LOCATION AWARE Applications

SAMPLE CHAPTER

Richard Ferraro
Murat Aktihanoglu

MANNING

Location Aware Applications

Richard Ferraro
Murat Aktihanoglu

Chapter 10

brief contents

10 The privacy debate

This chapter covers

- Explaining what privacy really means
- Exploring the two sides of the privacy debate
- Understanding who manages privacy within location-aware applications
- Considering the impact of privacy legislation

We started part 3, the final part of the book, by discussing in chapter 9 the different ways in which we can monetize location -aware applications and ser vices. Where these services are directed at the general public, extra care is required because of the ongoing debate over privacy of location data.

If you were to survey an expert panel of mobile and web professionals about what they thought was the number-one hurdle to a wider and faster spread of LBS, we'd bet a large sum of money that their answer would be "privacy concerns."

More and more, the terms *privacy* and *location* are menti oned together (try Googling for the two terms together, and you'll get over 1,980,000,000 entries), and the driver behind this is that people value their locational privacy above all

other types of privacy (religious privacy, cultural privacy, behavioral privacy, and so on).

Because of this, any LBS developer or entrepreneur worth their salt needs to pay special attention to their customers' attitudes to privacy:

- What is the general public afraid of?
- How can you allay their fears?
- Is there a price on privacy?

As well as answering these questions, LBS pioneers need to understand that there's still a degree of irrational fear of privacy being invaded by new-fangled technologies. This makes it essential to educate the general public (and your customers) about this topic by properly informing them of their rights and how their privacy will be respected.

But you can do this only if you have a good grasp of what we mean by *privacy*, especially when it comes to location, and this chapter sets out to give you the essential information to safely navigate the choppy waters of the privacy debate. This means that if you're a developer building consumer-targeted applications, you'll be able to, at the very least, comply with privacy legislation and avoid nasty fines. By tailoring your service to allay privacy fears, you may also carve out a stronger position within the consumer market.

10.1 What do we mean by privacy?

That privacy has acted as a brake on the early adoption of LBS is perhaps the only aspect of the privacy debate that's beyond question. This has been fueled by popular imagery of big brother–like spying on private individuals and, in a sense, by a growing voyeuristic instinct in the population at large (witness the success of reality TV shows like *Big Brother*, *Temptation Island*, and others).

But what do we mean by privacy, and why are so many people worried about losing it?

10.1.1 Defining privacy

Privacy is the ability one has to control personal information about oneself.[1] An infringement of privacy can be seen as a reduction in a person's freedom to control his or her personal information. Privacy can be also seen as "the right to be left alone" or the condition in which people have limited access to personal affairs and information of others.[2]

Concerns about privacy relate to the confidentiality of accumulated individual data and the potential risks that individuals experience over the possible breach of confidentiality. In extreme circumstances, improper handling of location information can place individuals in danger or seriously jeopardize their social life or finances.

---

[1] W. A. Parent, "Privacy, Morality, and the Law," in *Philosophy and Public Affairs* vol. 12, no. 4 (1983):269–88.

[2] Philip Brey, editorial introduction, "Surveillance and Privacy," in *Ethics and Information Technology* 7, no. 4: 183–84.

The fact that privacy is a very wide concept has prompted some observers to narrow the exact meaning of privacy for digital services that use location. The term *locational privacy* (also known as *location privacy*) was coined in 2009 to describe

> *The ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use.*[3]

By managing locational privacy, you can protect private individuals from malicious interrogation of location databases to answer the following sorts of questions:

- Did you go to an antiwar rally on Tuesday?
- Did you walk into an abortion clinic?
- Did you see an AIDS counselor?
- Have you been checking into a motel at lunchtime?
- Were you the person who anonymously tipped off safety regulators about the rusty machines?
- Which church do you attend? Which mosque? Which gay bars?
- Who is your ex-girlfriend going to dinner with?[4]

Several studies have conceptualized privacy concerns in more detail: The Concern for Information Privacy (CFIP) instrument was developed by Smith et al.,[5] which identified four dimensions of information privacy concerns:

1. *Collection* reflected the concern that extensive amounts of personally identifiable data are being collected and stored in databases.
2. *Unauthorized secondary use* reflected the concern that information is collected from individuals for one purpose but is used for other secondary purposes without consent.
3. *Errors* reflected the concern that protections against deliberate and accidental errors in personal data are inadequate.
4. *Improper access* reflected the concern that data about individuals is readily available to people not properly authorized to view or work with that data.

These four key privacy concerns are illustrated in figure 10.1.

It's essential that developers and providers of LBS take into account these four dimensions when rolling out LBSs in order to prevent potential privacy breaches.

Now that you understand what we mean by the term *privacy* and the generalized concerns it may provoke, we can look into the different sides of the privacy debate and some more specific concerns that have arisen.

---

[3] Andrew J. Blumberg and Peter Eckersley, "On Locational Privacy, and How to Avoid Losing It Forever," August 2009, available at http://www.eff.org/wp/locational-privacy.

[4] Ibid.

[5] H. J. Smith, J. S. Milberg, and J. S. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly*, vol. 20, no. 2 (1996): 167–96.

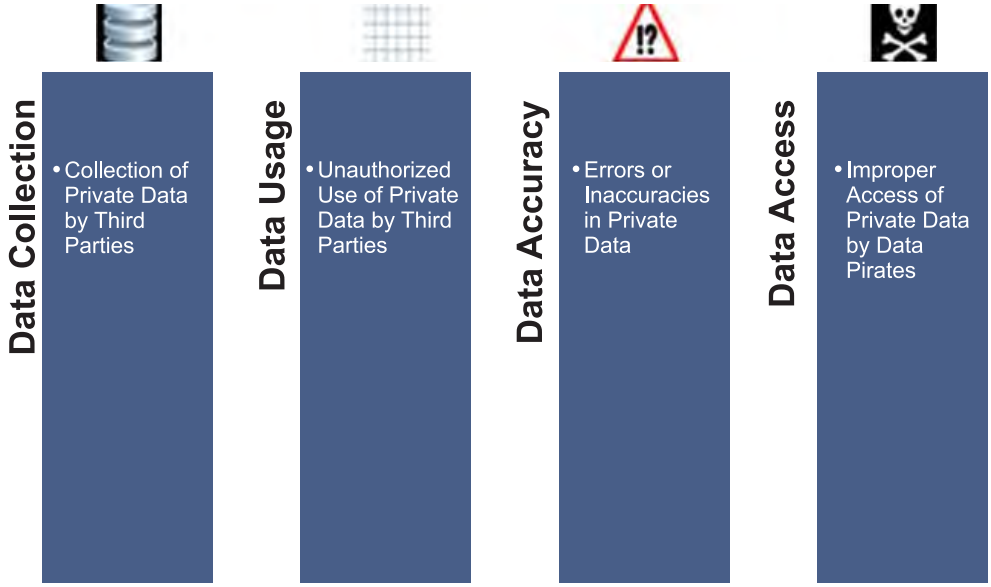

Figure 10.1 **The four pillars of privacy concerns (adapted from the CFIP Instrument by Smith et al.), which include data collection, data usage, data accuracy, and data access, summarize the current fears surrounding privacy within the general public.**

10.2 The privacy debate

The debate over privacy isn't a recent one, but the digital revolution has stoked the fire of controversy and caused heated social, economic, and political discussions around the globe. In this section, we'll look at what makes privacy controversial and what privacy threats exist today. We'll consider concerns over relatively new push technologies that send information to mobile users automatically by detecting their exact location. We'll also look at how placing control back in the hands of users through the opt-in concept can be an effective way of overcoming controversy.

Questions (many of which remain unanswered) surrounding privacy abound, and there's such a myriad of conflicting interests that the debate continues to grow unchecked:

- Who is responsible for privacy?
- Is it up to the individual or the state to govern privacy?
- When is it acceptable to forego privacy?
- When and how should individuals be notified about potential privacy breaches? By whom should they be notified?
- Is it possible to put an economic price on privacy?
- Where should the ethical and commercial lines be drawn in order to respect people's right to privacy?

- Should privacy protection in the digital world mirror the same safeguards of the real world?
- Is it acceptable to market certain services according to the real-time location of individuals?

Much of the concern surrounding privacy is not only that private information is collected but that it's happening "pervasively, silently, and cheaply." Although it's clear that unless you're a hermit living on a desert island, complete privacy is impossible, it's perhaps the ease with which detailed personal information can be gathered and processed that spooks the general public. Indeed, in the world of today and tomorrow, private information is quietly collected by ubiquitous devices and applications and available for analysis to many parties who can query, buy, or subpoena it—or pay a hacker to steal a copy of everyone's location history.[6]

We'll now look in a bit more detail at the privacy threats that users face and how a breach of security can impact these users.

10.2.1 Privacy threats

The four concerns highlighted by the CFIP instrument translate into a variety of privacy threats, which can be grouped in the following broad categories:

- *Spamming*—The flooding of an individual's inbox with unsolicited messages
- *Phishing*—The criminally fraudulent process of attempting to acquire sensitive information such as usernames
- *Identity theft*—A form of fraud in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources
- *Undisclosed government usage*—Used by government agencies for taxable status verification, for example
- *Malicious use of personal data*—By competitors, stalkers, bullies, and the like

Figure 10.2 matches the probability of these varied instances of security breaches (or privacy incidents) with the impact that they would have on the individuals concerned.[7] It helps to understand that even a seemingly innocuous tracking of online activity (such as online banking), point A on the chart, exposes individuals to significant risks (such as unauthorized bank transfers).

It also suggests that even the use of aggregated personal profiles (point B on the chart) carries significant risks for personal privacy, helping us to understand the rigorous checks and balances that developers need to juggle to deliver an LBS acceptable to the various parties involved.[8]

---

[6] Blumberg et al., "On Locational Privacy."

[7] David Riphagen, Probability Impact Matrix of Privacy Incidents, October 23, 2008. "The Online Panopticon. Privacy Harms for Users of Social Network Sites," 3TU (TU Delft, TU Eindhoven, and University of Twente), Centre for Ethics and Technology.

[8] David Riphagen, "Privacy infringement—Directions for protecting users' privacy online," June 25, 2007.

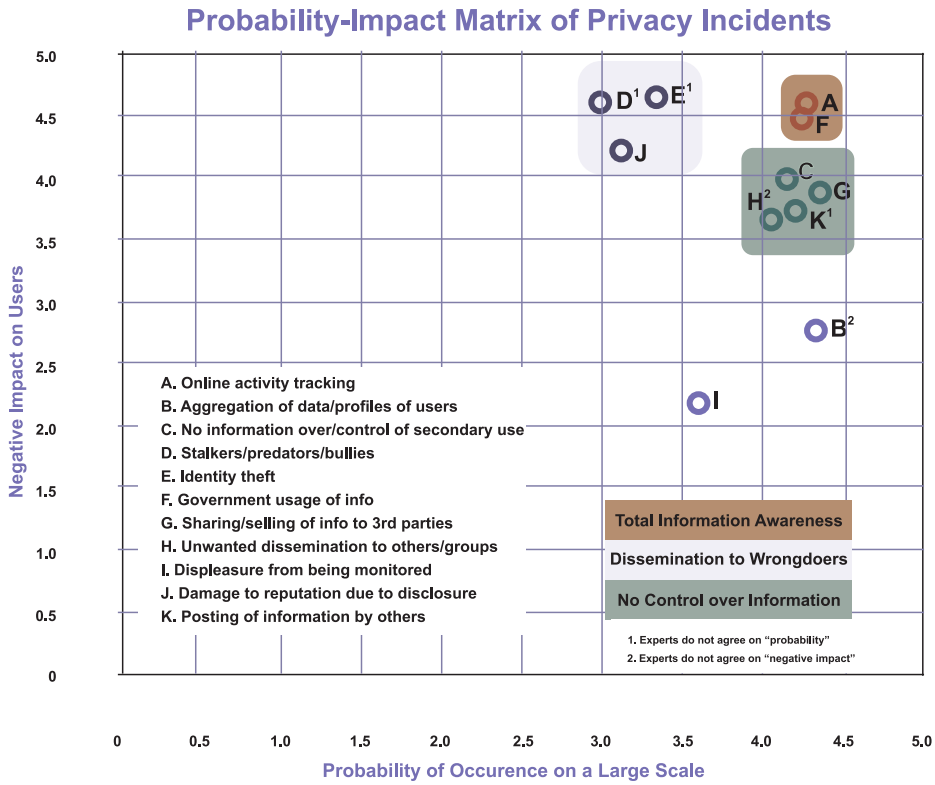

Figure 10.2 **Probability - Impact Matrix of Privacy Incidents shows the likelihood of different privacy breaches occurring and the negative consequences (from minor to serious impacts, such as identity theft). (Source: David Riphagen; reproduced with permission)**

A good example of the kind of controversy th at privacy issues can stir up is provided by the case of the Google Street View service, shown in figure 10.3 (an add-on to Google Maps p roviding 360-degree street-level views of places aro und the world). Launched in different countries from 2008 onward (from the United States to Europe to Japan), the service has repeatedly met with public outcries of indignation over privacy infringements and more than the occasional lawsuit.

Individuals are particularly upset that photos of their private homes are now available for everyone to see and that, in some cases, the faces of people snapped in the photos contained in Street View are recognizable—you can see not only the private home of someone but also the face of the person living there.

Google's point of view was succinctly stated in one lawsuit filing in the United States:

Complete privacy does not exist.

Figure 10.3 Screenshot of Google Street View (part of Google Maps) shows snapshots of street scenes in several countries across the world (from Japan, the United States, and Europe) but the service stirred controversy for infringing personal privacy because real people were depicted at specific locations.

Although Google generally doesn't break any laws in providing the service, the passionate nature of the privacy debate means that reactions are strong. One commentator, Osamu Higuchi (himself an IT professional), was highly critical of Street View in Japan and is representative of how culture plays a large role in determining the acceptability or not of potentially intrusive services:

> *In our way of living, you do not unilaterally, and in a machine-readable form, lay open people's living spaces to the whole world.*

Other commentators complained that although it's true that Street View does nothing other than present the same images anyone walking down the streets represented could see anyway, in reality Google is presenting a view to the entire world from the eye level of a person who is over 2.5 meters high, a person like none who actually exists.

Although the extent of the reaction has differed according to culture, overall Google has been forced many times to make faces, buildings, or sites invisible at the request of governments. It was perhaps Google's brushstoking the fire of the privacy debate that has led both global social networking giants Facebook and MySpace to initially block the rollout of the location add-on features to their service (though in 2010 Facebook rolled out Facebook Places in the United States and then in Europe). This is good news for start-ups offering location-based social networking, with newbies foursquare and Texas-based Gowalla (you saw them in chapter 5) expanding rapidly.

Now that you understand the specific privacy threats that individuals may face through unauthorized access to private data, we can move on to consider how push location methods are adding an extra fear specifically related to location. For every problem there's a solution, so we'll wrap up the next section by seeing how opt-in methods can be a useful way to allay this location privacy fear.

10.2.2 Push versus pull location

As you first saw in chapter 1, privacy legislation makes a distinction between subscribers of communication networks, such as mobile, who are actively requesting a location-aware service by opting in (and so consent to revealing their location) and those who are opting out. This difference in behavior is critical, because most of the privacy issues for LBS center on the idea of being tracked without knowing it.

Although the opt-in capability appears on the surface to be a convenient solution to the privacy issues of LBS, it's worth bearing in mind that this is only part of the answer. The deck is stacked against people choosing to take inconvenient measures to protect their privacy: it's often too hard for the average consumer to understand what options there are to avoid a location being recorded and too hard to keep researching these questions as they interact with new LBS services. In today's digital age, people haven't been able to adjust quickly enough to the advances in technology to intuitively choose the right option.

Whether the subscriber opts in or not determines which type of LBS service can be delivered:

- *Active use, or pull*—The location is requested by the consumer. Typical examples are location information (weather, local search) and navigation.
- *Passive use, or push*—The request for location is not initiated by the consumer. Typical examples are buddy finding and fleet tracking. Marketing companies can also potentially use push services to offer certain services available in certain places according to the real-time location of individuals, though the fear of LBS spamming is curbing this activity at the moment. Ironically, using location as an additional target parameter would allow advertisers, at least in theory, to send fewer and more relevant commercial messages, benefiting both the end user and the advertiser.

Subscribers who opt out can't use push services, because these work only where the mobile device has been allowed to track its own location.

Opting in versus opting out

The opt-in concept is fundamental to how LBS services manage privacy today. Privacy legislation has adopted this concept, and consumers are increasingly familiar with the notion. It's important to note though that much (if not all) of the general public opt in on the basis of trust, without fully acknowledging the TOS (terms of service) of the LBS.

The whole idea of opting in and opting out is to give the individual control. To a great extent, it appears that individuals' privacy concerns are affected by the level of control inherent in the delivery mechanisms of location content (that is, pull or push).[9] Because in pull-based LBS, the individual exercises greater control over the interaction, the decision to initiate contact with a service provider is voluntary, and location information is provided only to complete the requested transaction (for example, to inform the individual of the location of the nearest taxi). In contrast, in push-based LBS, the location information is tracked to target individuals who will likely be sent unsolicited information/services when they appear within the vicinity of, say, a retail store.

General consensus exists about using opt-in procedures to seek approval from users to capture and use their positioning history. There's disagreement as to whether this should happen on a case-by-case basis or once and for all. Although the first approach may not be acceptable from a usability perspective, the second may lead to some customers no longer being aware about their location data being shared.

In some cases, the decision of how to implement opt-in procedures will be out of the hands of the LBS service provider. Several mobile operators impose strict conditions for consumer-oriented LBS applications (such as friend-finder services) in order to shield themselves from the possibility of privacy breach lawsuits. "When in doubt, take the safest option" seems to be the common credo among mobile operators, despite openly attempting to foster openness and innovation.

Although things are changing, it's worth spending a few moments to understand which players are involved in managing the privacy game, from mobile operators to developers.

10.3 Who manages the privacy of LBS?

Five key players are involved in determining how the privacy of LBS is managed (excluding governmental agencies and lawmakers). Not all have an equal say, and the role of some players is being quickly reinvented. These players are[10]

- Mobile network operators
- Handset vendors
- Location aggregators
- Third-party developers
- Internet companies

---

[9] Heng Xu, Sumeet Gupta, Pan Shi, "Balancing User Privacy Concerns in the Adoption of Location-Based Services: An Empirical Analysis across Pull-Based and Push-Based Applications," available at https://www.ideals.illinois.edu/handle/2142/15224.

[10] Claire Boonstra, Guus van Knippenbergh, Sander Meijers (Open Mobiel Internet Initiative—OMI2), "Location Based Services on Mobile Internet," November 2008, available at http://sprxmobile.adix.nl/wp-content/uploads/2008/11/final-lbs-whitepaper-final-nov-2008.pdf.

Mobile operators and their view on privacy

As a developer of LBS, you should be aware that most mobile operators take a very conservative view of privacy. If your plans include being on portal or on deck as a highlighted LBS service with the mobile operator, you should consider adding extra privacy protection measures.

We'll now look in detail at each of these five players involved in managing privacy:

- *Mobile network operators*—Fortunately for the mobile ecosystem, the so-called walled gardens, which were set up by mobile network operators (MNOs) in order to control exactly what services were delivered to customers, are crumbling. Until recently, carriers controlled the whole LBS value chain. They were the only entities having access to the position of the user via control-plane technologies and at the same time initially generally allowed only hosted, carrier-branded, third-party applications, blocking GPS functionality to all other applications. If you weren't one of the few chosen ones to feature on deck with the mobile operator, you were left scraping the barrel at the long tail end of marketing. Instead, we're seeing what can be referred to as open playgrounds being created by mobile operators. These are dedicated developer environments with relatively streamlined procedures for bringing new apps to market.

  This doesn't stop MNOs from simultaneously imposing limitations on accessing their location platforms. Almost no MNO currently offers anything other than pull mechanisms for location detection by consumer LBSs (the user has to request to be located), although the push mechanisms discussed previously (tell me automatically where I am and push relevant info to me) would yield the greatest benefits to the user.
- *Handset vendors*—Some handset vendors such as Nokia are gradually taking over the role of carriers in the LBS value chain by providing their own A-GPS service on Secure User Plane Location (SUPL)–compatible handsets. As such, Nokia acts as the gatekeeper of the users' privacy. The recent announcement to open up access to Ovi Maps to third-party developers makes this role even more important. Nokia uses location data to establish reference databases of Cell IDs and Wi-Fi hotspots in order to offer alternative positioning capabilities in indoor environments to its end users.
- *Location aggregators*—In an attempt to open up their location assets and generate additional revenue, North American carriers such as Sprint are starting to partner with location aggregators such as uLocate, WaveMarket (now called Location Labs), and LOC-AID, through whom third-party developers obtain access to location data. In many cases the aggregator takes over the carrier's privacy gatekeeper role.

- *Third-party developers*—The arrival of the SUPL standards has made installing any third-party LBS application on any GPS smartphone possible. Importantly, it's now up to users to protect their own privacy by checking the trustworthiness of the developer before deciding to opt in. Users are the gatekeepers of their own privacy by controlling which applications to install.
- *Internet companies*—With the arrival of geo-enabled mobile web browsers and LBS applications, privacy control is being put squarely in the hands of internet companies such as Google, which offers applications such as Mobile Maps including local search and the Latitude friend-finder and social networking solution. As the barriers between mobile and traditional web continue to blur and greater convergence is achieved, internet companies are likely to have a greater role in managing privacy on mobile devices.

10.4 Privacy legislation

In 1995 the European Union adopted a series of directives (now in force across the EU), dealing with privacy of users of LBS, which are the subject of ongoing amendments to keep them relevant to changing technology. According to the EC directives regarding privacy (95/46/EC, 97/66/EC, and 2002/58/EC IV), three key principles must be followed when deploying LBS: disclosure, consent, and data security. The main thrust behind each principle is summarized here:

1. *Disclosure*—Any company that acts as a location data collector should disclose to consumers what kind of data is being collected about them and the purpose or use of such collection. Transparency by the data collector is key within this principle.
2. *Consent*—The data collector should obtain the data subject's consent before collecting their personal data. This is also referred to as opt in and opt out for the use of location.
3. *Data security*—Data collected should be protected by adequate security measures against accidental loss, theft, disclosure, destruction, illegal processing, or something similar. Archiving of personal location data can be done only with the explicit approval of the user.

10.4.1 Avoiding the data privacy booby traps

Some general guidelines are available to help LBS developers and entrepreneurs comply with privacy legislation on personal data, alleviate privacy concerns of the users, and avoid potential litigation:

- Don't collect data in the first place.
- If you have to collect data, don't store it.
- If you really have to store data, anonymize it.
- If you really need to store data and can afford to, encrypt it.

Avoid legal compliance costs

If a corporation retains logs that track individuals' locations, it may be subject to legal requests for that information. Such requests may come in different forms (including informal questions, subpoenas, or warrants) and from different parties (law enforcement or civil litigants). There are complex legal questions as to whether compliance with a particular request is legally required, optional, or even legally prohibited and a liability risk.

This legal complexity may even involve international law. For instance, US corporations that also have operations in the European Union might be subject to European data-protection laws when EU citizens visit the United States and use the US company's services.

Corporations with large locational datasets face a risk that lawyers and law enforcement will realize the data exists and begin using legal processes to obtain it. The best way to avoid this costly compliance risk is to avoid having identifiable location data in the first place.[11]

DON'T COLLECT DATA IN THE FIRST PLACE

This may seem easier said than done, and it's inevitable that perhaps some data is collected. While limiting data retention is an important protection for privacy, it's no substitute for the best protection: not recording that information in the first place. It's worth dedicating time and effort to really consider which information absolutely needs to be collected. If you're unsure of whether some data is needed, the best default approach is not to collect it.

IF YOU HAVE TO COLLECT DATA, DON'T STORE IT

LBS providers should retain user location information only as long as business needs require, and then they must destroy or render unreadable such information on disposal. If it's necessary to retain location information for long-term use, where feasible, LBS providers should convert location information to aggregate data (see the next point).

Because storage space is cheap and getting cheaper, nowadays it's more a case of resisting temptation by not storing data, because this is often the path of least resistance. If you have to store data temporarily, be aware that secure deletion tools are necessary to make sure that deleted data is really gone.

IF YOU REALLY HAVE TO STORE DATA, ANONYMIZE IT

The majority of LBS services store data at an aggregate level only, grouping personal usage history by geography (neighborhood, city, country), gender, age, or other variables. This aggregation makes it possible for third parties to use the information while protecting the anonymity of individual users. We should note that even the existence of location databases stripped of identifying tags can leak information.

---

[11] Blumberg et al., "On Locational Privacy."

For instance, if you know that John is the only person who lives on Brocko Bank Lane, the datum that someone used a location-based service on Brocko Bank Lane can be reasonably linked to John. Generally speaking, one solution to this problem is to restrict the use of location-based services to high-density areas, though this may not be a practical solution in some cases.

IF YOU REALLY NEED TO STORE DATA AND CAN AFFORD TO, ENCRYPT IT

Using cryptography and careful design to protect location privacy from the outset requires engineering effort. It's not a cheap solution and tends to be used more widely with highly sensitive information (such as financial records). Modern cryptography allows data processing systems to be designed with a whole spectrum of privacy policies, ranging from complete anonymity to limited anonymity to support law enforcement. Although not cheap, data encryption provides both the LBS user and the service provider with the greatest peace of mind.

Now that we've looked at specific data storage issues related to location data, it's worth seeing how best practice guidelines have filled the gap in the current privacy legislation. Although there's no legal requirement to comply with these guidelines, this is advisable as tighter and more specific legislation comes into place over time.

10.4.2 Best practice guidelines: Cellular Telephones Industries Association

The Cellular Telephone Industries Association, or CTIA, publishes recommendations on how LBS services should deal with privacy legislation, particularly referring to how the responsibilities should be allocated between the mobile operator or wireless carrier and the LBS application provider. The CTIA bases its recommendations on three cardinal principles, those of notice, consent, and safeguards.

Rewarding the user for providing location data

Users of mobile services are increasingly becoming aware of the value their location data represents to LBS vendors. In the advertising space, users have come to expect something in return when agreeing to receive advertising messages on their phones. Both in Europe and the United States, LocatioNet is offering a free navigation service subsidized by advertising. Although for the time being it might be difficult for many vendors to have the cost of their services fully covered by advertising, they should at least offer discounts to users who opt in for advertising.

Similarly, the "free services in return for access to location history" paradigm will start to gain momentum. This is particularly true for applications such as TomTom MapShare, where location data is used to improve the quality of the service. The same holds for Google and Nokia, which have used location data from private individuals in the past to build reference databases of base station Cell IDs and Wi-Fi hotspots.

There's something fundamentally unethical about letting users pay full price for information they've helped to collect. All players in the location ecosystem will have to realize that the location goldmine comes at a price.

Table 10.1 maps out the different responsibilities in the case of a typical LBS application, clearly highlighting areas that require consent and notice.

The CTIA suggests that LBS providers should give notice, especially if location information is to be used for any purpose other than providing the LBS itself. It goes on to distinguish between implicit and explicit consent, to account for the fact that some users may not be aware of or be in a position to control the tracking of their position, for example, in the case of fleet tracking or employee monitoring. Here, consent would be implicit or reasonable based on the case of the employee's work contract.

The CTIA also states that LBS providers must allow LBS users to revoke their prior consent to disclose location information to all or specified third parties. Where technically feasible, LBS providers may provide for selective termination or restriction of individual LBS applications upon LBS user or wireless carrier account holder request (see table 10.1).

In terms of safeguards, the CTIA makes the following recommendation on the security of location information:

> *LBS Providers should employ reasonable administrative, physical and/or technical safeguards to protect a user's location information from unauthorized access, alteration, destruction, use or disclosure. LBS Providers should use contractual measures when appropriate to protect the security, integrity and privacy of user location information.*

As a final protective measure, it recommends that LBS providers should provide a resource for users to report abuse and provide a process that can address that abuse in a timely manner.

A wireless carrier provides its users with a wireless device having on-deck access to a mapping service enabled by third-party software. The wireless carrier provides the user's location information to the third party, which in turn informs the user of services in the area.

Privacy International, an NGO advocating for privacy

Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. Its campaigns around the world aim to protect people against intrusion by governments and corporations that seek to erode the right to privacy. It believes that privacy forms part of the bedrock of freedoms, and its goal is to use every means to preserve it. At the moment, PI doesn't offer anything resembling a stamp of approval for companies adopting good privacy conduct, and this remains a need waiting to be filled.

In the final part of this section on privacy legislation, we'll look at how mobile companies in the LBS ecosystem have been able to meet legal requirements in ways that attempt to minimize the impact on performance of location-aware applications.

Table 10.1 Best practices and guidelines for location-based services according to the US-based CTIA, making a clear distinction between the responsibilities of the wireless carrier/mobile operator and the LBS application provider

Wireless Carrier	Application Provider
A wireless carrier is an LBS provider because it provides the location to the third party.	An application provider is an LBS provider because it receives location information from a wireless carrier to provide an LBS to a mobile user.
The wireless carrier should provide a notice to its account holder that: • the device is location-enabled; • an authorized user may use a location application available on deck or on the main menu; • by initiating the service, the account holder authorizes the disclosure of the user's location to the third party whenever the LBS is used; • it may retain information regarding the user's location and use of the LBS for as long as it has a business need; • the user should review the application provider's privacy policy to understand how it uses and protects location information; • the user should not initiate the service if he or she does not want to share location information with the third-party application provider; See Section 4.A as an example.	The application provider should provide notice to the LBS user that: • the user's location is being collected in order to provide the service; • the location information (will/will not) be disclosed to others; • the location information is retained only so long as necessary to provide the service (e.g., to provide the location of the nearest ATM to the LBS user's location on the map); • aggregate location information may be created by removing or obscuring personally identifiable information; • aggregate location information may be used to provide location-sensitive advertising; • no further notices or reminders will be provided.
By purchasing the wireless service with location-enabled services, the account holder agrees that the wireless carrier may disclose a user's location information to the third-party application provider.	The user agrees to the terms and conditions governing the service.

10.5 Complying with privacy legislation

Developers have at their disposal five main tools to both curb privacy fears and comply with privacy legislation:

- Setting user profiles
- Opt-in screens
- Fuzzy location
- Terms of service
- Geofencing

We'll take a look at each of these tools in turn, with some practical examples from live applications where appropriate.

10.5.1 Setting user profiles

Many LBS vendors include settings and features in their applications in order to allow users to manage and control their privacy.[12] For example, Google Latitude gives users the option to be visible or invisible to their friends. The full range of settings that can be adjusted is potentially limitless and can include controls over the following:

- Who sees what (Let co-workers see what I do near the office but not elsewhere.)
- Which locations are private and which are public (My home location is always private.)
- Whether others can contact or add users according to proximity (I don't want to appear in public listings.)
- How recent a location trail is (I want to share my last known location with a 24-hour delay.)

Ultimately, a balance needs to be found between sufficient levels of privacy protection and the overall customer experience. Settings should also be as flexible and user friendly as possible. In particular, the user should be able to easily switch off location sharing at any time.

Similarly, settings defining when and which locations are shared add to the overall feeling for the end users of being in control. Manual settings greatly deteriorate the user experience, with many users forgetting to switch on and/or configure their applications on a continuous basis. Some LBS applications put full control in the hands of the end user by allowing only manual position sharing; users decide when and where to share their location, either via address input or by clicking their position on a map. This lowers the temporal resolution of location data.

Nokia has attempted to combine privacy setting flexibility with ease of use by allowing users to share locations selectively but automatically, based on matching current positions and predefined favorite places. Locations are broadcast only when users are at or near a publicly defined and allowed place that doesn't require the user to take any action.

Dynamic or more intelligent ways of regulating settings (with the possibility of porting preferred location settings from one service provider to another) ultimately point the way to managing user settings in the future.

10.5.2 Opt-in screens

You saw in section 10.2 how the opt-in concept was essential to comply with basic privacy standards of LBS. In practice, regular opt-in reminders should be issued. How this is done will vary slightly according to both the mobile operator (for on-deck services)

[12] Dominique Bonte, "Exploiting the Location Goldmine While Respecting Privacy—A Delicate Balance," ABI Research.

and the mobile development platform being used. On some Nokia devices running Symbian OS, for example, the device may force an opt-in message every time location is being tracked. On the iPhone it's more typical for one-off opt-in screens to be used rather than repeat ones. Figure 10.4 show typical iPhone screenshots of the Starbucks and AccuWeather applications' opt-in screens. Both of these applications can only deliver meaningful results if the opt in is accepted, so in reality users have little choice to opt out if they want to use the application.

Some argue that the biggest issue with opting in is the lack of information provided to the user about how often and for what purpose the location data will be used. In the case of Google Maps at launch, users didn't understand they were contributing to Google's efforts to build a reference database of Cell IDs and Wi-Fi hotspots used as alternative positioning technologies to complement GPS for indoor coverage.

Opt in is clearly a more sensitive issue when it comes to social networking applications, particular those that are open to the general public. The Dopplr iPhone application is a good example of opt in linked to user settings, which allows users to find relevant information around them, based on their location (opt in) but at the same time keeping their location footprint private (opt out). The relevant screenshots from the Dopplr application are shown in figure 10.5.

Opt-in screens have their value, but another way to protect privacy in LBS applications is to use a "fuzzy" position instead of a precise one, which we cover next.

Figure 10.4 **iPhone screenshots of the Starbucks and AccuWeather applications' opt-in screens**

Figure 10.5 **Screenshots from the Dopplr iPhone application, showing how users can opt in to use their current location to view local services or people but opt out from granting access to their private location data or footprint for use within anonymized statistics**

10.5.3 Fuzzy location

A popular way to protect privacy is to share a fuzzy position instead of precise GPS coordinates. Inaccurate location sharing was and still often is the only possibility on non-GPS handsets. Although alternative positioning technologies based on Cell ID and Wi-Fi are becoming more widespread, they don't offer the same accuracy as GPS. Reducing accuracy is also offered as a deliberate privacy protection measure on GPS handsets, sharing neighborhood or city location attributes instead of precise coordinates. At the same time, the reduction of the spatial—but also temporal—accuracy of location information limits both the user experience and the usefulness of the historical location data to third parties.

10.5.4 Terms of service

A good terms of service (TOS) agreement is an essential part of any location-aware application, and erring on the side of caution is a sensible play when it comes to privacy protection. For example, Centrl (a US-based LBS provider) adopts a safe policy by keeping the user's last known location for a week and doesn't store the user's location history. If the user doesn't log in for more than a week, the last location is also removed. (You can read GyP Sii's full TOS here as a useful benchmark: http://corporate.gypsii.com/content/view/8/.) GyPSii also anonymizes data on user behavior it stores by aggregating it in line with other LBS services, like Dopplr.

10.5.5 Geofencing

Geofencing is a relatively new development within the area of location-aware apps. A geofence is a virtual perimeter for a real-world geographic area. The basic concept is to allow users to draw virtual fences around neighborhoods or other locations where a user may want to allow a location service to know where they are and places where

they prefer not to. In this way, geofencing can be used to test whether presence inside the fence is true or false in order to trigger some sort of action.

A developer may set a dynamic geofence (that is, a radius around a specific type of location, such as a supermarket chain) or a static one (that is, around a school or home location).

The interesting idea from a privacy point of view is that it allows users to set their own blackout areas, where their location will always be unknown to the mobile application that's active. Alternatively, a geofence may be used to trigger push notifications (which we explored in section 10.2). Users could automatically check in to services like foursquare when entering the geofence of a particular location.

In the last section of this chapter, we looked at some practical guidelines for complying with privacy legislation when applied to location-aware applications on mobile devices. Although it's difficult to cover every individual potential privacy issue that may arise, the set of tools at the disposal of developers that we covered provides good compliance with current privacy legislation.

10.6 Summary

Privacy remains a hotly debated area for location-aware or location-based services, with opinions heavily polarized between those who believe online privacy no longer exists and those who wish to preserve total control of their private life (without perhaps realizing that true privacy is a utopia in today's digital age). The debate is likely to be around for a while yet, and service providers should play their cards wisely by complying with legislation and promoting transparency over data usage. Increasingly, the ability to demonstrate reliable privacy protections will offer firms a competitive edge if they can persuade their customers that their service offers more robust and trustworthy privacy protections. As we continue to move toward always-on services with continuous real-time updates, the challenges of dealing with the increased complexity and volume of private data will grow. Successful location-based services will need to strike a balance between crafting a simple-to-use application and one that simultaneously allows the user to always be in control over what they reveal, to whom, and when.

With competition intensifying and better and better apps being rolled out, allowing users to easily discover your star application is vital to guarantee your success. In the next chapter, we'll consider the key aspect of application distribution to ensure the best result from the development efforts involved in building your location-aware application.

MOBILE TECHNOLOGY

LOCATION-AWARE Applications

Ferraro • Aktihanoglu

Mobile customers want entertainment, business apps, and on-the-go services that recognize and respond to location. This book will guide you through the technology and business of mobile applications so you can create competitive and innovative apps based on location-based services. It is an engaging look at the LBS landscape, from choosing the right mobile platform, to making money with your application, to dealing with privacy issues. It provides insight into a wealth of ideas for LBS development so you can build the next killer app.

What's Inside

- Managing location-aware content
- Making money from location-based services
- Augmented reality and tablets
- Detailed examples for iPhone and Android

This book is written for developers and business pros—no prior knowledge of location-based services is assumed.

Ric Ferraro cofounded GeoMe Communications, a location-aware app innovator. **Murat Aktihanoglu** is the founder of Centrl.com, a location-based social network.

For access to the book's forum and a free ebook for owners of this book, go to manning.com/Location-AwareApplications

"A practical technology- and business-oriented introduction."
—Gabor Paller, Ericsson

"Clear and concise. You will never be lost while reading this book."
—Jeff Addison
Southgate Software Ltd.

"The Rosetta Stone of location-based mobile services."
—Valentin Crettaz, Goomzee

"A definitive source ... highly recommended!"
—Dr. Florian Resatsch
friendticker.com

ISBN 13: 978-1-935182-33-7
ISBN 10: 1-935182-33-1
54499
9 781935 182337

MANNING $44.99 / Can $51.99 [INCLUDING eBOOK]