Privacy in LBS: Dilemma *vs* Realities

Nitin Kulkarni[#1], Narendra S. Chaudhari[*2], Sanjay Tanwani[**3]

[#]*Department of Computer Application, Acropolis Institute of Technology & Research, Indore, India*
[*]*Discipline of Computer Science & Engineering, Indian Institute of Technology, Indore, India*
[**]*School of Computer Science & IT, Devi Ahilya Vishwavidyalaya, Indore, India*

[1]nitin.kul@gmail.com
[2]nsc0183@gmail.com
[3]sanjay_tanwani@hotmail.com

Abstract **- In this information age, with ubiquitous computing we leave trail of our digital usage everywhere, putting privacy at stake. Privacy preserving is beyond doubt an identified priority today and multiple research initiatives have been undertaken to address it. However, the casual attitude of users and providers in handling the information revealed during the use of Location Based Services (LBS) raises a serious concern over privacy. The existing approaches to preserve privacy seem inadequate. In this paper, the core concerns regarding LBS privacy, possible attacks and the effectiveness of approaches are addressed. Finally, open challenges that need immediate attention in the given domain are discussed.**

Keywords **- Location Based Services, LBS privacy, Attacks, Privacy protection, Location Privacy.**

I. Location Based Services (LBS)

Location Based Services (LBS) are the class of applications that amalgamates physical location of the target entity to provide *value-added services* and *dynamic client experience*. LBS is revolutionizing how people interact-with and experience their surroundings (Table 1).

TABLE 1
SOME OF THE POPULAR AREAS OF APPLICATION FOR LOCATION BASED SERVICES.

Application area	**Popular examples**
Emergency/ Safety	Public safety and medical services
Information services	News updates & weather forecasts
Tracking services	Logistics, road conditions, resources, devices
Entertainment services	Gaming, Dating services
Social Networking	Facebook, Instagram, Twitter
Business	Advertisements, Billing
Travelling / Navigation	Route assistance & Navigation

Changing lifestyle, demand for autonomy and desire to be networked on-the-move with pervasive mobile technology in a backdrop of an accelerated pace of miniaturization, use of global positioning system (GPS) and rapid commercialization of mobile devices, has led to proliferation of LBS.

II. LBS Privacy Concerns

The benefits of using LBS cannot be ruled out, however, information revealed while using these services via a typical LBS ecosystem [1][2] that has multiple technological elements collaborating seamlessly (Fig 1) to augment human life experiences; calls for a systematic review and more concentrated look over privacy concerns while using these services.

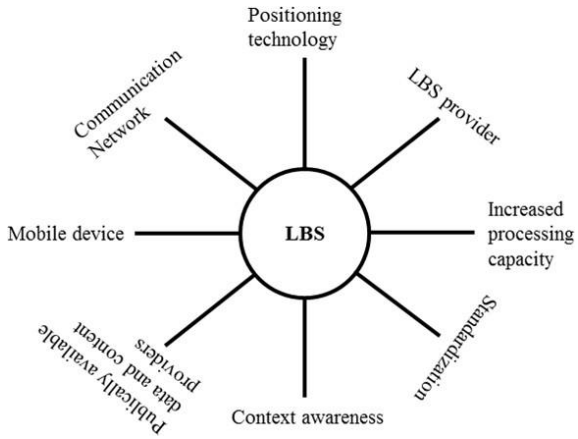

Fig. 1 Inter-operating components of LBS ecosystem

Privacy threats to LBS privacy may come from varied attacks at different levels [2][3] (Table 2) –

TABLE 2
TYPES OF ATTACKS IN LBS

Type of attack	**Description**
First-hand communication (**Level 01**)	Compromised mobile device
Trust breach (**Level 02**)	Information is relayed from an authorized to a malicious party intentionally
Observation attacks (**Level 03**)	Adversary observes and tracks its target user
Inference /analytical attacks (**Level 04**)	Combining collected facts from different data sources to draw inferences about the target

Moreover, the level of privacy and benefits (and/or risks) associated with the casual or continual use of an LBS application by the user is affected by (1) his/her *understanding about privacy* and (2) *awareness/consent about the information collected* i.e. whether the information is gathered *knowingly*/*un-knowingly* and if it is shared by him *mandatorily* or by *choice* (Table 3) [4]

TABLE 3
TYPES OF USERS FOR AN LBS APPLICATION

Users	**Understanding about privacy risks**	**Approach towards sharing information**
Naïve user (**NU**)	Low	Casual
Competent user (**CU**)	Intermediate	Thoughtful
Mandatory user (**MU**)	Not applicable	Not applicable

Mandatory user (mostly the case of government applications) seems to have no choice (by law) however; the other two can control (in a theoretic sense) information dissemination.

TABLE 4
LBS USER VULNERABILITY FOR ATTACKS
(NA STANDS FOR NOT ACCESSIBLE)

Type of attack	**NU**	**CU**	**MU**
First-hand communication (**Level 01**)	High	Medium	NA
Trust breach (**Level 02**)	High	High	NA
Observation attacks (**Level 03**)	High	High	NA
Inference /analytical attacks (**Level 04**)	High	High	NA

Privacy is a perception of the user. However, we can still draw following conclusions -

a. Lack of awareness of naïve users (**NU**) makes them the soft targets.
b. Competent user (**CU**) is aware and hence the risk varies with his/her alertness level while revealing the information.
c. Mandatory user (**MU**) has to trust the agency.

Assuming, the information is collected knowingly and choicely, CU can secure his/her device (against Level 1 attacks) and limit or intelligently share information (against Level 3 & 4 attacks), for Level 2 attacks the trust in information aggregator is ultimate. For MU with no choice and control, the privacy risks at all levels is directly proportional to the trust and security levels of the agency (on behalf of trusted party like government) holding the information.

So, LBSs are double edged sword, it has potential to enrich life while risking the privacy of its end users.

III. Privacy Dilemma

LBS user faces a trade-off, whether or not to use LBS. However, benefits of LBS demands risking privacy. The two extreme choices with use of LBS are –

a. Get convenience, forget privacy, or,
b. Achieve perfect privacy, forget convenience.

Complete privacy is possible only in isolation and hence it's practically infeasible. The more practical approach would be to find an *intermediate solution* (between the two extremes). However, with intermediate solution another factor that comes-up is the Quality-of-Service (QoS).

LBS QoS is directly proportional to amount & accuracy of information provided to the LBS application; without which it loses its worth. Expectation for QoS without compromising privacy again leaves users in a state of uncertainty while sharing the informational elements. The user is hence perplexed with following questions in mind –

a. Shall I use or not use LBS?
b. If I choose to use LBS, is my privacy adequately protected, while ensuring certain levels of QoS?

Cultural advancements and socio-technical trends psychologically compel users to share the information for perceived benefits from the use of LBS; putting a pressing need for robust privacy preservation mechanisms in place.

IV. Privacy Preservation in LBS

As in [5] and proposed by Danezis, privacy can be classified as *hard privacy* and *soft privacy*. The protection goal for *hard privacy* is *data minimization*, assuming that the personal information is not yet divulged to the malicious parties. Whereas, *soft privacy* tries to implement algorithms to preserve location information (*location privacy*) and/or service parameters (*query privacy*) as both are closely related and, given one may reveal other[6]. Moreover, the user may query LBS in *snapshot* (single query in distinct time) or *continuous* (periodically recurring query) mode with adversary being *local* (compromised device or outside attacker sniffing communication channel) or *remote* (malicious LBS server) [6][8].

According to literature, privacy preservation approach may be implemented in the form of – Policies & Law (Regulations & Privacy policies) and Computational techniques (algorithms)

A. *Regulations* are implemented as acts and rules from regulatory / government authorities.

1) Challenges to effectiveness
(a) Non-compliance.
(b) Amendments not able to keep up pace with technological developments.

2) Reasons for ineffectiveness
(a) Malicious business intents supported by loopholes & workarounds in implementation / enforcement of rules.
(b) Lack of awareness and/or & casual approach towards rules, and associated privacy risks by the service providers.

3) Cost of ineffectiveness
(a) Information leak / privacy breach (end user).
(b) Lack of goodwill and trust (enforcing agency).
(c) Social disintegration (ecosystem).

B. *Privacy policy* is defined by the service provider itself.

1) Challenges to effectiveness
(a) Lack of enforcement by the service provider.
(b) Ambiguity and lack of transparency in policies defined.

2) Reasons for ineffectiveness
(a) Malicious intent and non-transparent business operations.
(b) Casual approach towards end user's privacy needs.
(c) No direct control of any regulatory authority over businesses privacy policy and its clauses.

3) *Cost of ineffectiveness*
   (a) Information leak / privacy breach (end user).
   (b) Lack of goodwill and trust (organization).
   (c) Social disintegration (ecosystem).

C. *Computational approaches* are implemented as protection mechanisms (algorithms) on server and/or device levels.

1) *Challenges to effectiveness*
   (a) Trust breach by the server in server based approaches.
   (b) In server free approaches, high processing & communication costs with compromised QoS (delayed/declined responses) due to operational problems like - sync among peers and lack of trust due to possibly malicious peers in adhoc network.
   (c) Less focused (researched) and limitations of exiting privacy preserving approaches to address privacy sufficiently; keeping in mind the pace of technological developments (data analytics and inference/association algorithms) together with social trends to keep connected with ubiquitous computing and easy connectivity (easy release and availability of data).

2) *Reasons for ineffectiveness*
   (a) Business intents, expectations for quick gains by businesses and service providers with not so well-formed or uniformity in laws about how the user data should be handled.
   (b) Tradeoff between level of privacy and performance (QoS) with existing infrastructure.
   (c) Lack of awareness and casual approach towards handling privacy sensitive data by involved parties and end-users.
   (d) Lack of formal, candid framework to understand privacy holistically and effectively implementing preserving mechanism with changing socio-technical trends.

3) *Cost of ineffectiveness*
   (a) Information leak / privacy breach (end user).
   (b) Lack of goodwill and trust (organization).
   (c) Social disintegration (ecosystem).

Privacy is subjective in its own sense, together with the *information* (in form of *identity*, *location*, *time* or any combination of these[7]) revealed, it also involves *contexts*, *assumptions*, *intentions*, *perceptions* and *trust* between the involved parties; and therefore, a whole new approach needs to be adopted to achieve privacy in a righteous sense.

V. Conclusion

LBS is an emerging domain offering benefits to its end-users and service providers. However, privacy concerns while using LBS cannot be neglected. In this paper, we identified threats to privacy and discussed about the effectiveness of approaches that try to preserve it. While accessing effectiveness of different privacy preserving approaches, we were successful in finding out certain shortcomings and hence conclude that privacy needs to be re-assessed and be dealt in more holistic way. Also there are some open challenges/possible future directions in this domain that needs immediate attention to achieve desired effect –

A. *Data privacy:* Once the data is revealed and stored with the provider it may be misused resulting in privacy leak hence, quantification of trust (on provider) may be helpful in this regard.

B. *Query privacy:* Most of the approaches for privacy preserving aims at preserving location privacy. However, protection of *service attributes* (query privacy) is equally important as it is closely related to location privacy and may lead to privacy leak.

C. *Generic framework for privacy preserving:* Current research for privacy preserving lacks generic framework that can take care of all privacy components, the need of the hour is to re-assess privacy through formal quantification and adversary modeling.

VI. Scope of Extension

Privacy is belief formed based on certain qualitative (experiences) and quantitative (compliance) measures; hence, to measure and control privacy risk, we need to revisit and define level of privacy achieved in terms of *compliance* (of privacy policies and law), *effectiveness of computational approach* (implemented algorithms for privacy protection) and privacy as it is *perceived* by LBS user.

References

[1] M. Bakillah, S. H. L. Liang, and A. Zipf, "Location-Based Services," *Int. Encycl. Geogr. People, Earth, Environ. Technol.*, pp. 1–18, 2017.

[2] R. Gupta and U. P. Rao, "An Exploration to Location Based Service and Its Privacy Preserving Techniques: A Survey," *Wirel. Pers. Commun.*, vol. 96, no. 2, pp. 1973–2007, 2017.

[3] P. In and P. Computing, "Survey O N Location Privacy in," *Context*.

[4] K. Michael, "Location-Based Services and the Privacy-Security Dichotomy," no. October, pp. 91–98, 2006.

[5] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements," *Requir. Eng.*, vol. 16, no. 1, pp. 3–32, 2011.

[6] R. Analysis, "2017 年第 13 期 - 基於風險的血液安全管理." pp. 1–2, 2017.

[7] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Pers. Ubiquitous Comput.*, vol. 18, no. 1, pp. 163–175, 2014.

[8] A. T. Tran, "Network Anomaly Detection," *Proc. Semin. Futur. Internet Innov. Internet Technol. Mob. Commun.*, no. September, pp. 55–61, 2017.