

1-1-2004

Privacy Issues in Location-Aware Mobile Devices

Robert P. Minch
Boise State University

Privacy Issues in Location-Aware Mobile Devices

Dr. Robert P. Minch

rminch@boisestate.edu

Dept. of Networking, Operations, and Information Systems

College of Business and Economics

Boise State University

Boise, ID 83725-1615

Abstract

Location awareness, the ability to determine geographical position, is an emerging technology with both significant benefits and important privacy implications for users of mobile devices such as cell phones and PDAs. Location is determined either internally by a device or externally by systems and networks with which the device interacts, and the resultant location information may be stored, used, and disclosed under various conditions that are described. Thirteen specific privacy issues are enumerated and discussed as examples of the challenges we will face as these technologies and their associated products and services are deployed. Regulation by governments, standards organizations, industry groups, public interest groups, and marketplace forces are discussed as it may help address privacy issues.

1. Introduction¹

We are on the cusp of a new era in technology where the location of computing and communications devices can be determined accurately and inexpensively. This will have particular importance for location-aware mobile devices such as cell phones and PDAs, and will raise a large number of privacy issues related to the collection, retention, use, and disclosure of location information. Drivers of the issues we will face include: (1) technologies such as geographical positioning systems (GPS) that can be inexpensively incorporated into even very small portable devices; (2) government mandates such as Enhanced 911 (E911) in the United States that require the incorporation of location-determination capabilities in certain devices such as cell phones; and (3) marketplace opportunities for products and services that exploit location information and fall

under the rubric of mobile commerce or m-commerce. Location awareness is a subset of context-aware computing, which also considers other contextual information such as user, time of day, nearby people and devices, and user activity. It is typically considered the most or one of the most important contexts, and few contexts other than location have been used in actual applications [4].

There is little doubt that location-aware (sometimes also called location-enabled) mobile devices have enormous potential for enhancing safety, convenience, and utility in our lives. Already emergency services are being improved by the ability of responders to quickly locate persons making emergency calls on enhanced 911 cell phones or involved in accidents in location-aware vehicles. Parents can monitor the location of their children, who can summon assistance with a “panic button” on location-aware watches. Time and location-sensitive weather, traffic, and navigation information can be tailored to better meet the needs of users in specific locations. Even existing conveniences such as the ability to track package delivery from city to city may be enhanced to the extent that recipients are able to obtain precise estimates of delivery times and even track package locations as they are driven through the neighborhood to their house. Soon, consumers will benefit from many new offers of products and services that may be personalized and tailored based their location and the locations of other entities that they deal with. Market research firms estimate the worldwide market for location-specific services market to be \$18.5 billion to \$20 billion by 2005 to 2006 [19].

Unfortunately, the same technologies that bring the benefits mentioned above also raise myriad privacy issues due to their capability to collect, store, use, and disclose the locations of those who use them. Freedom of movement and rights of privacy may be compromised due to tracking of citizens in what some fear could become a “Big Brother” society. Workplace practices such as employee monitoring,

¹ Portions of this paper are partially based on [29].

already controversial, may be exacerbated when location information is added to other data collected. Intrusive marketing practices may be further enabled through extensive consumer profiling based on shopping and travel patterns. Correlation of a person's location with identifiable facilities such as clinics may allow inferences to be drawn concerning health and other intensely personal information. Even personal safety may be jeopardized in cases such as stalkers being able to locate and track their victims.

Privacy has many definitions, including "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [31, p. 7] and "the selective control of access to the self" [1, p. 24]. An examination of various privacy definitions [16] derived a formal definition as an "abstract skeleton" of the means and ends of privacy where privacy "as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" [16, p. 10]. The present research will build upon the definition of [31] and employ a working definition of privacy as essentially an information and communication-based construct—namely the manner and extent to which persons can control how information about them is: (1) collected; (2) retained and/or maintained; (3) used; and (4) communicated, disclosed or shared. Location privacy may then be defined as privacy relating to location-specific information.

Privacy has been studied in a variety of online contexts and has been ranked as the top concern of Internet users, with various surveys reporting large majorities of online users being concerned about privacy [26]. Unfortunately, location-related privacy has received relatively less attention to date. For example, a recent special issue of the Journal of Social Issues on privacy contained only a handful of passing references to location or location privacy in the entire issue of ten articles [17]. At this point in time, still relatively early in the development and implementation of location-aware mobile devices and when businesses are rapidly investigating their possibilities for future products and services, it is important that privacy implications be considered. In doing so, we may be able to not only safeguard against clear abuses of the technology, but also guide its implementation to reassure the public and promote acceptance to reap the many available benefits in appropriate contexts.

This paper describes exploratory research in preparation for theory building and empirical investigation. It attempts to identify important privacy issues related to location-aware mobile devices, and

organize them according to the four information and communication-related components in the working definition of privacy presented above. It is outside the scope of the present research to attempt a comprehensive theoretical framework encompassing all relevant dimensions of privacy; technological capabilities and uses of location-enabled mobile devices; and social, legal, and public policy implications. By enumerating important questions that occur where emerging technologies and privacy components intersect, however, it is hoped that both future theory building and empirical research will be facilitated.

In following sections we will first place issues of location-aware mobile devices in context by addressing the basic technology issues involved. This essentially determines what is and is not technically feasible now and in the near future. The next section outlines the privacy issues that arise from the conjunction of technical feasibility and government/marketplace activities that might use location information. A representative sample of important issues is enumerated and discussed. Regulation is then discussed—a broad term covering the various entities and agencies that might structure and regulate the use of location information and provide the appropriate levels of privacy protection to constituents while promoting appropriate advances in new products and services. Finally, a summary and conclusions section recapitulates major issues, identifies future challenges, and suggests further research needed.

2. Technology and Context

There are many possible structures or taxonomies that could be used to organize discussion of location-aware mobile devices and their privacy issues. The one chosen here has several advantages. First, it incorporates the major definitional components of location privacy in terms of location-related information processing while also corresponding to the temporal sequence they will typically follow in practice. These activities are the: (1) collection; (2) retention; (3); use; and (4) disclosure of location-related information. Second, it is consistent with other taxonomies suggested in related contexts such as privacy concerns in Internet marketing [30]. In [30] the areas of privacy concern are improper acquisition (collection), improper storage (retention), improper use, and privacy invasion as it related to customer data. Disclosure was treated as a combination of improper use and privacy invasion. Finally, proposed legislation and regulation such as the Location Privacy Protection Act of 2001 [15], which addressed the

“collection, use, disclosure of, and access to consumer location information,” tend to use similar categories of issues and similar terms. In the remainder of this section, therefore, the four activities of collection, retention, use, and disclosure of location-related information are discussed to provide a broad technology and context background; privacy issues will then be more specifically addressed in following sections.

2.1 Location information collection

Collection of location information can first be categorized according to the two main methods for determining a mobile device’s location: internally and independently by the device itself or externally by other devices it communicates with. In the cellular communications industry, these are sometimes called handset-based or network-based approaches, respectively [11]. By far the most prevalent method for independent location determination, particularly on a geographically macro scale worldwide, is the Geographical Positioning Systems or GPS. With this method, a GPS receiver inside the device receives information from several of 24 orbiting satellites maintained by the U.S. government. With reception from at least three satellites, position may be calculated in two dimensions; with four satellites in three dimensions; and with more (even handheld devices commonly simultaneously receive from six to twelve) accuracy and reliability improve. With the removal of a signal-degrading method called selective availability in 2000 [10] typical accuracy is within approximately 10 meters, and with various methods of information enhancement, supplementation, averaging, etc. it can be within a meter or less. Note that these mobile devices act only as receivers, therefore location determination is indeed done independently and neither the satellites nor any other external entity knows the device’s location.

External determination of location information is done in a variety of ways and with varying characteristics of accuracy and reliability. Perhaps the simplest method is to approximate the location of a mobile device according to a known location of another device it communicates with. For example, Phase 1 of enhanced 911 emergency response service (E911) in the U. S. [19] relies on the locations of cellular telephone towers to approximate the location of cellular telephone handsets to within about ten kilometers. Accuracy depends on the geographical configuration of the network and the particular technologies in use. In shorter-range networks such as Bluetooth, location of participating network nodes may be determined within ten meters or less. More

sophisticated location determination may be done through measurements and calculations related to latencies and other characteristics of the communicated signals themselves. For example, Phase 2 of E911 [6] relies on multiple cell towers to triangulate the location of handsets to within 50-150 meters, with various hybrid and enhanced approaches achieving even greater accuracy. Interestingly, E9111 legislation and regulations allow communications providers to choose either the internal or external location determination methods, and to date at least some providers have opted for each.

There are other technical issues in location information collection, such as whether location determination occurs automatically or on request, whether collection is continuous or discrete, and further issues related to accuracy and reliability. For m-commerce and other applications requiring the location of devices indoors or with much greater accuracy than technologies such as GPS allow, other methods are possible. For example, sensor networks for mobile devices have been demonstrated with an accuracy of a few centimeters [25]. There are also additional ways of defining location awareness. In addition to absolute methods such as used with GPS, there are relative methods that refer to what located objects are nearby, and the closely related proximity awareness that results when several items are cognizant of each others’ relative locations [14].

2.2 Location information retention

Retention of location information has two main technical components. The first, where the location information is stored, is similar to but independent of the determination issue: whether the location information is retained only on the local device or externally at other facilities. Even if location is initially determined independently by the device, it may be (and often is) subsequently transmitted to other elements in a larger system or network for additional processing and use. Of course an externally determined location is by definition retained externally as well, although this may be only temporarily. The second technical component concerns the quantity and persistence of location information—how much is stored and for how long—and other characteristics of the stored information itself. For example, many location-enabled devices maintain a list of discrete locations and/or vector-distance information that can be used to re-create a “breadcrumb trail” of the device’s movements.

Specialized server strategies for maintenance of location information have been proposed for applications such as mobile e-commerce [13].

Consumer concerns in such applications may prove to be at least as important as technical considerations, however, as a majority of adults surveyed disagree with the proposition that “Most businesses handle the personal information they collect about consumers in a proper and confidential way.” [9]

2.3 Location information use

Use of location information is limited only by processing ability and ingenuity of system designers and users in particular applications. Typically computation of speed, direction, and geographical relationships between entities are initial steps in further processing. For example, the processing of location information for a rental car can be used to determine whether the car is exceeding the speed limit, approaching the car rental office, or parked next to other rental cars. Other common location-enabled applications already in use or under development include [19]:

- Destination guides, where maps, directions, and other information can be adjusted to a user’s current location
- Environmental condition reports that are location-dependent, including weather and traffic reports
- Wireless advertising and electronic coupons, including offers that may be made to potential customers in real time as they approach storefronts
- Finders for friends, cars, children, etc.
- Roadside assistance, in which responders may be dispatched either upon request or automatically (in the case of a crash, for example)
- Real-time routing assistance, where a user’s direction and speed are taken into account as turn-by-turn instructions are given to guide a user to a destination
- Other mobile information services such as yellow pages, where retrieved information may be customized with locational context, e.g., by sorting information on Chinese restaurants according to their distance from a user’s location.

Use of location information will be discussed more with regard to specific privacy-related applications and issues later.

2.4 Location information disclosure

Disclosure of location information has many relatively non-technical privacy-related issues discussed later, but also a number of highly technical aspects. For example, information and communications security has an essential role to prevent unauthorized disclosure of location information. This is particularly important where location information determination, retention, or use occurs externally to a user’s device and such information is communicated over wireless networks where traffic may be intercepted by unauthorized parties. Disclosure issues also arise where there are different providers of the basic communication traffic and the supplemental location information. For example, a (non-carrier) commercial m-commerce vendor may place devices on cellular carriers’ towers to listen to traffic and determine locations.

One of the most significant technical initiatives dealing with location information disclosure is the Geographic Location/Privacy (Geopriv) working group sponsored by the Internet Engineering Task Force [7]. Its charter states that its primary task is “to assess the authorization, integrity, and privacy requirements that must be met in order to transfer such information, or authorize the release or representation of such information through an agent.” [7]. Markup languages and other methods for specifying user geographic location privacy preferences are addressed in the group’s work.

In order to support m-commerce, it will commonly be necessary to exchange information among a number of parties. In a location-enabled m-commerce environment, for example, the following scenario might be typical:

1. The customer uses an integrated device with both computing and communications capability, likely connected to the Internet via wireless WAN (e.g., PCS), LAN (e.g., WiFi/802.11x), or PAN (e.g., Bluetooth).
2. The customer’s location is determined, possibly independently though a technology such as GPS, but quite likely through interaction with a communications carrier if the device has cellular telephone capabilities, or perhaps while roaming among wireless LAN or PAN zones.
3. Location information is shared between device/user, carrier/network, and businesses or other service organizations. This may be done automatically in subscription-based services such as traffic alerts, initiated by the user for information requests (so called “pull” applications), or initiated by marketing

activities of companies wishing to solicit customers (“push” applications).

4. Additional information necessary to complete business transactions, if any, is exchanged for credit verification, etc. In some cases even this may involve location information, as location relative to national boundaries and other factors may affect the conduct of business.

Of course, the above exchanges of information including location engender a number of disclosure issues, some of which will be addressed in the following sections.

3. Issues

We are now in a position to discuss privacy issues that arise from location-enabling technologies and their applications. This can be done within the previously-described framework addressing the collection, retention, use, and disclosure of location-related information—largely by asking the following question within each category: What intersections of technologies, applications, and marketplace or governmental activities create the potential for important privacy-related implications? Example issues, both existing and foreseeable, will be included. It should be noted that in the topical order treated, issues become more complex and controls more difficult as we progress, i.e., once location information has been collected and stored, it becomes more difficult to control its disclosure than if it had not been collected and stored at the outset.

3.1 Collection issues

The primal issue concerning the collection of location information for a device is, of course, who determines whether location determination is enabled or not. For devices owned by their user, with independent location determination and with no compelling outside interests (e.g., a hiker using a handheld GPS), few would argue against the owner/user normally being in control. Exceptions would include legally mandated circumstances—an extreme example being court-ordered location tracking of parolees via non-removable monitoring devices. User choice is not technically possible with external location determination (e.g., cellular telephone systems must at least know what cell towers a user is near in order to forward calls), or permissible with regulated communication systems such as E911 (where devices and providers are required to disclose location information for emergency response).

Furthermore, location determination is not always a simple and independent yes or no question. Varying degrees of location precision might allow determination only of whether a user is within a particular service area or otherwise-defined zone, rather than their precise location within these regions. One-time, ad-hoc, or randomly scheduled location determination may prevent effective further processing of location information to compute speed and direction, while continuous or systematically-scheduled determination may allow this inferential processing. Note however that the privacy issues raised in location information collection are relatively minor, as there is little potential for abuse until that information is retained, used, or disclosed in some way.

3.1.1 Issue 1: Should users of location-enabled devices be informed when location tracking is in use? Should they be permitted to turn it off? Should an opt-in or opt-out approach be used? What factors will determine these answers?

3.2 Retention issues

Retention issues for location information concern what information is stored, where it is stored, how long it is stored, and how securely it is stored. Some of these issues closely relate to usage and disclosure, and thus if they involve significant processing or transfer of information that will be treated in later sections. As with collection issues, however, the very first issue of importance is who decides the answers to the questions raised by the above issues of what is stored, where it is stored, and indeed whether anything at all is stored to begin with. A user exercising free choice and giving informed consent is presumably much less susceptible to unwanted privacy invasion than one without complete information or right of refusal.

3.2.1 Issue 2: Should users of location-aware devices be permitted to control the storage of location information?

What information is stored is important because the identifiability and level of detail affect potential future uses (and abuses) of the information. For example, if the location of a multi-user mobile device is stored at one particular time, this would not necessarily allow strong inferences about the user of the device. If, however, location information is recorded along with a sequence of authenticated transactions (e.g., a user uses a mobile phone to purchase items from vending machines using supplemental authentication each time) then the

information might be linked to a particular user rather than the device alone.

3.2.2 Issue 3: Should location information as stored be personally identifiable, or should the user have options to preserve degrees of anonymity?

Where information is stored is important because it helps dictate who controls the information and how it can later be used or disclosed. Locally stored information that is erasable by a device's user is less vulnerable to abuse than externally stored information. In particular, information stored externally in large centralized databases opens up the possibility for information matching against other databases that may be objectionable. For example, in the U. S. it is already against the law to discriminate against loan applicants based on the neighborhoods they live in. If consumer credit providers were to base individual purchase authorizations partly on the location of merchants involved, this could create a similar potential for unlawful discrimination.

How long information is stored determines many future uses of the information, particularly for long-term tracking and pattern recognition. It may be of little note that a specific person was recorded, seemingly by coincidence only, near the scene of a crime, but what if that person was present at the scene of several similar crimes over the past year? Should the location records of individuals be subpoenaed in civil court cases such as divorces, or available to law enforcement agencies without search warrant?

3.2.3 Issue 4: What legal protection should a person's historical location information have against unreasonable search and seizure?

There are substantial legal frameworks controlling gathering and use of information on individuals. In the U. S., consumer credit laws allow consumers to examine and challenge the accuracy of credit information maintained about them by reporting agencies. Health privacy laws strictly control the security and disclosure requirements that hospitals and other health care providers must follow. Because location information spans these and other contexts, it may be necessary to consider additional privacy protections that are specifically location-related.

3.2.4 Issue 5: Should there be other controls governing aspects of stored location information, such as verifying accuracy, specifying retention periods, requiring particular levels of security, etc.?

There are many additional technical aspects relating to the security of location information, such as encryption. These information and communications security topics will be treated as outside the scope of the present research.

3.3 Usage issues

The use of location information in conjunction with the processing and communications power of today's computers and networks opens up an almost unbounded number of privacy issues. These begin with relatively simple systems such as the GPS in rental cars, which have stirred much controversy with their ability to detect speeding, unauthorized travel across state lines, etc. Usage issues and disclosure issues (the latter discussed in the next section) are often closely related, but may be distinguished by the extent to which information is shared with second or third parties. Independent operation of a stand-alone GPS unit shares location information with no other entity. Location of a cellular phone via triangulation from cell towers shares information between two parties—the device/user and the carrier. The carrier may offer a number of services to the user (navigation assistance, weather and traffic reports, etc.) and even retrieve information specific to that location from external third-party services, while still not revealing the user's location to any third party. We will deem any such scenarios where a user's individual location information is not revealed to a third party as usage issues.

We have emphasized devices such as cellular telephones to this point, largely because of their widespread deployment and early adoption of location technologies, but there are many other location-aware scenarios as well. For example, a vending machine recognizing a user's PDA using Bluetooth technology as it comes into range is a location aware application and has significant usage issues. Vending machine providers could store information about individual user purchasing patterns by locations and times, and use this information to personalize offerings to those users in the future. Other such non-carrier-based systems include information kiosks for tourists that can keep track of visitors' travels as they move about and request information from the kiosks [12].

3.3.1 Issue 6: Does the use of location information by a second party such as a communications carrier, even if not disclosed to third parties, create the potential for unfair advantage for those carriers or abusive use of the information by those carriers?

Although one of the first and most basic uses of location information is to associate located devices to users, there are several possibilities for this device/user mapping. Even with single-user devices (which presumably eliminate the problem of indeterminacy of association to an individual) users might be identified in several ways. They might be uniquely identified by name, or they might enjoy varying levels of anonymity. For example, a user might be identified only as:

1. A member of a group (e.g., a tour group visiting a resort).
2. A customer of a business (e.g., a Sprint customer rather than a Verizon customer).
3. A user that visited a location, facility, etc. on an earlier occasion (such as a repeat customer to a vending machine).
4. A pseudonym, chosen by the user to allow linking of related transactions, etc. without necessarily revealing the user's true name.

3.3.2 Issue 7: To what extent should users of location-enabled services be allowed to choose their own level of identifiability/anonymity?

3.4 Disclosure issues

Unlike usage issues discussed in the prior section, disclosure issues arise when individual identifiable location information about a user is shared with a third party such as an m-commerce provider. For example, cellular telephone providers, including AT&T Wireless and Sprint PCS, have been found sending user telephone numbers to web sites visited from Internet-enabled phones [8]. This level of personal information disclosure provides those web sites with significant advantages in tracking users. With the addition of location information, if it were to also be disclosed, significant privacy concerns would be created.

There are too many disclosure considerations to completely treat individually here, but an enumeration of some of those most important is possible. They include:

- Some level of disclosure may occur automatically and/or unavoidably as users access commonly-used services. For example, subscription-based wireless LAN "hot spot" services need to authenticate users for billing purposes, and will naturally associate users with particular wireless LAN locations.

- In some cases consent for disclosure may be implied, e.g., if your vehicle is equipped with the OnStar system and you are involved in an accident, your location information will be forwarded to emergency responders.
- Disclosure may arise as part of contractual arrangements between private parties, e.g., if a car rental agreement specifies that the vehicle is not to be taken across state lines and that its location will be monitored.
- Disclosure may be required by law, if for example a government agency mandates tracking of its own property and equipment (and, by implication, employees or others associated with that equipment).
- Disclosure will almost certainly occur in the marketplace unless prohibited or discouraged. Just as database marketing firms have offered for sale the phone numbers of virtually every resident in countries such as the U. S., it seems inevitable that location information will similarly be marketed.

3.4.1 Issue 8: What level of disclosure control should be dictated by government regulation? By the affected individual customers, users, etc.? By other parties?

Some of the above questions will be addressed in the next section.

4. Regulation

Regulation and control of location information may come from several sources. Many governments are now considering new privacy laws covering location information, and courts are extending existing legislation into related new areas. Non-governmental organizations such as standards bodies, industry/trade groups, and advocacy/public interest groups have become involved. Finally, the marketplace and consumer tastes and preferences may provide a controlling influence.

4.1 Governmental regulation

In the U. S., government regulation of location-aware mobile devices comes from extension of existing law and from new law [23]. Section 222 of the Communications Act of 1934 [5] requires that carriers use customer proprietary network information (CPNI) only for provisioning services requested by customers. The Wireless Communications and Public Safety Act of 1999 empowered the Federal Communications Commission (FCC) to deploy location-based enhanced 911 services but also

strengthened privacy by amending the definition of CPNI to include location information and prohibiting certain marketing uses of CPNI. A bill specifically addressing location privacy, the Location Privacy Protection Act of 2001 [15], which would have required customers of location-based services to give their informed consent for disclosure of location information, was referred to Senate committee but not passed into law. Despite an increasing number of governmental agency rulings and interpretations, bills introduced in congress, and court cases, location privacy law in the U.S. is still at a nascent stage.

Outside the U. S., the legal environment for location privacy varies. In Norway, the Personal Data Act [22] requires consent for processing sensitive data such as location data [27], although the English translation of the Act [22] does not include the term location. In Finland the Personal Information Law and Law about Privacy and Security of Telecommunications are said to have some applicability to location privacy even though “There are no laws in Finland that actually concern location information” [14]. Thus it appears that the legal status of location privacy is evolving in a number of countries.

4.1.1 Issue 9: What governmental legislation and regulation is appropriate to assure citizens’ rights of privacy in an era of location-aware mobile devices?

4.2 Standards-based regulation

Several standards bodies have become involved in location privacy. The Internet Engineering Task Force (IETF), the standards body most responsible for core Internet standards, has established the Geopriv working group mentioned earlier [7]. The group’s tasks include assessing requirements and recommending formats and protocols for exchange of privacy-related information, and in March 2003 it issued an Internet Draft [28]. It has also been proposed that the World Wide Web Consortium’s Platform for Privacy Preferences Project (P3P) might be extended to include privacy-related rules such as “No one may retain my location information for longer than one day” or “Business Acquaintance X can be told my specific location weekdays and my current city on weekends.” [20]

4.2.1 Issue 10: Will non-governmental, voluntary standards be sufficiently strong and sufficiently accepted by industry and consumers to be effective?

4.3 Industry/trade group regulation

Trade groups such as the Wireless Advertising Association are proposing guidelines for business practices in areas including consumer issues and privacy [21]. In general, these efforts are immature and have not been widely implemented.

4.3.1 Issue 11: Will industry/trade group standards be sufficiently strong and sufficiently accepted by industry and consumers to be effective?

4.4 Advocacy/public interest group regulation

Groups including the Electronic Privacy Information Center (EPIC, www.epic.org), the Center for Democracy and Technology (CDT, www.cdt.org), the Electronic Frontier Foundation (EFF, www.eff.org), and Privacy International (www.privacyinternational.org) have recognized location privacy issues and have begun acting in watchdog and advocacy roles. EPIC and CDT have submitted comments to the FCC [3] [24] urging further rulemaking to clarify and implement legislation and court rulings in these areas. They raise a number of issues such as the need for technology-neutral standards that can be applied across wide ranges of diverse products and services, and make the claim that strong rules are in the best interests of both consumers and the industry.

4.4.1 Issue 12: Will advocacy/public interest groups be capable of sufficiently monitoring the burgeoning location-aware industries, and sufficiently effective in protecting the public’s interests?

4.5 Marketplace regulation

Like other information technology vendors, suppliers of location-aware products and services commonly maintain privacy policies. The AT&T Wireless Policy [2], which is several thousand words in length, includes sections addressing what information AT&T collects, uses, and discloses about customers. It addresses release of personal information to comply with laws and court orders, to respond to emergencies, and to support various business needs. It also includes a section entitled “Presence, Location and Tracking” notifying users that their location is known whenever their devices are turned on and that location information will be provided to emergency responders—in some cases without user consent. Finally, it notes that optional services offered to customers may make further use of location information and will be governed by separate

policies. One of these optional services offered by AT&T Wireless, called “mMode Find Friends,” [18] allows groups of users to share their location information with2in the group. Customers are allowed to choose which other users are able to access their location information, and can turn off that particular service (but not location determination in general) with a “visible/invisible” control.

4.5.1 Issue 13: Will consumers demand, and will suppliers provide, privacy-related capabilities, features, and policies with their products and services that are sufficiently strong and accepted to be effective?

5. Summary and Conclusions

The addition of location-awareness capabilities to computing and communications devices will surely have profound business and societal impacts. In order to properly reap the many possible benefits, it will be necessary to carefully consider the privacy implications of the technology and provide the safeguards necessary to both protect rights of individuals and facilitate the orderly evolution of privacy-enabled products and services.

There may be few easy answers to the privacy questions raised by location-aware devices. No single control is likely to assure privacy. Not all uses of location information can be anticipated, and not all abuses can be prevented. Further research will be needed in many areas, including: (1) theories of location-based information and location-based privacy; (2) technical capabilities of location-awareness itself; (3) applications in the commercial marketplace, government sector, and elsewhere; (4) normative or prescriptive consumer/user rights and responsibilities; and (5) empirical research into consumer/user attitudes, concerns and preferences. By anticipating as many benefits and problems in advance as possible, we will best be able to guide the future of this important technology.

References

- [1] Altman, I. *The Environment and Social Behavior*. Monterey, CA: Brooks/Cole, 1975.
- [2] AT&T Wireless Policy. <http://www.attws.com/privacy>.
- [3] Comments of the Center for Democracy and Technology. (Submitted to the FCC as WT Docket No. 01-72, DA-01-696.) April 6, 2001. <http://cdt.org/privacy/issues/location/010406fcc.shtml>.
- [4] Chen, Guanling and Kotz, David. A Survey of Context-Aware Mobile Computing Research. Dartmouth Computer Science Technical Report TR2000-381.
- [5] Communications Act of 1934: As amended by the Telecommunications Act of 1996. <http://www.fcc.gov/Reports/1934new.pdf>.
- [6] Federal Communications Commission. Fact Sheet: E911 Phase II Decisions. http://www.fcc.gov/Bureaus/Wireless/News_Releases/2001/nw10127a.pdf.
- [7] Geographic Location/Privacy (geopriv) Charter. <http://www.ietf.org/html.charters/geopriv-charter.html>.
- [8] Ghosh, Anup and Swaminatha, Tara. Software Security and Privacy Risks in Mobile E-Commerce. *Communications of the ACM*, Vol. 44, No. 2, February 2001.
- [9] Harris Interactive. Harris Poll #17, March 19, 2003. http://www.harrisinteractive.com/harris_poll/index.asp?PID=365
- [10] Interagency GPS Executive Board. President Ends Selective Availability Effective Midnight on May 1, 2000. <http://www.igeb.gov/sa/>.
- [11] Jana, Rittwik et al. Location Based Services in a Wireless WAN Using Cellular Digital Packet Data (CDPD). *MobiDE 2001*, ACM, 2001.
- [12] Kubach, Uwe and Rothermel, Kurt. Exploiting Location Information for Infostation-Based Hoarding. *ACM SIGMOBILE*, July 2001, Rome Italy.
- [13] Lai, Jin and Miyazawa, Tatsuo. MRM Server: A Context-Aware and Location-Based Mobile E-Commerce Server. *International Conference on Mobile Computing and Networking*. New York, ACM Press, 2002.
- [14] Levijoki, Sami. Privacy vs Location Awareness. http://www.hut.fi/~slevijok/privacy_vs_locationawareness.htm.
- [15] Location Privacy Protection Act of 2001. Accessed through title search at <http://thomas.loc.gov>.
- [16] Margulis, S. T., Conceptions of Privacy: Current Status and Next Steps. *Journal of Social Issues*, Vol. 33, No. 3 (1977), pp. 5-21.
- [17] Margulis, S. T., Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues*, Vol. 59, No. 2 (2003), pp. 243-261.
- [18] mMode Features. <http://www.attws.com/mmode/features/findit/FindFriends/QA.jhtml>.
- [19] Mobileinfo.com. Location-Based Services. <http://www.mobileinfo.com/LocationBasedServices/>.

[20] Morris, John. Position Paper on “P3P and the Privacy of Location Information.” W3C Workshop on the Future of P3P. <http://www.w3.org/2002/p3p-ws/pp/cdt2.pdf>.

[21] Nelson, Ruth. Do You Know My Location? Privacy, E-Personalization, and the Smart Phone. Pricewaterhouse Coopers, 2001. <http://www.pwcglobal.com>.

[22] Norwegian Parliament. “Act of 14, April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act).” http://www.personvern.uio.no/regler/peol_engelsk.pdf.

[23] O’Connor, Mark. Privacy Laws and Wireless Location Services: Does the Law Let You Do That? Presentation to Internet World Wireless, February 22, 2001. http://www.l-olaw.com/Publications/wireless_location_services.pdf.

[24] EPIC, Reply Comments of Electronic Privacy Information Center. http://www.epic.org/privacy/wireless/epic_reply.pdf

[25] Savvides, Andreas et al. Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors. *ACM SIGMOBILE*, July 2001, Rome, Italy.

[26] Sheehan, Kim. Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, Vol. 18, 2002, pp. 21-32.

[27] Snekkenes, Einar. Concepts for Personal Location Privacy Policies. ACM: EC’01, Tampa Florida, October 2001, pp. 48-57.

[28] The Internet Society. Geopriv Requirements. March 2003. <http://www.ietf.org/internet-drafts/draft-ietf-geopriv-reqs-03.txt>.

[29] Thomas, Michael. Privacy Issues in Location-Aware Mobile Devices. Unpublished draft in partial fulfillment of MIS 597, Directed Research, Boise State University, Spring 2002 (Supervised by Dr. Robert Minch).

[30] Wang, Huaqing et al. Consumer Privacy Concerns about Internet Marketing. *Communications of the ACM*, Vol. 41, No. 3 (March 1998), pp. 63-70.

[31] Westin, A. *Privacy and Freedom*. New York: Atheneum, 1967.