Supporting Location Information Privacy in Mobile Devices

Deveeshree Nayak[1], M. Venkata Swamy[2], and Srini Ramaswamy[3]

[1] KIIT University
Bhubaneswar, India
deveeshree@gmail.com
[2] University of Arkansas at Little Rock
AR, USA
vxmartha@ualr.edu
[3] Industrial Software Systems
ABB India Corporate Research Center
srini@ieee.org

Abstract. Social networking has evolved as a basic amenity in today's interconnected world. Users of social media tools do not always keep up with privacy policies and its adverse effects. It is very common that even experienced users are often caught unaware of actions that happen behind the interface screens of their interconnection devices. Many-a-time mobile application developers take advantage of such user complacency and leak location information from the device (and hence information about the user) to other applications. Though there has been considerable alerts raised on the issue of location information leakage, there are situations wherein applications sneak through these 'walls' and connect with devices / applications to extract / query desired information from the firmware. In this work, we provide a in-depth review of literature on this emerging area of social interest, and propose a four-layer context-based authentication framework (4-CBAF) to address location privacy concerns. The 4-CBAF framework provides a facility for users to share pertinent information only if the user specifically authorizes such information sharing. The 4-CBAF is intelligent enough to reduce the number of human interventions that a user should attend to. The effectiveness of the proposed 4-CBAF is also demonstrated for check-in application for Facebook using smart devices.

Keywords: Location, Privacy, multi-level authentication, Context, Mobile.

1 Introduction

Today's sophisticated mobile technologies makes modern civilization to realize the world as a small and intensely interactive entity. An individual's geographical location at a point in time is thus by-and-large easily accessible. The major disadvantage with the adoption of such technology is the unpredictable and inadvertent disclosure of private information; in this work we are concerned with location disclosure. Privacy leakage and discovery of personalized data poses a major threat to users by

C. Hota and P.K. Srimani (Eds.): ICDCIT 2013, LNCS 7753, pp. 361–372, 2013.

allowing the use of the referring mobile device as a location tracker. In [11], the authors identify thirteen major issues related to this technical approach. Location based tracking systems use various techniques to keep track of location information of users which in turn increases the risk on the misuse of private and secure information of individuals [12]. In addition to tracking individual location, estimation of location also may create severe privacy risks such that all comprehensive available records of location data produce nearly accurate predictions about the user [13]. There are techniques to assemble public information to produce private information though the private variable is not explicitly leaked to intruder. Information flow models attempted to address these issues in such cases.

Despite economic downturns, the advances and proliferation of mobile devices has continued to be on the rise, and is one of the most pervasive consumer electronic devices to expand unsurpassed global penetration during the past decade. Global Positioning System (GPS) have matured as a standard for smart mobile devices. Advances in mobile computing technology have enabled users to adopt location based services (LBSs) for routine activities. Individuals and organizations are leveraging location information for heuristics and investigative analysis [3]. LBSs through its accompanying suite of tools have attracted customers and hence become very popular within a short time. Some of the LBSs include Google Latitude, FindMyFriends, GeoMe, CouponApp, etc.

In general, LBS applications accumulate location information for an arbitrarily long time to provide attractive services to their users. However, they raise doubts in the user's mind about the exact nature and limitations of their individual privacy. It is not that every time a user may wish to divulge her/his location information to these applications or other individuals. The key problem hence is to provide support for occasional location information disclosure while also supporting contextual blocking of tracking users continuously [2]. These problems have led to several studies about privacy of location in mobile devices. Policies indicate that device manufacturers should design devices to support privacy-enabling and provide user-based control to individuals for selective sharing of location information. The study recommends mobile operating system providers to include necessary tools for privacy protection. Upon complaints from customers and legal recommendation from federal governments, all the mobile OSs allow users to select applications to access location data (eg. GPS). Selective access to applications is often sufficient in many instances. However, such technology is not yet clearly capable of contextual selection of access grants for applications that interact with these selective applications due to an open API structure for add-on applications development. In this paper, we propose a framework to incorporate a 4-layer context based authentication framework (4-CBAF) to address such elevated concerns in mobile environments.

The proposed 4-CBAF introduces a component that authenticates and authorizes requests from applications to access location information. The 4-CBAF component inherits properties from layered authentication proposed in [10]. The primary objective of the component is to authorize location information access. The layered approach distinguishes functionality of authentication, authorization and context based authorization in achieving the purpose. Each layer serves a distinct purpose and in all they verify "who are you, what you know, what you have, what is the purpose". The privacy components 4-CBAF not only verifies the requesting application validity but also verifies whether the application is legal to access location information at the given context. The decisions are based on policies devised in the component. The policies are

dynamic and can be updated upon demand. This paper discusses the feasibility of the 4-CBAF framework in mobile devices. The outcomes of our exploratory study are the following:

- Identify privacy leakage of location information in mobile device applications
- Proposed a component architecture, 4-CBAF, to address the privacy issue
- Demonstrate that the improvements differ from current state-of-art technologies in accessing location information
- Discuss the feasibility of the proposed solution in real-time check-in application for Facebook in mobile devices.

The rest of the paper is organized as following. Related work is discussed in Section II. Existing location information privacy tools are discussed in Section III, and the proposed 4-CBAF component is illustrated in Section IV. Its feasibility in real-time application usage in presented in Section V, which is followed by conclusions and future work in Section 6.

2 Related Work

Several researchers have argued that when the collection of location information can cause a violation of privacy, suggested consent is necessary [30]. Users who share their location information often realize late that it may have impact on sensitivities within their culture and society [14]. There are tools to ease the sharing, such as GTWhois [15] and Visual Route [16], from where an intruder can collect users' location information such as IP address, email address and ISP. Although these variables cannot be used to derive accurate geographical location, one can predict the user's city and street. The US Privacy Act of 1974 [17] identifies an individual's right to privacy of her/his personal information. But location privacy is not included within this law. Several laws [18-21] have been passed to protect location privacy which necessitated a user's approval to broadcast his/her location data. It has been mentioned that a user's physical location cannot be disclosed publically because of privacy risks. Simultaneously, the European Union has approved a law - The Directive on privacy and electronic communications [22] – also known as the E-privacy Directive, which deals with the security, confidentiality and integrity of location information, user's opinion and user's personal information. Until now, however, there are no specific laws to check privacy leaks in applications utilizing location tracking system (LTS) [23]. The copious use of LTS applications in mobile devices has increased privacy risks for individuals. Research in [24-29] showed how a location tracking system is a threat to users in their day-to-day life. By monitoring the location of an individual, intruders integrate the recorded data to build his/her profile which violate fundamental rights of a user [29]. Motivated by these laws and studies, the objective of our work is to study and propose the development of a software check-pointing framework / mechanism to ensure privacy preservation while using location based services.

The increase in availability of information coupled with increased computing power in GPS-enabled smart devices makes it possible to deploy context sensitive services where the access of the resources is determined by a user's contextual need. The location of a user allows for establishing context and motive through data mining and hence poses an increasing threat to the individuals' privacy [31]. In LBSs, the requested resources are available to an individual only if the individual is at specified location [32]. LBSs are uncomplicated context based privacy implementations but pose a security threat by leaking individual's whereabouts without the users' explicit knowledge. The notion of privacy also diverges between countries and cultures [33-36]; for example between the US and India, where India is an example of a joint society and USA is an example of idiosyncratic civilization [37]. In India, while privacy concerns are relatively low compared to US [36], physical and societal threats by blatant privacy violations pose an immense threat; this is due to ignorance and unavailability of legal and structural recourse for such violations. Hence despite cultural differences, there are situations where privacy plays critical role in an individual's life. Therefore, LBS users have the right to take decision on their privacy while being served by LBSs. End users, irrespective of culture, often commonly find it objectionable for LBSs to advertise information about an individual [38]. Most individuals will strongly object to the leak of personal information without user's knowledge [39]. Literature asserts that a professed control, over revelation and subsequent use of personal information, plays an important role in a individuals' seclusion concerns and information disclosure performance [40]. Thus there is an urgent need for strong authentication and authorization techniques for privacy in LBSs [41].

GPS technology is often piggy backed with Navigation and Tracking services (NTs) to track and monitor a mobile user's geographical position. Ethical conflicts arise in tracking an individual who has right not to be monitored. There are unanswered questions by assumed consent – that attacks the core of an individuals' privacy [42].The work of Dobson and Fischer [44], Garfinkel et al. [44], Michael and Michael [45], Perusco and Michael [46], Kaupins and Minch [47], Perakslis and Wolk [48] and Stajano [49] have pointed out the need for a deeper understanding of moral principles in widespread use of LBSs. Tools such as Google Earth [50], NASA WorldWind [51], Microsoft VirtualEarth [52], and Skyline Globe [53], etc. generally provide GPS data of the user; which is often not desirable to end users who assume their privacy rights are protected. With the help of Google Earth like tools, an antagonist can pinpoint nearly the exact location of an individual by disregarding the privacy laws [54].

3 LBS Support Frameworks

3.1 Current State-of-Art

Until recently mobile operating systems did not have checks for authentication of applications for accessing location data. The mobile OSs now include a tool to allow/block an application to gain access to location data. A reference model for location privacy in mobile devices is LORE. LORE is an infrastructural design to support

location aware applications. A method is proposed to publish a fake location to hide an individual's location information [4]. Dissemination of location information from identity protects one's privacy from dissuading monitoring of an individual by reconstructing path of an individual's track [5]. Identifying a range of queries and assigning an artificial id to protect privacy of an individual can address privacy in traffic monitoring systems [6]. A unified framework is developed using anonymity techniques, by hiding, often by obfuscation [8]. By taking various dimensions of attacks and location information into account, in [7] the authors developed a method to quantify location privacy.

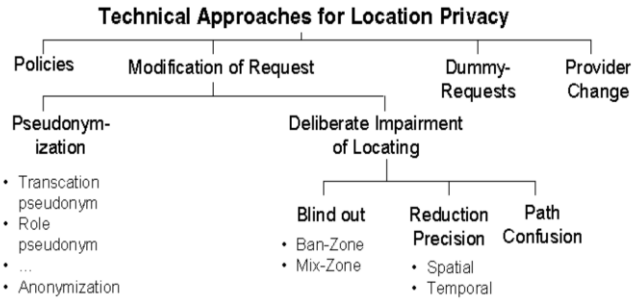

Fig. 1. CurrentTechnologies for Location Privacy [8]

As shown in Figure 1, most of the studies thus far have focused on techniques such as modification, faking, etc., but do not discuss policies to authenticate a request to grant access to location data selectively while providing privacy. Our work focuses on developing a framework based upon a multi-layered authentication mechanism using context based techniques (ex. is the request trustable), authentication techniques (who are you), and authorization techniques (what you want). In other words, our work attempts to address privacy issues by developing an appropriate encompassing framework to deploy privacy policies. The dearth of research in this area can be discerned by the 'policies' leaf in Figure 1; this area is currently critically ill-defined and often left to the mobile application developers and providers for interpretation.

3.2 Problem Definition

LBS have been evolving at a rapid pace to exploit location information availability so as to support effective customer services. However, as in every race in the market-driven world, that attempts to meet customer demand for information, often times, customers themselves are 'put' in a position of disadvantage by not knowing exactly how much privacy is being lost by such intrusive applications over time. Mobile application service providers retrieve location coordinates with the intent of providing value-added services. There are many instances where the service providers leak location information directly or indirectly using inferences. For example, in restaurant rating services, wherein a user rates a restaurant when she / he visits a restaurant is

allowing for crowd sourcing to publish about food quality and ambience. The service provider is not publishing the location of the user directly but the application execution context could infer that the user was at the restaurant. If one assumes that employers of this user may monitor their employees' activities using third party services, and that the user may not want such information broadcast at all times, this could become an inadvertent privacy invasion scenario. Though there are tools to block a service provider access to location information, they do block the service provider themselves, as user are often left with an option to either share information all the time, or never at all. Such examples create the necessity for more fine-grained authorization of requests to location information besides authentication of service provider themselves. Alternately, the problem can framed as implicit "privacy depravation" - through a distinct lack of authorization mechanisms that curtail the sharing of private information based on certain contexts. Hence authentication of the requestor by default deprives the user of their right to privacy – i.e. by installation of the restaurant rating service – where the user may rightly be a user wanting to know / publish about 'good' restaurants during *some* times – but not essentially share such information about their visits to one of these restaurants *all* the time. But the application installed on their mobile device does not differentiate this in any significant manner. In this context, it is good to recall that while authentication verifies the identity of service provider, authorization verifies the service provider has rights to access to the requested information.

4 4-Layer Context Based Authentication Framework (4-CBAF)

Mobile operating systems are developed through a model driven engineering process. There are primarily three layers in these operating systems. One is the Core OS layer which interacts with the firmware, other is Core Services which talks to Core OS layer to provide services to higher layer, and the remaining layer is applications which includes media, touch, and third party applications. Figure 2 shows the architecture of one such mobile OS, the iOS.

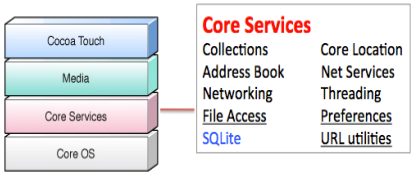

Fig. 2. iOS Architecture

The Core Services layer implements location services by communicating with the Core OS API. In this paper we term location services as Navigation and Tracking Services (NT services); one of the core services in mobile operating systems. NT service components do not take privacy into account while providing services. The primary goal of NT services is to provide location based services to applications. Hence the current architecture of such systems is incapable of protecting users from privacy leakages. These limitations have motivated us to introduce a layered framework for authentication and authorization of service requests. The proposed layer for protecting privacy is presented in Figure 3. Partner and 3rd Party NT API and core NT API are shielded by a

privacy protection layer called 4-layer Context Based Authentication Framework (4-CBAF) component. The 4-CBAF components analyses a given service request from third party application through a 4-level of authentication and authorization techniques. The component is illustrated in detail in the following.

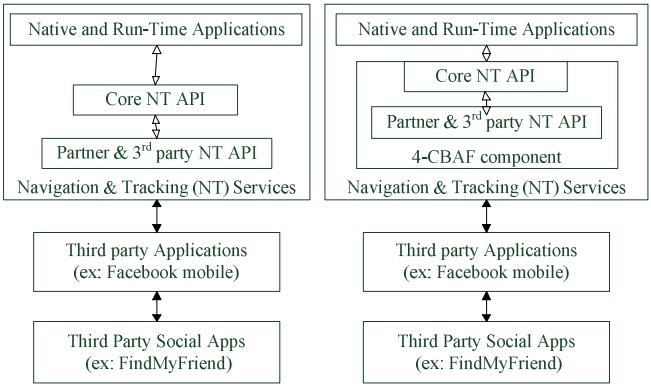

Fig. 3. Original and Proposed Mobile API architecture

The 4-CBAF component is developed from the lessons learned from our earlier work [10], which suggests that we need to employ a multi-layered approach to prevent one-stop defaults for authorization requests. Given the need for such authorization mechanisms by applications, we adapt a four-layer framework for authorization. Each of the 4-layers serves distinct actions to validate and authorize a request. The design of the four layers is presented in Figure 4.

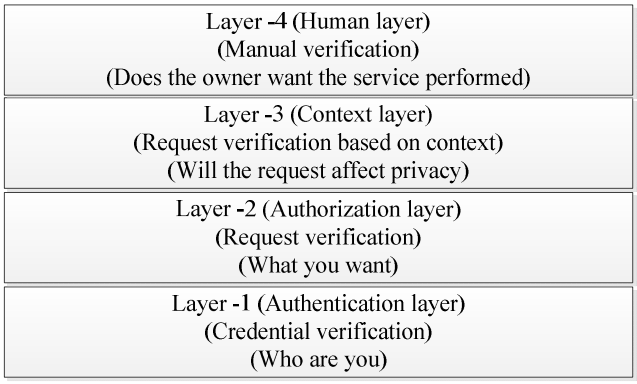

Fig. 4. Proposed 4-CBAF framework

Layer 1 is naïve which is simple authentication mechanism to identify a requestor. In simple words, the layer-1 authenticates the requestor irrespective of whether the requestor authorized for the requested service or not. Layer-1 could be password

based authentication (PAP or CHAP) or key based. The primary purpose of layer-1 is to verify the requestor's credentials and to identify requestor i.e. who is the requestor. If Layer-1 passes the authentication check, then Layer-2 is invoked for the authorization of the requestor's request. Layer-2 verifies whether the requestor is legal to access the service. The layer-2 follows rule-based authorization technique and the owner of the device defines the rules. With effect from complaints from user community, mobile operating systems now include this feature i.e. to block an application from accessing location API.

If successful at Layer-2, then Layer-2 sends the request to Layer-3 for context-based authorization. The layer-3 verifies whether the service at the given context is legal or not. This layer requires more information from the requestor regarding the purpose of the service request. If the purpose is valid, layer-3 passes the request and the service is granted. Otherwise, the request is sent to owner of the device for manual verification. In the exceptional case that Layer-3 fails, the request is forwarded to Layer-4 which triggers human intervention to take manual action. This proposed layered architecture provides fine grained authorization mechanisms and each layers service a distinct and critical purpose. Table 1 summarizes the improvements of the proposed 4-CBAF architecture over current architecture.

Table 1. Improvements over current architecture

Layers	Current	4-CBAF
1. Authentication	Not implemented	PAP, CHAP, or key based
2. Authorization	Implemented	Rule based
3. Context Authorization	Not implemented	History, knowledge based
4. Manual Verification	Not implemented	Available, but may not be needed

The purpose of each layer can be demonstrated in a real time scenario as discussed in the following section.

5 Case Study

A social networking service is an online service platform that focuses on facilitating the building of social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. Facebook is one of the most popular social networking platforms and has been migrating on to smart devices at a rapid acceleration. Facebook provides a platform called wall on which a user posts his/her announcements. There are many facebook applications and mobile applications that automate the posting for users' providing ease of access. These applications access device services to generate information for such posts. Smart devices include features such as GPS, gyroscope, etc. GPS is one of the most useful and controversial feature

in smart devices. GPS locates the position of a device and mobile OSs provide core NT API to upper layers of the OS. To expose the privacy threats with the existing architecture, consider an application for check-in feature. The check-in application takes location information from device and friends' names that are with the user at the specific time and posts that information on the user's Facebook wall as a check-in message.

Now assume a user say 'A' and the set of users that are family and friends of 'A' is F(A). 'A' is visiting a restaurant with some his/her family and friends i.e. with a set of users R (A) <F(A). In this scenario, check-in application reads the location information from device which is the restaurant and list of users who are along with 'A' i.e. R(A) and posts a message on 'A's wall. This is visible to all the friends of 'A' that include F(A)-R(A). This kind of posts without user's consciousness, can cause social problems and originate unpleasant relationship issues. This might lead to break-ups at some point of time. Table 2 describes how the post is authorized in original OS architecture and in proposed 4-CBAF based architecture.

Table 2. Check-in application authorization

Layer	Current	4-CBAF
1. Application authentication	Not implemented	Successful
2. GPS service authorization	Successful	Successful
3. Context based authorization	Not implemented	Failed
4. Manual Verification	Not implemented	Implemented but not needed

From the Table 2, the check-in application generated message is posted on facebook wall upon authorization from GPs module for the application in original OS framework. In proposed 4-CBAF, the application is a legitimate requestor and legal to access GPS service but raise privacy concerns in given context and thus failed in layer-3. Therefore, the proposed architecture can address privacy issues in cases where current architecture does not support.

Another popular such social networking service such as micro-blogging activity is Twitter. Assume an application say tweetMyGeo which tweets all your geo-local positions time to time periodically. It is very usual that a mobile user, who downloads this application, relegates his/her twitter login credentials keeping trust on the application. There is a privacy check service neither on the twitter side nor in mobile device side. The 4-CBAF comes to rescue approach can support such users by providing a check point to such applications. The proposed models will blocks applications such as tweetMyGeo from obtaining GPS location of the mobile device through its 3rd Llayer-3. Context based authorization fails because it learned from history that the application broadcasts location information through twitter.

6 Conclusion

Social networking has been evolving as a basic amenity in today's world. Users of such social media tools do not always keep up with privacy policies and its adverse effects on its users. It is very common that users are caught unaware of the actions by applications installed on their devices. In this work, we have proposed and demonstrated the need and use of a four layer context-based authentication framework (4-CBAF) to address privacy concerns. The 4-CBAF framework provides facility to warn a user not to share sensitive information such as location and to share if the user insists to do so. The 4-CBAF is intelligent enough to reduce number of human interventions that a user should attend. Location information is a case and the 4-CBAF can be realized in privacy critical systems. The effectiveness of the proposed 4-CBAF is demonstrated for check-in application for Facebook in smart devices. Our next step is to implement the 4-CBAF in mobile devices.

References

1. Chen, Y., Liu, D.: Location-Aware Services and its Infrastructure Support. In: Enabling Technologies for Wireless E-Business, pp. 312–334. Springer, Heidelberg (2006)
2. Weiser, M.: Some Computer Science Issues in Ubiquitous Computing. Communications of the ACM 6(7), 75–84 (1993)
3. Harter, A., Hopper, A.: A distributed location system for the active office. IEEE Network 8(1), 62–70 (1994)
4. Chang, W., Wu, J., Tan, C.C.: Enhancing Mobile Social Network Privacy. In: IEEE Global Telecommunications Conference (GLOBECOM 2011), December 5-9, pp. 1–5 (2011)
5. Hoh, B., Gruteser, M., Xiong, H., Alrabady, A.: Enhancing Security and Privacy in Traffic-Monitoring Systems. IEEE Pervasive Computing 5(4), 38–46 (2006)
6. Xie, H., Kulik, L., Tanin, E.: Privacy-Aware Traffic Monitoring. IEEE Transactions on Intelligent Transportation Systems 11(1), 61–70 (2010)
7. Shokri, R., Theodorakopoulos, G., Le Boudec, J., Hubaux, J.: Quantifying Location Privacy. In: IEEE Security and Privacy (SP), May 22-25, pp. 247–262 (2011)
8. Shokri, R., Freudiger, J., Hubaux, J.-P.: A unified framework for location privacy. In: 3rd Hot Topics in Privacy Enhancing Technologies, HotPETs (2010)
9. Decker, M.: Location Privacy-An Overview. In: 7th International Conference on Mobile Business, ICMB 2008, pp.221–230, July 7-8 (2008)
10. Nayak, D., Ramaswamy, S.: A Multi-level Contextualization Framework for Authentication in Mobile Payment Applications. In: 11th International Conference on Wireless Networks (ICWN 2012), USA, July 16-19 (2012)
11. Minch, R.P.: Privacy Issues in Location –Aware mobile devices. In: 37th Hawaii International Conference on System Sciences, Big Island, HI, USA. IEEE Computer Society (2004) ISBN 0-7695-2056-1
12. Wang, J.I., Loui, M.C.: Privacy and Ethical issues in location–Based Tracking systems. In: Proc. of the 2009 IEEE International Symposium on Technology and Society, Wasington DC, USA (2009)
13. Bowen III, C.L., Martin, T.L.: A survey of Location privacy and an Approach for SolitaryUsers. In: 40th Hawaii Intnl. Conf. on System Sciences, Big Island, Hawaii (2007) ISBN 0-7695-2755-8

14. Zhu, C., Wat, K.K., et al.: Privacy and Social Effects in Location Sharing Services. In: Proceeding of 2012 IEEE First International Conference on Services Economics, Hawaii,USA, June 24-29 (2012)
15. GeekTools, "GTWhois," Centergate Research Group, LLC (2003)
16. VisualRoute, "VisualRoute 2006 Personal Edition," Visualware, Inc. (2006)
17. The Communications Act of 1934, 47 U.S.C(151-614), Public Law 416 (1934)
18. The Location Privacy Protection Act of 2001 (2001)
19. The Wireless Privacy Protection Act of 2003 (2003)
20. The Wireless Privacy Protection Act of 2005 (2005)
21. The Wireless 411 Privacy Act (2005)
22. European Union Directive on Privacy and Electronic Communications (2002)
23. Dowdell, E.M.: You are here! Mapping the boundaries of the Fourth Amendment with GPS technology. Rutgers Computer and Technology Law Journal 32(1), 109–139 (2005)
24. Lockton, V., Rosenberg, R.S.: RFID: the next serious threat to privacy. Ethics and Info. Tech. 7(4), 221–231 (2005)
25. Michael, M.G., Fusco, S.J., Michael, K.: A research note on ethics in the emerging age of uberveillance (überveillance). Computer Communications 31(6), 1192–1199 (2008)
26. Perusco, L., Michael, K.: Control, trust, privacy, and security: evaluating location-based services. IEEE Technologyand Society Magazine 26(1), 4–16 (2007)
27. Peslak, A.R.: An ethical exploration of privacy and radio frequency identification. Jour. of Business Ethics 59(4), 327–345 (2005)
28. Wasieleski, D.M., Gal-Or, M.: An enquiry into the ethical efficacy of the use of radio frequency identification technology. Ethics and Information Technology 10(1), 27–40 (2008)
29. Lin, D., Loui, M.C.: Taking the byte out of cookies: privacy, consent, and the Web. Computers and Society 28(2), 39–51 (1998)
30. Lin, D., Loui, M.C.: Taking the byte out of cookies: privacy, consent, and the Web. Computers and Society 28(2), 39–51 (1998)
31. Hengather, U., Steenkiste, P.: Avoiding privacy violation caused by context –sensitive services. In: Forth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM 2006), March 13-17, p. 233 (2006)
32. Myles, G., Friday, A., Davies, N.: Preserving Privacy in Environments with Location-Based Applications. IEEE Pervasive Computing 2(1), 56–64 (2003)
33. Xu, H., Gupta, S., et al.: Effectiveness of privacy Assurances Approaches In Location-Based Services:A Study of India and United States. In: Proceeding of Eighth International Conference on Mobile Business (2009)
34. Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., Colautti, C.: Internet users' privacy concerns and beliefs about governmentsurveillance: An exploratory study of differences between Italy and the United States. Journal of Global Information Management 14(4), 57–93 (2006)
35. Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., Colautti, C.: Privacy Calculus Model in E-commerce - a Study of Italy and the United States. European Journal of Information Systems 15(4), 389–402 (2006)
36. Kumaraguru, P., Cranor, L.: Privacy in India: Attitudes and Awareness. In: Danezis, G., Martin, D. (eds.) PET 2005. LNCS, vol. 3856, pp. 243–258. Springer, Heidelberg (2006)
37. Milberg, S.J.B., Smith, J.S.H.J., Kallman, A.E.: Values, Personal Information Privacy Concerns, and Regulatory Approaches. Comm. of the ACM 38(12), 65–74 (1995)
38. Nowak, G.J., Phelps, J.: Understanding Privacy Concerns: An Assessment of Consumers's Information-Related Knowledge and Beliefs. Journal of Direct Marketing 6(4), 28–39 (1992)

39. Wang, P.: Information-Systems Solutions for Transborder Data Flow Problems for Multinational Companies. International Journal of Information Management 13(1), 29–40 (1993)
40. Margulis, S.T.: On the Status and Contribution of Westin's and Altman's Theories of Privacy. Jour. of Social Issues 59(2), 411–429 (2003)
41. Bertino, E., Kirkpatrick, M.: Location-Aware Authentication and Access Control-Concepts and Issues. In: International Conference on Advanced Information Networking and Aplications(AINA), May 26-29. University of Bradford, Bradford, UK (2009)
42. Michael, K., McNamee, A., Michael, M.G.: The Emerging Ethics of Humancentric GPS Tracking and Monitoring. In: Proc. of the International Conference on Mobile Business (ICMB 2006), Copenhagen, Denmark, June 26-27. IEEE Computer Society (2006) ISBN 0-7695-2595-4
43. Dobson, J.E., Fisher, P.F.: Geoslavery. IEEE Technology and Society Magazine 22(1), 47–52 (2003)
44. Garfinkel, S.L., et al.: RFID Privacy: An Overview of Problem and Proposed Solutions. IEEE Securityand Privacy Mag. 3(3), 38–43 (2005)
45. Michael, K., Michael, M.G.: Microchipping People: the Rise of the Electrophorus. Quadrant, 22–33 (March 2005)
46. Perusco, L., Michael, K.: Humancentric Applications of Precise Location-Based Services. In: IEEE Conference on e-Business Engineering, pp. 409–418. IEEE Computer Society, Beijing (2005)
47. Kaupins, G., Minch, R.: Legal and Ethical Implications of Employee Location Monitoring. In: 38th Hawaii Intnl. Conf. on System Sciences (2005), http://csdl2.computer.org/comp/proceedings/hicss/2005/2268/05/22680133a.pdf
48. Perakslis, C., Wolk, R.: Social Acceptance of RFID as a Biometric Security Method. In: Proceedings of the IEEE Symposium on Technology and Society, pp. 79–87 (2005)
49. Stajano, F.: Viewpoint: RFID Is X-ray Vision. Communications of the ACM 48(9), 31–33 (2005)
50. Google Earth, http://earth.google.com/
51. NASA World Wind, http://worldwind.arc.nasa.gov/
52. Microsoft Virtual Earth, http://www.microsoft.com/virtualearth/
53. Skyline Globe, http://www.skylinesoft.com/
54. Fleet, G.J., Williamson, M.: Research data in Google Earth: how do we protect privacy and meet ethical obligations? In: Proceeding World Congress on Privacy, Delta Brunswick, Saint John, New Brunswick, Canada, August 25-27 (2009)