Privacy in Augmented Location based Services -A Paradox

Supraja S
Systems Engineer, Infosys Ltd.
Mysore
India

ABSTRACT
The world is on the threshold of taking technology to an all-new level. With Augmented Reality (AR) applications taking over the markets at a rapid pace, the thin line difference between user interface and the physical world seems to have been obliterated almost completely. Though this has completely revolutionized the way users and technology evangelists have started thinking and simplified the way of looking at the world, it comes with its own perilous security and privacy implications. Amongst the numerous domains into which AR has divulged, the most sensitive sphere includes Location Based Services (LBS). This has been prophesied as a reason to rethink and worry about, however, the development is still on the rise and little has been looked into protecting users' privacy. This paper will delve into issues that raise a concern in terms of privacy and some suggestive measures that could be taken into consideration.

General Terms
Augmented Reality, Location Based Services, Security and Privacy measures.

Keywords
Privacy, Augmented Reality, Location Based Services, GPS, Pervasive Mobile computing applications.

1. INTRODUCTION
The world has transitioned into mapping graphics generated on various gadgets into real-world environments. This powerful breakthrough in technology is called Augmented Reality. This has been happening with such a transparent and fluid transition that it has completely revolutionized the way users of various augmented systems perceive the world. Creating and using such systems might bring sheer delight to developers, designers, businesses and end-users, however, it could be termed, as completely redefining the way privacy ought to be looked at in the 21st century [5] and puts an end to anonymity.

It will certainly not feel right to be monitored by strangers walking past you in a causeway for they would have access to your personal information through their smartphones or handhelds. Also, this poses a huge security threat. While many experts claim that AR can be used effectively by defence agencies to counter terrorism and other illicit activities, many fail to acknowledge the fact that the converse is also true. We cannot imagine how this technology can be exploited by extremist organizations and the gravity of delinquencies they will be able to commit when such sensitive information becomes easily available.

With a dive into capturing Location Based Services, AR applications have indeed captured the attention of the markets and offer something that everyone across the globe has been looking forward to. The fact that this will aid in user friendly navigation systems cannot be denied, however, it will be pushing the boundaries of user privacy and personal security will be at a huge stake.

This paper, will explore the use of AR in Location Based Services, the various security and privacy concerns it raises, existing laws and ethics in India and ways to address these issues.

2. AR IN LOCATION BASED SERVICES
Technology has become invasive into our lives. [4] We no longer find the necessity to ask for directions to a place, thanks to numerous navigations systems, rapid increase in GPS applications and indeed normal human interaction has been sidestepped. Collectively, such systems are called Location Based Services (LBS). One no longer feels strange in a foreign land and manages to travel and navigate with ease.

With the advent of AR systems, the existingsystems have evolved into more user-friendly and powerful applications. The volume of information that such systems can provide is immense and you get complete information of a place, building or even more granular information such as every floor or room in a building by simple positioning of your AR device to face the building or place that interests you (see Figure 1). Be it locating a café of your choice or rushing to a hospital; to checking the menu of the café or taking an appointment with a doctor in the closest hospital, everything can happen with just a mere tap of your finger.Such is the potential that these applications and services can offer. Some appropriate examples of these would be Nokia's City Lens and Layar.

These systems come in various capabilities by using many different technologies for mobile computing that is available today for location sensing. [2]

2.1 Using Scene Analysis
This technique circumvents any form of geometric calculations and instead it requires a map that is already stored with the objects that are required. In a static scene analysis technique, the system essentially compares the features that are available to an existing map that can then fetch the desired information. This is also sometimes called calibration. Likewise, in differential scene analysis, the users' changes are monitored and based on the subsequent scenes that are generated the user is tracked.

2.2 Proximity

Ina system that is based on proximity, retrieval of accurate positioning information is not possible. These systems are capable of only providing proximity information such as serving base stations of a known object. The key idea of using this technique is to calculate the distance between known reference points or pre-defined objects that lie within the proximity.

2.3 Geo-Positioning System (GPS)

GPS satellites orbit the earth and their signals are free to be used by anyone. The GPS receivers that are embedded within devices which are capable of supporting it perform a location estimation based on the time differences in arrival of signals from 4 different satellites hovering over that region. It computes 3 major parameters to point to a location, viz. latitude, longitude and altitude. Owing to its accuracy and low cost, GPS stands out as the most preferred option for outdoor location sensing.

2.4 Cellular Network Triangulation

In situations where users don't have access to an active data connection, an alternative to GPS for outdoor location sensing can be achieved by means of a technique called cellular network triangulation. It essentially makes use of any three adjacent base stations and uses a technique similar to proximity to compute the location of the device, which in this case will essentially be a smartphone that is served by a service provider. However, this is feasible only when the service provider has a well-defined and established network with a reasonably large number of base stations.

2.5 Indoor Location Sensing

Unlike outdoor location sensing, indoor location sensing techniques do not have access to base stations or satellite signals. Owing to a lot of alternatives available, indoor location sensing is quite adaptable and can pick from a variety of technologies based on the expected accuracy, speed and cost. Some of the technologies used are diffused infrared, ultrasound, radio frequency identification, wireless LAN and Bluetooth.

3. CHALLENGES HURLED BY AUGMENTED LBS

The rapid rise in this domain raises privacy concerns to alarming levels. Our view of the real world will not be restricted to what our naked eye can see. AR systems will start turning the real-world panorama into a playground very soon where people will kindle their creative skills which will start creating illusions and deceive the common public.

It is aneminent fact that ever since the culture of social networking took over, self-disclosure of private and sensitive data, especially photos, has become too common and most of the general users fail to understand the gravity of privacy and security threat that it poses.

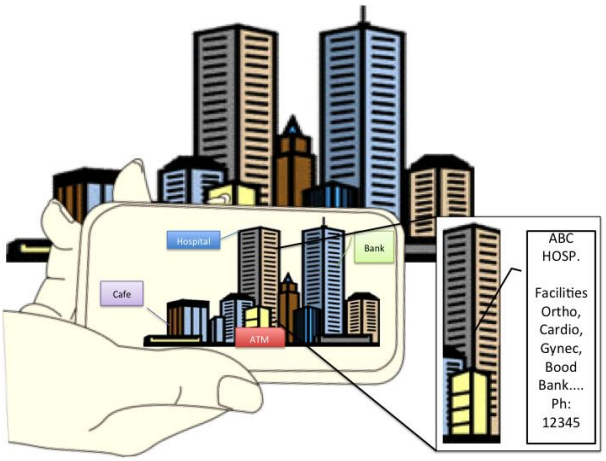

Figure 1: Depiction of AR in LBS

Combining publicly available online social network data with off the shelf face-recognition technology for the purpose of large-scale, automated, real-time, peer based individual re-identification and inference of additional and potentially sensitive personal data, AllesandroAcquisti and Ralph Gross [6] conducted a series of experiments in 2009. The results can be seen in Table 1.

Table 1.Experiments by Acquisti and Gross and their outcomes

Exp. No.	Experiment	Result
Exp. 1	Online-Online Re-Identification	1 out of 10 dating site members were identified.
Exp. 2	Online-Offline Re-Identification	1 out of 3 subjects were identified
Exp. 3	Online-Online Sensitive Inferences	27% of the subjects' 5 Social Security Number (SSN) digits were identified with 4 attempts starting from faces.

It has been over a couple of years since these experiments were conducted and the situation has only worsened since. Based on the above findings and further research [3], some major challenges are as follows.

3.1 Profiling

Profiling will lead to a seamless integration of online and offline lives. Your movements will become easily traceable with users tagging their location information on social networks. Moreover, apart from just revealing information of your current location, it could also expose a lot of related sensitive information such as photos, your travel agenda etc., which is capable of making your personal holiday a short travel film to many strangers.

3.2 Unauthorized augmented publishing

This includes many media agencies filling in excessive details of things that might be of your interest whether or not you requested for it. If hoardings and billboards were demanded to be removed by certain governments in parts across the country, imagine walking down the street and your device

screen gets filled with unsolicited advertisements and lucrative offers from various other agencies based on your previous visits to that location or your search queries. Excessive information than required is always a nuisance. This leads to our next concern.

3.3 Augmented behavioral targeting

This relates to the distress that can arise due to people targeting your emotional sensitivity. Excess of pervasive computing has reached a disturbing level by capturing emotionally private and sensitive information. It has led to the emergence of what is called Personal Predictable Information (PPI) [6] posing extreme perils to individuals in terms of their personal security and privacy.

All these, lead to serious repercussions in the human society that might even lead to social detachment. Gone are the days when video capturing was considered an intrusion into one's privacy; for now, with these augmented LBS systems, one's movements can be constantly monitored as these devices are not bound to a specific location like the surveillance cameras and will be constantly acquiring data as the user transitions between various situations and locations.

The privacy intrusions may be subtle and most of the intrusions will probably not be because of a specific piece of information that was retrieved or captured but instead because of a series of information that were gradually collected by these devices over a prolonged period of time. [8] All these challenges lead to coming up with a solution to resolve the ongoing conflict between ubiquitous computer use and protecting personal privacy rights.

4. LEGAL CONSIDERATIONS FOR PRIVACY PROTECTION

Spatial law is a set of legal issues associated with geospatial technology and the collection, use and transfer of location and other types of data. This law is still unclear and very little precedents exist. [1]

In June 2011, India passed a new privacy package that included various new rules that apply to companies and consumers. [10] A key aspect of the new rule requires that any organization that processes personal information must obtain a written consent from the data subjects before undertaking certain activities. It is stated that the application of this rule is still uncertain.

As per the Information Technology (Amendment) Act, 2008, [11] a couple of new privacy related amendments were made. Section 43A deals with the implementation of 'reasonable security practices for sensitive personal data or information' and provide for the compensation of the person affected by 'wrongful loss or wrongful gain'. Section 72A provides imprisonment for a period of up to 3 years and/or a fine up toRs.5 lakh for a personwho causes 'wrongful loss or wrongful gain'by disclosing personal information of another person while 'providing services under the terms of lawful contract'.

With the digital world flooded with personal data, a report by the World Economic Forum (WEF) titled 'Rethinking Personal Data: Strengthening Trust', published in collaboration with Boston Consulting Group, it can be said that the scope for abuse of personal Information is bound to increase. [12]

Every person in the European Union (EU) has the right to access all the data that a company holds on him or her. A perfect example quoted was that of an Austrian national Max Schrems of Viennawho asked the largest social networking site Facebook Inc. for a copy of every piece of information it had collected on him since he had created an account with it two years earlier.Schrems was delivered a CD packing a 1,222-page file—roughly the length of Leo Tolstoy's panoramic War and Peace, one of the longest novels ever written.The data included information which Schrems has deleted, but had been stored in Facebook's servers, according to ThreatPost, a publication on Information Technology (IT) security run by Kaspersky Lab, a leading maker of anti-virus software.[12] However, India has no such privacy law incorporated into the system as yet!

Moreover, with the gradual implementation of Unique Identification Number system or 'Aadhaar' as it is called, that the Government is planning to implement, the reasons to worry have increased multiple folds. This will make our society at large more vulnerable as compromising just one unique number will reveal all sensitive information of the person concerned.

Yet another program that draws worry lines on the face of citizens is the National Intelligence Grid (NatGrid) project, which aims to connect the databases of airlines, banks, telecom operators and other private and public sector companies to support investigative agencies with real-time information. This will facilitate miscreants in a way that they need not try to attack or penetrate into many individual databases to get information about a target victim, but instead breaking into one grid will give them wholesome access to well integrated and consolidated sensitive information. This project is planned to get implemented in 4 phases, the initial two of which will be released in 2014. It will only be efficient if the government starts taking necessary security measures, which are yet to be addressed.

The Government's various attempts to regulate Internet content have been construed as efforts to impinge individual's freedom of speech and expression. The debate on Right to Information (RTI) and Privacy is still ongoing. At the inaugural session of the 7th Annual Convention of Central Information Commission on Friday, 12th October 2012, Prime Minister Manmohan Singh called for 'maintaining a fine balance between RTI and right to privacy, the latter of which stems out the fundamental Right to Life and liberty. The citizens' right to know should be circumscribed if disclosure of information encroaches upon someone's personal privacy'.

These laws and statements still leave behind a lot of questions and we are yet to resolve what the environment tracks and shares and what remains private. Widespread use of these systems and extensive location-aware devices will only lead to more such questions and the impingement on personal privacy will keep intensifying.

5. ADDRESSING PRIVACY ISSUES

Though many measures have been suggested, little has been taken into consideration in the existing systems. It has become essential to develop guidelines and interface frameworks that ensure a privacy-aware design of interfaces and information displayed across private built-in systems include easy-to-use safeguards against unintended projection of sensitive information.[9]

Privacy services can be deployed which can aid in addressing the primary challenge of conflict between more pervasive augmented applications utilizing the sensitive information of users and the need for privacy protection in a computing environment of many such applications.[2] Addressing privacy issues is more complicated than addressing security issues. When it comes to privacy, you cannot just draw the line between what information can be used or shared and what cannot, whereas, in security, we know for a fact that a set of security functions must be implemented in the system.

5.1 Approaches for addressing privacy issues

In order to address the above privacy issues, some of the below suggested approaches could be adopted.

5.1.1 Increasing awareness of potential privacy breach

With privacy issues that are posted in the current environment such as social networks, it is quite obvious that majority of users of these systems largely remain unaware of the privacy implications. It is therefore necessary to educate people on its repercussions. These could be achieved by various means such as pre-launch workshops, privacy specifications and manuals sent along with the devices similar to usage manuals that are existent.

5.1.1.1 Maintaining an audit trail

The service providers must maintain a detailed audit trail of every packet of information transmitted or received across devices. This will facilitate in tracing back on loopholes when an issue is raised. Also maintaining an audit trail will help adhere to legal norms and ethics and there will always be documents to support when it comes to facing legal obligations.

5.1.1.2 Intelligent alert

Intelligent alert mechanisms can be implemented which will probably be of utmost use to lame users who are not very sound with the technical backend operations when it comes to using these high end Augmented Location Based Systems. An intelligent alert is essentially a privacy protecting mechanism that can probably trigger alerts every time the user performs an operation which puts him in a risk of sending out private and sensitive data. The alert mechanism will prompt on the user screen whenever an application uses his personal information or when he accidentally publishes his data that can be vulnerable or that might leave a trace on the system without the user's knowledge. These alerts will help the user to decide whether or not he intends to go ahead with that specific operation.

5.2 Mechanisms that can be adopted

Protecting privacy in Augmented Location Based Systems can be broadly grouped under two heads viz. Identity Anonymity and Location Privacy.

5.2.1 Identity anonymity

This can be achieved by means of using a proxy based anonymity system. This can be used to provide both privacy and accountability. Here the user and server interaction takes place by means of a user proxy and a server proxy. For example, every time a user keys in the name of a place that he is looking for, the request is transmitted from a proxy that poses to be the user. Therefore, the personal information or sensitive data of the user is not published anywhere. Even the device information remains secure and it is only the information of the proxy that is transmitted. This creates a security abstraction layer at the user's end.

Another means by which sensitive data can be compromised is by directly attacking the server that processes the user's requests and trying to retrieve sensitive information. To address this, a server-proxy can be used which mimics the original server and has a copy of the required protocols. However, this proxy server does not save any data in itself. Thus, each time an attacker tries to penetrate into the server, he is actually acting upon a proxy that poses to be the server and therefore his attempts to retrieve any kind of data or information goes in vain.

Also secure routing mechanisms can be adopted each time the user contacts the server or the proxy such as onion ring routing. Certain existing proxies that are available are Anonymizer (www.anonymizer.com) for user-proxy and Rewebber (www.rewebber.de) for server proxy.

5.2.2 Location privacy

Location privacy can be achieved by means of using location information security. Geopriv (Geographic location/privacy) is a location privacy framework that is provided by IEEE Work Group. It essentially defines a location object that conveys location information and possibly privacy rules to which Geopriv security mechanisms and privacy rules are to be applied.

Another way by which it can be achieved is by means of an identity pseudonym, which hides user's identity by making network traffic anonymous in a location-based application. One example is that of Beresford and Stajano [15] who have designed a privacy-protecting framework based on frequently changing pseudonyms, thereby effectively mapping the problem of location privacy onto that of anonymous communication.

5.3 Protecting From Wardriving

Wardriving, which is a traditional method to track Wi-Fi networks while on the move, can also be used to locate users on specific wireless networks and procure their information which can then be mapped on to any LBS. Wardriving is still not considered illegal and cannot be completely prevented. However, some basic measures can be adopted to make it difficult for hackers to penetrate and fetch your information as given below:

5.3.1 SSID Securing

The Secure Set Identifier (SSID) is a public name that is used to identify a wireless network. This, if not secured, can be potentially used to retrieve information from a router about the devices and users connected to it. Therefore securing this is highly necessary. To begin with, the routers will have to be configured to prevent broadcasting of SSID and must be secured with either WEP or WPA/WPA2 encryption.

In order to avoid storing or being logged in Google's Location Server, suffix your SSID with *"_nomap"* string. [16]

5.3.2 MAC Filtering

We can add access tables to our router which will allow only permitted devices to connect to the router.Thereby, unauthorized devices will not be able to log on to the network. This can be done by adding MAC address filters so that only recognizedand authorized devices will be able to get access to a specific router and wardrivers can get eluded.

5.3.3 DHCP Client Limitation

Out of the box, there is no restriction on the number of DHCP clients that your router can give out. But enforcing a limit on this aspect will become a challenge for wardrivers. This is because they should have static addresses in order to gain access to the network and more specifically they will have to fall into the same subnet range. Most novice attackers who try to penetrate networks with readily available tools and little knowledge of networks will not be able to identify the subnet range and therefore this will try to administer yet another step in protecting from wardrivers.

Finally, location information policies must also be kept in mind while addressing the privacy issues. This will primarily focus on building a set of policy frameworks that will help in addressing the issue of privacy violation and thereby facilitate users to interact freely with location-based applications.

6. CONCLUSION

We are yet to resolve what the environment tracks and shares and what actually remains private.[13] The potentially pervasive nature of Augmented Location Based Systems cannot be denied, however, development of these systems cannot be terminated in a techno-centric future where every fundamental need will be addressed only by using technology. Therefore, right from the formative stages of building these systems, caution must be exercised. Building them in a secure fashion by protecting user privacy is sine qua non.

7. REFERENCES

[1] Kevin D.Pomfret, Centre for Spatial Law and Policy "Augmented Reality: Legal and Policy Considerations", www.perey.com

[2] Pei Zheng, Lionel M.Ni, 2009, "Smart Phone and next Generation Mobile Computing" book, Morgan Kaufmann Publishers.

[3] Nilesh Zacharias, Feb 2010, "5 Real problems in an Augmented World", digitallynumb.com/post/399172973

[4] Future Conscience website, Sep 2009, "Augmented reality: The good the bad and the ugly"

[5] Adam Clark Estes, Feb 2012, "The reality of Augmented Reality", The Atlantic Wire.

[6] AllessandroAcquisti, Ralph Gross, Nov 2011, "Privacy in the age of Augmented reality", Talk or presentation, TRUST autumn 2011 conference.

[7] Randall K. Nichols, Panos C. Lekkas, 2006, "Wireless Security- Models, Threats and Solutions" book, Tata McGraw-Hill Publishers.

[8] Stephen S. Intille, Amy M.Intille, Sep 2003, "New Challenges for privacy law: Wearable Computers that create electronic digital diaries", MIT House_n technical report.

[9] EuricoRukzio, University of Duisburg-Essen and Lancaster University; Paul Holleis, DOCOMO Euro-Labs; Hans Gellersen, Lancaster University, 2012, "Personal projectors for pervasive computing", IEEE CS.

[10] Ryan, Falvey, Merchant, Oct 2011, "Regulation of the cloud in India", Journal of International Law, Volume 15, No.4

[11] "Information Technology (Amendment) Act", 2008, Ministry of Law and Justice, Government of India.

[12] SurabhiAgarwal, Leslie D'Monte, SahilMakkar, May 2012, "Data Boom! Why is India paranoid about privacy?", Live Mint and Wall Street Journal.

[13] Ramon Caceres, AT&T labs, Adrian Friday, Lancaster University, 2012, "UbiComp systems at 20: Progress, Opportunities and Challenges", IEEE pervasive computing.

[14] S. Pase, 2012,"Ethical considerations in Augmented Reality applications", Fielding Graduate University, EEE6059.

[15] A. R. Bresford, F. Stajano, 2003, "Location Privacy in pervasive computing", IEEE pervasive computing.

[16] http://support.google.com/maps