e concreta as principais contribuições desta tese. No entanto, na Seção 7.1 fazemos uma discussão mais detalhada destas contribuições. Essas podem ser descritas como segue.

- Projeto de uma arquitetura de provisão de contexto - MoCA - e a implementação de alguns serviços que constituem o núcleo desta arquitetura;
- Definição de um modelo conceitual e de um conjunto de requisitos para auxiliar o projeto de um serviço de privacidade;
- Estudo e pesquisa com usuários sobre questões de privacidade relacionadas ao uso de aplicações sensíveis ao contexto, em especial, àquelas baseadas em localização;
- Discussão de algumas questões fundamentais sobre o benefício e o risco de invasão de privacidade decorrente do uso de tecnologias sensíveis ao contexto e, principalmente, como elas podem ou devem tratar estas questões;
- Projeto e implementação de um serviço de privacidade, o CoPS.

1.8 Organização da tese

Esta tese está organizada da seguinte forma. O Capítulo 2 faz uma discussão geral sobre sistemas sensíveis ao contexto e à localização, e apresenta uma visão geral da arquitetura MoCA e de seus serviços de provisão contexto computacional (CIS) e de localização (LIS). O Capítulo 3 descreve o modelo conceitual que especifica os papéis e o padrão de interação entre as entidades de um serviço de privacidade e discute alguns requisitos que tratam dos principais desafios relacionados à configuração e à manutenção da política de privacidade do usuário. Em seguida, o Capítulo 4 apresenta a arquitetura e implementação do serviço de privacidade de contexto CoPS (**C**ontext **P**rivacy **S**ervice) que se adequa ao modelo e implementa os requisitos de privacidade propostos no Capítulo 3. No Capítulo 5, são discutidos a metodologia e os resultados da avaliação qualitativa e de desempenho do CoPS. O Capítulo 6 descreve uma comparação com os principais trabalhos relacionados na área e, o Capítulo 7, apresenta as considerações finais da tese, salientando as contribuições do trabalho e as pesquisas futuras.