6
Trabalhos correlatos

A pesquisa sobre serviços de provisão de contexto e gerenciamento de privacidade das informações do usuário tem sido o foco de estudo de muitos grupos de trabalho. A seguir, apresentamos uma discussão comparando as principais diferenças entre as abordagens adotadas neste trabalho e as adotadas por outros grupos de pesquisa. Como a pesquisa sobre privacidade é bem abrangente, existem inúmeros outros trabalhos que tratam das questões de privacidade relacionadas ao anonimato (103, 19), confidencialidade dos dados (através de mecanismos de criptografia) (104), controle de acesso (105), serviço e arquitetura de privacidade para a Web (106), dentre outros. Entretanto, neste capítulo, nós nos preocupamos em fazer uma comparação sistemática 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.

Vale ressaltar que o estudo das abordagens e princípios de projeto de outros serviços de provisão de contexto, discutidos nesta seção, nos inspirou no desenvolvimento dos serviços da MoCA e nos permitiu identificar novos requisitos para o projeto do serviço de privacidade.

6.1
Serviços de provisão de contexto

A tese de doutorado publicada por Hong em (30) é um dos principais trabalhos relacionados a nossa pesquisa. De uma forma mais geral, esse trabalho foi estruturado em três etapas principais para tratar das questões relacionadas ao desenvolvimento de aplicações sensíveis ao contexto e à privacidade, são elas: 1) pesquisa e análise das principais necessidades de privacidade do usuário e do desenvolvedor de aplicações sensíveis ao contexto. Nessa pesquisa foram analisados dados de uma grande variedade de fontes, tais como entrevistas, relatos sobre o uso de aplicações, formulários eletrônicos, dentre outros. 2) estudo dos principais desafios relacionados ao projeto de interfaces gráficas para aplicações ubíquas sensíveis à privacidade (107) e 3) projeto e implementação de uma arquitetura (9), chamada ContextFabric (*Confab*),

que auxilia o desenvolvimento de aplicações móveis sensíveis ao contexto de localização e a privacidade. Essa arquitetura provê um framework para coleta, armazenamento, processamento e apresentação da informação de contexto. Todas essas operações são implementadas localmente no dispositivo do usuário. Na *Confab* todas as informações são armazenadas em espaços de tupla, que por sua vez, têm o seu acesso controlado através de operadores *in* e *out*. Esses operadores possuem métodos que determinam como, por quem, quando e quais dados podem ser lidos do ou armazenados no espaço de tupla.

Ao contrário dos serviços de provisão de contexto da MoCA (Monitor e CIS), a Confab implementa a coleta e processamento da informação dentro da mesma arquitetura de software, tornando muito complexo a incorporação e utilização de novas fontes de contexto (por exemplo, novos tipos de sensores). Conseqüentemente, isso limita o uso da arquitetura ao gerenciamento de variáveis de contexto bem específicas. Em sua versão inicial, a Confab só coleta e gerencia informações de localização.

Harry Chen propõe em sua tese de doutorado (93, 108) uma arquitetura chamada "*Context Broker Architecture* (*CoBrA*)" formada por *brokers* responsáveis por manter e compartilhar parte do espaço de contexto monitorado (por exemplo, contexto das salas de aula, auditório, corredor, elevador, etc). Os principais componentes dessa arquitetura são: *CoBrA Ontology (COBRA-ONTO)* responsável por definir uma representação de contexto que usa a *Web Language Ontology - OWL* para definir ontologias que facilitam o compartilhamento das informações de contexto; *Context Reasoning Engine (CoRE)* responsável pela lógica de inferência usada para integrar os dados de contexto obtidos a partir de diferentes fontes. Além disso, o componente *CoRE* detecta e resolve algumas inconsistências na informação de contexto inferida, por exemplo, filtrando as variáveis de contexto com valor fora de um intervalo válido. Por último, o *Module for Privacy Protection (MoPP)* implementa uma linguagem (*policy language*) para os usuários definirem as regras de controle de privacidade e, além disso, oferece uma máquina de inferência que, a partir de tais regras, determina quais informações do usuário podem ser compartilhadas.

Diferentemente da abordagem adotada pelo nosso trabalho, as arquiteturas CoBrA e Confab tratam a provisão de contexto e as questões de privacidade como uma solução integrada. Considerando que a maioria dos sistemas tratam segurança e privacidade como aspectos secundários e opcionais, o desenvolvedor de uma aplicação usando essas abordagens não poderia usar, se necessário, somente a solução de provisão de contexto ou gerenciamento de privacidade como serviços independentes.

Além disso, ao contrário dessas arquiteturas, o CIS oferece uma comu-

nicação baseada em eventos que permite às aplicações serem notificadas das mudanças de estado dos dispositivos móveis e da rede sem fio. Através do serviço de eventos, as aplicações podem fazer consultas mais flexíveis através de expressões lógicas que combinam diferentes variáveis de contexto. No entanto, ressaltamos que a arquitetura CoBrA oferece uma representação da informação de contexto baseada em ontologias, mais flexível e que, além de outros benefícios, permite a integração e fusão de informações de contexto provenientes de diferentes fontes. Como trabalho futuro, pretendemos integrar ao CIS o modelo de representação de contexto proposto em (109) para usufruir de tais benefícios.

Existem inúmeros outros serviços e arquiteturas que auxiliam o desenvolvimento de aplicações sensíveis ao contexto. Por exemplo, Context Toolkit (110), PARCTab System (111), Guide System (112), Cyberguide (113), dentre outros. Naturalmente, cada arquitetura tem uma aplicabilidade específica que atende às necessidades de uma determinada categoria de aplicações. No entanto, diferentemente das arquiteturas mencionadas, pretendemos disponibilizar serviços de provisão de contexto que, além das funcionalidades de coleta e processamento de contexto, oferecem recursos para o controle de privacidade das informações de contexto gerenciadas.

6.2 Serviços de privacidade

Existem vários trabalhos que fazem uma discussão prescritiva e analítica sobre requisitos, dificuldades e desafios dos sistemas sensíveis a privacidade. O trabalho discutido em (13) argumenta que privacidade não é simplesmente um problema de controle de acesso, mas é um processo contínuo das negociações das fronteiras da revelação, identidade e tempo. Esse artigo discute de forma sistemática algumas questões que nos ajudaram a compreender melhor o relacionamento entre privacidade e tecnologia da informação. Harper em (7) apresenta um estudo sobre as atitudes das comunidades diante da introdução da tecnologia no seu meio. Rejeição ou adoção de uma tecnologia podem resultar de posturas, a priori, ideológicas, que não estão relacionadas com os objetivos da tecnologia. Isso nos leva a acreditar que propostas genéricas de serviços de privacidade tendem a ser mal sucedidas diante da impossibilidade de se adequar as reações das diversas comunidades em relação a intrusivisidade das tecnologias. A pesquisa publicada em (14) discute o quanto serviços baseado em localização podem ser considerados intrusivos à privacidade dos usuários e discute se serviços de localização centralizados trazem mais ou menos riscos de privacidade do que serviços de posicionamento implementados

pelo próprio dispositivo. Dentre as suas conclusões, esse artigo argumenta que a ênfase de desenvolvimento deve ser dada a serviços de posicionamento implementados pelo próprio dispositivo, semelhante ao que é feito no projeto *Place LAB* (69). No entanto, serviços de rastreamento do usuário implementados por outrem podem ser bem sucedidos (i.e., aceitos/usados) se os usuários têm uma simples opção de desligar/desativar o rastreamento.

Em uma outra pesquisa, Patil & Lai em (10) discutem o quanto controle de privacidade entre pessoas que se conhecem pessoalmente afeta suas atitudes no sentido de tornarem-se mais cautelosas e conservadoras. Nessa pesquisa, os autores perceberam que os usuários entrevistados definiram o mesmo nível de visibilidade da informação de localização para os seus colegas de trabalho, no horário de trabalho, e para os seus familiares. Entretanto, o mesmo não acontece após o expediente de trabalho. Isso nos leva a crer que a identidade dos usuários e as circunstâncias em que a interação acontece determinam as atitudes das pessoas com relação à divulgação da sua localização. Essas e outras discussões serviram de base para fundamentar e justificar as decisões de projeto relacionadas ao modelo conceitual e aos requisitos de privacidade implementados no CoPS.

Além desses, analisamos também o trabalho de vários outros grupos de pesquisa que propuseram arquiteturas e serviços que tratam de questões de privacidade de localização. O grupo de trabalho IETF (*Internet Engineering Task Force*) Geopriv (114) identificou a necessidade de processar e transferir a informação de localização entre serviços e aplicações baseadas em localização, assegurando ao mesmo tempo, a privacidade dos indivíduos envolvidos. O Geopriv propõe que seja criado um objeto de localização que encapsula a informação de localização do usuário e os requisitos de privacidade associados a esta informação. Tais requisitos são encriptados e assinados digitalmente para garantir a confidencialidade da política de privacidade, e requer uma infra-estrutura de chaves pública para gerenciar a comunicação segura. Alguns dos requisitos de privacidade definidos pelo CoPS se assemelham aos definidos pelo IETF Geopriv, por exemplo, a divulgação da localização em diferentes granularidades e sob determinadas restrições temporal. No entanto, em função da abrangência da sua proposta e da complexidade de lidar com questões de privacidade de uma forma genérica, o Geopriv omite várias questões ligadas ao gerenciamento e manutenção da privacidade dos usuários.

Como descrito anteriormente, a Context Fabric (Confab) (30) é uma arquitetura para provisão de informação de localização que trata também do controle de privacidade. O projeto da arquitetura da Confab apresenta uma série de requisitos de privacidade que oferecem certa flexibilidade no uso de

uma aplicação sensível a privacidade, tais como o modo invisível, o controle de acesso interativo, a notificação de acesso. Um dos princípios de projeto do sistema é que a própria aplicação ofereça em sua interface mecanismos de controle de privacidade, a partir dos quais o usuário possa configurar a sua política de privacidade interativamente. Alguns de seus requisitos de projeto (e.g., modo invisível, notificação de acesso) foram adotados em 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, grupos hierárquicos, relatórios de acesso, *templates* de regras, perfis de privacidade, dentre outros.

Ao contrário da Confab, o CoPS oferece uma hierarquia de política de privacidade a partir da qual a organização pode definir, de forma opcional, a política que determinados usuários devem ser submetidos, e a política padrão que todo novo usuário pode aderir para garantir o mínimo de privacidade no uso de uma aplicação LBS. Além disso, a Confab não implementa um algoritmo de especificidade que permite ao usuário configurar um controle de acesso de granularidade fina para processar as requisições de diferentes usuários ou grupos de requisitantes. Em função disso, na Confab o usuário não tem a flexibilidade de configurar em cada regra o tipo de notificação a ser recebida, restrição de granularidade da informação a ser divulgada para um grupo de requisitantes específico, dentre outros. Sendo assim, apesar do propósito de alguns mecanismos de controle de privacidade do CoPS e Confab ser o mesmo, no CoPS, o usuário tem uma maior flexibilidade para decidir como e quando ele deseja usufruir de uma dada funcionalidade oferecida. Por exemplo, o usuário pode configurar em sua política que deseja ser notificado sempre que seu chefe tentar acessar a sua localização, mas não gostaria de receber notificações das tentativas de acesso de um colega de trabalho.

A Confab segue uma abordagem distribuída em uma rede *ad hoc*, na qual a informação de localização é inferida, armazenada e gerenciada no dispositivo do usuário final. Essa abordagem oferece ao usuário um maior controle sobre a informação, pois permite que ele tenha ciência de que, ninguém mais, além dele, detém às suas informações, ao contrário da abordagem centralizada na qual os dados são processados em um servidor da rede. No entanto, deve-se analisar as conseqüências dessa decisão de projeto. Nós acreditamos que, pelo menos com a tecnologia corrente, existem algumas desvantagens da abordagem descentralizada que podem comprometer a aplicabilidade do

sistema. Por exemplo, essa abordagem exige dos dispositivos clientes uma maior capacidade de processamento e armazenamento, um maior consumo de bateria, e a capacidade de descoberta e autenticação mútua junto aos demais nós da rede, etc. Entretanto, o autor não descreve como a arquitetura do sistema trata tais questões. Outro princípio de projeto da Confab que difere do CoPS diz respeito à definição da política de privacidade. Na Confab, a aplicação deve oferecer em sua interface opções de configuração que permitam ao usuário definir a sua política de privacidade. Essa imposição pode dificultar o projeto e desenvolvimento de novas aplicações, pois todas elas teriam que incorporar tais características de controle de privacidade. Diferentemente dessa abordagem, o CoPS permite o uso de uma interface específica para a configuração e gerenciamento da política de privacidade, sendo que esta pode ser usada pelo usuário independentemente do dispositivo ou aplicação utilizada.

Em uma outra vertente, o sistema de controle de privacidade *pawS* (*Privacy Awareness System*) proposto por *Langheinrich* em (94) provê algumas ferramentas que auxiliam o usuário a manter a sua privacidade pessoal e a garantir que os demais usuários respeitem-na. Esse sistema baseia-se mais em normas legais, sociais e no respeito mútuo do que propriamente no controle tecnológico mais rigoroso para gerenciar a privacidade dos usuários. No *pawS*, quando um usuário entra em um ambiente no qual existem serviços coletando dados de contexto (e.g. uma câmera de segurança), esses anunciam as suas políticas de privacidade através de uma mensagem de controle, chamada *privacy beacon*. Em seguida, o proxy de privacidade do usuário verifica se essas políticas, descritas no formato P3P (*Platform for Privacy Preferences*) (115), estão de acordo com as preferências de privacidade do usuário. Se elas estiverem em conformidade, os usuários podem usufruir dos benefícios providos pelos serviços disponíveis. Caso contrário, o sistema notifica o usuário sobre o conflito para que ele decida se vai ou não utilizar os serviços em questão.

No entanto, esse sistema não define mecanismos práticos para auxiliar os usuários a gerenciarem a sua política de privacidade. Além disso, ele não oferece meios que auxiliem os usuários a refinarem a sua política gradativamente, e a identificarem e bloquearem o acesso de possíveis infratores. O pawS considera que a política de privacidade dos usuários será respeitada em função das imposições das leis e da sociedade. Apesar de acreditarmos que as soluções legais e sociais são essenciais para o controle da privacidade, nós também acreditamos que os usuários devem ter acesso a soluções tecnológicas que lhes ofereçam mecanismos mais efetivos (i.e., práticos) para o controle da privacidade, permitindo-lhes tratar as exceções e/ou os casos mais específicos que requerem um controle mais rigoroso.

Ao contrário do CoPS, as arquiteturas CoBrA (93, 108) e pawS usam a informação de localização do usuário para avaliar as requisições de acesso ao contexto, permitindo assim a definição de controle de acesso dependente da localização. Na arquitetura CoBrA, o componente MoPP usa a localização do usuário e a sua proximidade física com relação a outros serviços (e.g., câmera de vídeo) para determinar quais restrições de acesso devem ser impostas sobre o compartilhamento de cada tipo específico de informação de contexto. De forma semelhante, a arquitetura *pawS* usa proxies de privacidade que consideram a proximidade do usuário a outros serviços para determinar quais regras de controle de acesso da política de privacidade devem ser aplicadas. 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.

Apesar de ser interessante por permitir um controle de privacidade dependente da localização, nós não incorporamos essa característica no CoPS, pois isso o deixaria dependente do serviço de contexto para avaliar uma requisição, afetando drasticamente a sua escalabilidade e confiabilidade. Se o CoPS implementasse essa funcionalidade, ele teria que consultar o provedor de contexto para obter a localização do subject/requester para, então, determinar o conjunto de regras candidatas a serem usadas para avaliar as requisições recebidas. Comparado a essas arquiteturas (CoBrA & pawS) no que diz respeito ao controle de privacidade, o CoPS oferece ao usuário um conjunto de mecanismos de controle de privacidade mais significativo que auxilia a definição e manutenção da política de privacidade do usuário e da organização.

Em (18) é proposto um *framework* de componentes para controle de privacidade que, como estudo de caso, foi integrado ao serviço de localização *LocServ (Location Service)* para permitir que os usuários divulguem as suas localizações de acordo com as suas políticas de privacidade. Através dos componentes *Validators*, o *LocServ* avalia se a localização de um dado usuário requisitada por um terceiro (i.e., um outro usuário ou uma organização) pode ser divulgada ou não. As políticas de privacidade dos usuários são representadas em um formato estendido do padrão P3P (115), que por sua vez, são encapsuladas pelos *Validators*. O sistema presume que uma organização confiável definirá um conjunto de *Validators* na tentativa de não sobrecarregar o usuário com a tarefa de configuração da política de privacidade. Para as situações atípicas em que a política padrão implementada pelos *Validators* não é apropriada, os usuários podem criar novos *Validators* através de ferramentas, consideradas pelos autores, "simples" e "intuitivas". No entanto, eles não demonstraram nenhum estudo sobre o uso dessas ferramentas que comprova a sua simplicidade na definição de novos *Validators*.

O CoPS apresenta algumas semelhanças aos princípios de projeto do referido *framework* de privacidade. Por exemplo, ambos baseiam-se em uma abordagem centralizada, restringem o acesso em função do tempo, utilizam grupos, *templates* de regras e implementam funções para um controle de acesso interativo. 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 de todas as exceções é uma abordagem simplista tendo em vista a complexidade e a quantidade de desafios relacionados a tal problema. Para tratar dos casos de exceção para acomodar as diferentes demandas por privacidade por parte dos usuários, foram propostos no CoPS outros mecanismos de controle de privacidade que auxiliam a definição e manutenção da política de privacidade tais como políticas de acesso, políticas de privacidade hierárquicas, notificações, dentre outros. Além do mais, não é descrito no artigo sobre o *framework* como a avaliação das regras é implementada e como são tratadas as regras conflitantes selecionadas para avaliar uma requisição. No CoPS, projetamos um algoritmo de especificidade que oferece ao usuário uma flexibilidade para especificar diferentes formas de controle de acesso a sua informação de localização/contexto sem que este precise se preocupar em configurar o que deve ser feito quando duas ou mais regras forem selecionadas para avaliar uma requisição.

Os trabalhos (116, 104) focam essencialmente na implementação do controle de acesso baseado em regras previamente configuradas pelo usuário. Por exemplo, Urs Hengartner em (104, 23) propõe um mecanismo de controle de acesso baseado em certificados SPKI/SDSI (117), que determina como as informações de localização dos usuários serão compartilhadas. O controle de acesso proposto por Hengartner oferece algumas propriedades que tornam o sistema mais flexível e facilitam o compartilhamento da informação de localização. Dentre os pontos de flexibilidade destacam-se: o controle da granularidade da informação revelada, o intervalo de tempo em que uma dada requisição é atendida e a avaliação da requisição em função da localização do requisitante. No entanto, o sistema proposto exige que o usuário configure de antemão toda a sua política de privacidade e não provê mecanismos para o usuário monitorar e refinar as suas preferências de privacidade. Em (116) Wagealla propõe um modelo baseado em confiança para controle de privacidade em sistemas sensíveis ao contexto. Entretanto, esse sistema requer que o usuário defina, a priori, o nível mínimo de confiança (de um requisitante) necessário para acessar uma dada variável de contexto. Como discutido no

Capítulo 3, tal imposição torna a configuração e manutenção da política de privacidade muito complexa e quase impossível de ser usada na prática.

6.2.1 Suporte a anonimidade

Existem várias propostas de trabalho que implementam abordagens diferentes para oferecer anonimidade aos usuários de aplicações LBS. A anonimidade pode ser utilizada para proteger a identidade de um usuário ou o acesso às informações que podem revelar a identidade real de um usuário (e.g., o endereço IP da máquina de um usuário pode revelar a sua localização, e a partir da localização e outras informações de perfis pode ser possível inferir a sua identidade). Gruteser e Grunwald em (19) propõem uma arquitetura de *middleware* e um algoritmo adaptativo (*cloaking*) para ajustar o controle da precisão espacial e temporal da localização para satisfazer as restrições de anonimidade. Na arquitetura do sistema, o usuário divulga a sua localização através de um proxy confiável. Este é responsável pelos ajustes de precisão da localização divulgada para os serviços com base na densidade de usuários em uma dada região. Para o controle de acesso à localização, o proxy implementa um serviço de *k-anonymity*, cuja finalidade é ocultar a precisão da localização de um usuário retornando uma área na qual ele está localizado e contém k-1 outros usuários. Uma outra abordagem para implementar *k-anonymity* proposta em (20) utiliza um conceito de "servidores cooperativos mistos" para evitar que a identidade do usuário seja revelada a partir da correlação do seu comportamento e do conhecimento prévio do ambiente no qual ele está inserido. A localização do usuário é encriptada e encapsulada dentro de outros dados a medida em que ela é roteada pelos servidores da rede. Essa abordagem dificulta o rastreamento dos dados, isto é, ela dificulta identificar quem os enviou, para onde estão sendo encaminhados e quando foram enviados. Por outro lado, ela introduz uma latência de rede muito grande, prejudicando assim, a qualidade da comunicação entre as entidades/usuários envolvidos.

Outras propostas discutidas em (21, 103), descrevem soluções para oferecer diferentes níveis de anonimidade na divulgação da localização do usuário. No entanto, o CoPS não provê suporte a esses mecanismos de privacidade da identidade e localização do usuário, pois esses não fizeram parte do escopo do trabalho corrente. Em algumas circunstâncias, podemos presumir que a anonimidade não é desejável, seja porque o usuário já conhece as identidades dos demais usuários com os quais pretende interagir (e.g., membros da família, colegas de trabalho, etc), ou porque o usuário não quer se esconder atrás de um pseudônimo/apelido digital que o impede de desfrutar da autoridade ou

benefícios que podem ser obtidos a partir da sua identidade real.

6.3 Discussões

Como foi mostrado, existem muitas infra-estruturas que apresentam abordagens e princípios de projeto bem diferentes para auxiliar o usuário a gerenciar a sua privacidade. Algumas dessas (18, 30) são integradas/acopladas diretamente ao serviço de contexto, o que dificulta a reutilização da proposta de gerenciamento de privacidade ou, até mesmo, não oferece a flexibilidade de tornar o controle de privacidade opcional para o desenvolvedor ou usuário do serviço de provisão de contexto. Por essas razões, projetamos o CoPS como um serviço à parte que permite o desenvolvedor decidir como e quando o serviço proposto pode ser utilizado. Além disso, outras arquiteturas apresentam uma abordagem de controle de privacidade de mais alto nível, ora confiando na *expertise* do usuário para gerenciar a sua política de privacidade (116, 23, 93), ora confiando nas normas legais e sociais para prover o nível de privacidade desejado pelos usuários (94). Apesar de também considerarmos a importância das leis e da *expertise* do usuário para gerenciar sua política, propomos através do CoPS, uma solução tecnológica complementar, que oferece mecanismos de controle de privacidade mais efetivos, do que os propostos nesses trabalhos, que permitem os usuários terem a flexibilidade de definirem as suas políticas gradativamente, no decorrer do uso de uma aplicação LBS. No próximo capítulo, apresentamos as considerações finais, as contribuições e as pesquisas futuras deste trabalho.