Preserving LBS Privacy: Issues & Challenges

Nitin Kulkarni[#1] , Sanjay Tanwani[*2], Narendra S. Chaudhari[**3]
#Department of Computer Application, Acropolis Institute of Technology & Research, Indore, India
*School of Computer Science & IT, Devi Ahilya Vishwavidyalaya, Indore, India
**Discipline of Computer Science & Engineering, Indian Institute of Technology, Indore, India
[1]nitin.kul@gmail.com
[2]sanjay_tanwani@hotmail.com
[3]nsc0183@gmail.com

Abstract : LBS usage is an identified privacy threat. Privacy is subjective in its own sense and hence difficult to address. In this work, we have tried to identify the core challanges in preserving LBS privacy inspite of fair understanding about the protection goals. We frame a privacy definition as per interpretation of issues & challanges and expect that it will help in development of an intelligent and scalable privacy preserving mechanism in the future.

Keywords : Location Based Services, LBS privacy, Privacy Challanges, GDPR, Privacy Protection, Protection goals

I. INTRODUCTION

Proliferation of portable mobile and wearable devices with inbuilt position sensors has drawn much attention to development and deployment of myriad location-based services in recent times. This has also led to ascension of a whole new market of location-based service providers servicing their clients with diverse location-based services. The growing use of location based services brought into focus the need for a concerted look on the privacy concerns of the users. Privacy undoubtedly is a topmost priority in LBS. However even with the clearly identified protection goals and privacy preservation mechanisms in place, a level of privacy that breeds trust and promotes LBS seems difficult.

II. LBS PROTECTION GOALS

LBS reveals personal identifiers of its user in the form of *identity information (ID)*, *location information (LI), time information (TI)* and/or any combination of these [1] (Table 1, *Appendix A*).

The decision of whether or not to use LBS is completely left with the user, though they are psychologically compelled to exchange the information for convenience LBS offers.

Still if user does not share the information at all about self, there exists a possibility of privacy breach, (as friends might be sharing some information [2]) on the other hand, if the user freely shares the information, possibility exists for vulnerabilty.

As evident (Table 1), the user may be spared only through complete isolation. (though this itself is contradictory [3]) which is highly impractical, in all other cases, user is a subject for privacy protection.

Privacy preserving in LBS is driven by two core principles - *data minimization* (a.k.a. *hard privacy, with less trust on other entities)* i.e. minimize the amount of data shared by the user and implementation of *privacy preserving mechanisms* (a.k.a. *soft privacy, when the data is already released by the user*) [4].

The inadequacy to address privacy issues in LBS usage with current level of understanding motivates us to study privacy and issues around it in more holistic sense.

III. CHALLENGES IN MEETING THE PROTECTION GOALS

LBS ecosystem involves multiple parties [5] - hardware manufacturers, software (operating system, core apps & third party) developers and human players (having their own motivations & conscious). Seamless flow of information across these, without any specific *control* or *accountability* [6-7] about how information is held, processed and/or (mis)used make privacy preservation a real tough task.

TABLE 2 : LBS ECOSYSTEM HUMAN PLAYERS AND THEIR MOTIVATIONS.

Player	**Motivation**
Consumers or end users	Fascinated by the convenience offered by LBS.
Business houses	Opportunity for business (data is new oil)
Hacker / Adversary	Fun, mischief, business.

Consumers or users are generally perplexed (*consent issue*) by the very concept of privacy and hence relinquish the control of information which then creates a privacy threat, whereas any adversary is unduly benefited lacking effective governance and loopholes in privacy preserving measures.

Even for the most cautious user data shared by others raises privacy threats. Moreover, the data collection done by business and applications (sometime much more than what they actually need, most of the time in legal agreement with user) and thereafter trading, aggregration and/or donating (on so called humanitarian grounds) the data to other agencies again put the users at risk.

TABLE 3 : PRIVACY HOLES IN LBS

Consent by users themselves	User divulge data about themselves casually.
Friends and acquaintance	Data shared (about user) by friends and acquaintance of the user.
Apps & services collecting data	*Malicious* (that intend to steal the information) or *legal apps* (that sometimes snoop more information than they actually need).
Business collaborations	Trading, exchange and cross analysis of data in commercial interests or otherwise.
Adversary attacks / Hacking	Attacks by miscreants (targeting both the individuals and the business houses in possession of data)

Governing bodies are clueless, they want to regulate, but cannot take action until the crime including non-compliance with regulatory policies) is committed and/or reported.

The very subjectivity (privacy perceptions), conflict of interests and privacy holes together (Table 2 & 3) makes LBS highly vulnerable and privacy preservation a real challenge.

IV. ADDRESSING THE CORE CHALLENGES

Core challanges in preserving privacy are not only technical [8] but also *moral* and can be attributed to *morality principles* governing behavior of any human players in the ecosystem (Table 2) [3].

Vulnerability in LBS therefore seem to stem from bad *technical* and/or *moral* judgement and is exploited (by adversary) to invade privacy. In the interconnected society where people need to know each other (socialize and share life experiences) perfect privacy is nothing [3] however, understanding root causes of risk and reducing the possibilities of malfunctioning or traps (enforcing integrity) would be helpful in promoting LBS usage.

TABLE 4 : VULNERABILITIES & THEIR ROOT CAUSE

Vulnerability	**Root cause**
System flaw	**Complexity** in design, testing and debugging.
Lack of privacy	Due to **budget constraints** or **shear ignorance** privacy is not given due importance in design.
Human action	**Ignorance** (casual sharing of data by users) and **Irresponsible** behavior (by organization aggregating the data).

Pace of technological developments (data science) and business competitions (justification of cost, primarily ROI) makes addressing complexity in system design and achieving prefect security/privacy difficult (Table 4).

Even if we are able to do so (with the most advanced and robust system in place), human actions (Table 4) exposes them to privacy attacks.

TABLE 5 : ISSUES IN PRIVACY PRESERVING

Issue	**Description**
Morality	Doing what is right and justified i.e. keeping integrity intact.
Intelligence	Understanding about privacy threats (internal and external) & know-how to deal with it, embedding privacy in design of systems (HW & SW).
Speed	Speed at which the preventive action can be taken if damage is suspected (proactiveness).
Accuracy	Accuracy with which the solution is applied once the flaw is detected.

European Union (EU) with General Data Protection Regulation (GDPR) in effect since 25th May' 2018 in an attempt to change the privacy preserving landscape emphasizes on *explicit user consent (with purpose limitation and duration for which the data can be held)*, user's *rights and control over personal information*, *accountability of data controller* holding the data*, transparency in data processing* and development of application keeping in mind *privacy by design* and *data minimization* principles [7].

V. CHANGING PRIVACY LANDSCAPE

Until GDPR, due to ambiguous regulations and little financial risks many LBSs tapping data were not much worried about consumer's privacy viewpoint [9]. However, with the new regulation coming up and Gartner warning that by the end of 2018 at least 50 per cent of companies were not in full compliance with the regulations (GDPR) we have entered the new data era, where businesses need to redefine their relationships with consumers bound by integrity, understanding and respect for their individual choices [10]. Aggregrators now need to be more proactive while dealing user privacy and are expected to go beyond a regular "compliance checklist" approach. Similarly, consumers now want control over their data [11].

VI. PRIVACY SECURITY DICHOTOMY

These terms are often used interchangeably; however, there is a subtle difference between the two. They have a common goal i.e. to protect sensitive data however the approaches are quite different. Security protects the system against any un-authorized access (physical and/or logical) whereas privacy tries to govern how the data is collected, held, used and/or shared. To some extent security helps preserve privacy though *vice-versa* may not be true [12].

VII. CONCLUSION

LBS usage is typical tradeoff between user's risk perception [13] and service usefulness. Research shows (Chart 1-3, *Appendix B*) that inspite of fading trust and high risk perceptions users readily trade their privacy for technology benefits and usefulness derived from LBS. The numbers are more prominent for youth.

Increasing awareness and regulations like GDPR lately have motivated users to demand more control over their data which only few (about 10%) beleive that they have, about 88% said that trust in service is a determining factor while sharing information and beleive that they would walk away if trust is lacking. Moreover, about 53% consumers would attempt to get back their data if given an option.[9-11]

As we interpret, "*Privacy is essentiallya trust in level of secrecy maintained about the part-of or complete communication (with transparency of purpose for communication) between (and to be mutually accepted and exercised by) consented parties (being aware about each others right to liberty) for the defined timeframe and valid data while respecting geographical, cultural and societal norms on humanitarian grounds*".

Time demands that LBS put security and privacy in the forefront of their business model, strive to implement (privacy mechnisms), meet (regulations) and transparently communicate (through strong privacy policy) with users to build brand (trust and reputation).

Based on explicit research, we understand that GDPR's recommendation to achive privacy through limiting data (*data minimization*) and *privacy-by-design* are the most crucial when it comes to empower LBS user. Hence we advocate the development of an *intelligent solution to address the underlying issues (Table 5) in accordance with GDPR guidelines* [7] that augment user ability to take smart decision and enables him to exercise increased control over his own data.

REFERENCES

[1] 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.

[2] N. Ajam, Location-based services and privacy, no. February. 2010.

[3] C. Friedt, "Privacy Author (s): Charles Fried Stable URL : http://www.jstor.org/stable/794941 Accessed : 07-06-2016 16 : 20 UTC Privacy *," vol. 77, no. 3, pp. 475–493, 2016.

[4] 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.

[5] M. Herrmann, M. Hildebrandt, L. Tielemans, and C. Diaz, "Privacy in Location-Based Services: An Interdisciplinary Approach," SCRIPTed, vol. 13, no. 2, pp. 144–170, 2016.

[6] EY, "Can privacy really be protected anymore ? Can privacy really be protected anymore ?," 2016.

[7] https://eugdpr.org/the-regulation/

[8] P. In and P. Computing, "Survey ON Location Privacy In Pervasive Computing," Context.

[9]http://fortune.com/2019/02/25/consumers-data-privacy

[10] https://www.information-age.com/gdpr-consumer-perspective-123467288

[11] https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html

[12] L. Perusco, K. Michael, and M. G. Michael, "Location-Based Services and the Privacy-Security Dichotomy," pp. 91–98.

[13] A. J. Iris, A. J. Norman, and S. Christiane, "Personality traits and concern for privacy: an empirical study in the context of location-based services," Eur. J. Inf. Syst., vol. 17, no. 4, pp. 387–402, 2008.

Appendix A

TABLE 1: THE TABLE LISTS THE INFORMATION ELEMENTS SHARED WHILE USING LBS WITH THE POSSIBLE RISK OF PRIVACY BREACH, THE "√" MARK STATES THAT THE CORRESPONDING ATTRIBUTE IS SHARED OR AVAILABLE, WHILE A "×" MARK STATES THAT THE ATTRIBUTE IS HIDDEN OR PROTECTED.

Protection goal			**Vulnerability**	
Identity	**Position**	**Time**	**Information Revealed**	**Need for additional Information ?**
x	x	x	Theoretically zero risk as it will be difficult to track the user.	Not of much use as user track is unavailable.
√	x	x	The user is clearly identifiable.	No additional information is needed to identify the requester.
×	√	×	Sporadic and/or continuous location information helps in tracking.	Background knowledge and semantics of location may help identify and track the requester.
√	√	×	The requester is clearly identifiable and traceable	No additional information is needed to identify/track the requester.
×	×	√	Temporal information in itself does not identify the user however, the time series may be constructed.	Background knowledge & observation with the time series may help in user identification / tracing.
√	×	√	The requester is clearly identifiable and traceable.	No additional information is needed to identify the requester.
×	√	√	The requester is not identifiable however completely traceable in space and time	Background knowledge and observation may help identify the user
√	√	√	The requester is clearly identifiable and traceable	No additional information is needed to identify/track the requester.

Source: *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.*

Appendix B (Page 1 of 2)

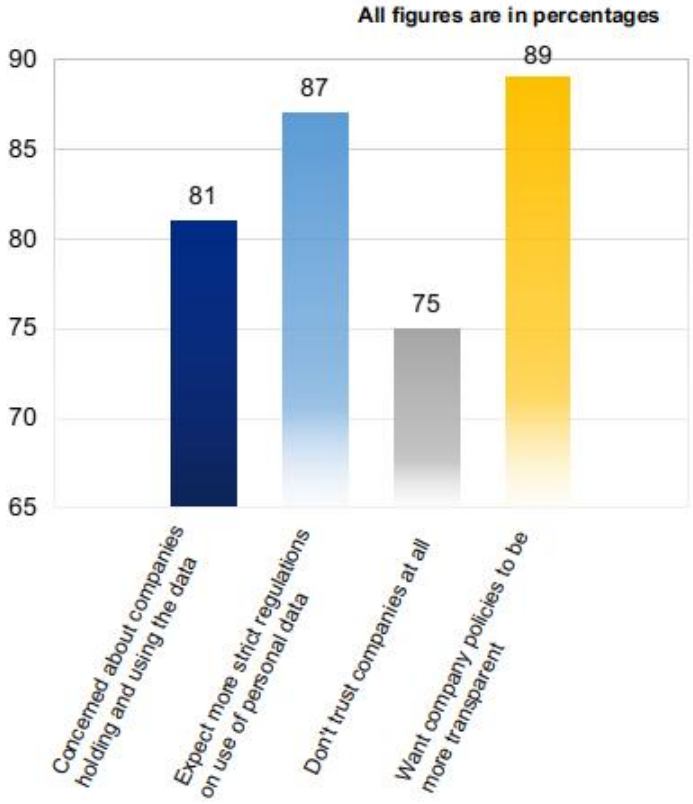

CHART 1 : USER TRUST IN COMPANIES IS FADING

Source: *http://fortune.com/2019/02/25/consumers-data-privacy/*

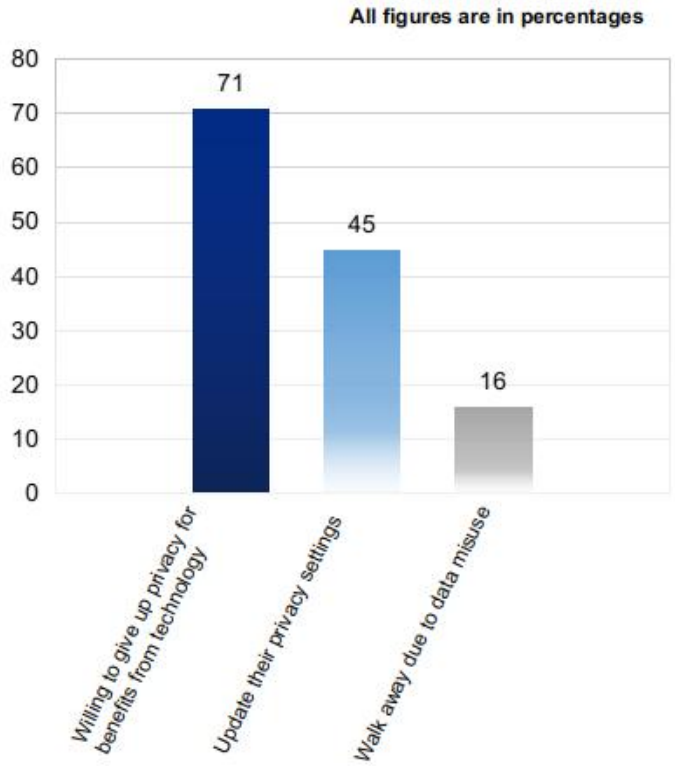

CHART 2 : CASUAL APPROACH OF USERS TOWARDS DATA PRIVACY.

Source: *http://fortune.com/2019/02/25/consumers-data-privacy/*

Appendix B (Page 2 of 2)

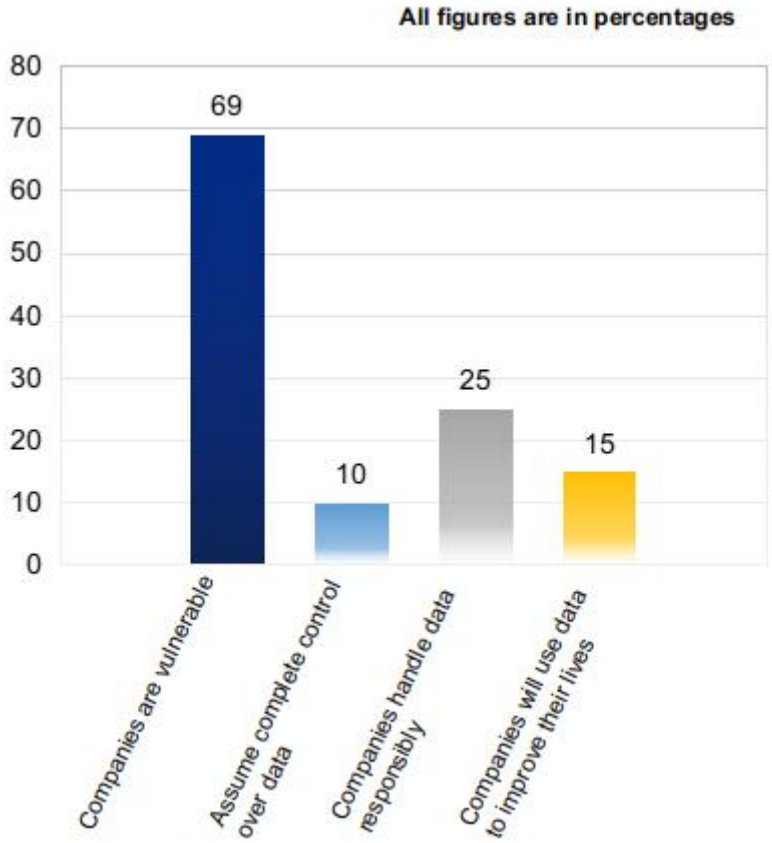

CHART 3 : USER PERCEPTIONS

Source:
https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html