Location Privacy: Privacy, Efficiency and Recourse through a Prohibitive Contract

N.J Croft*, **M.S Olivier****

*ICSA Research Group, Department of Computer Science, University of Pretoria, Pretoria, South Africa.

**ICSA Research Group, Department of Computer Science, University of Pretoria, Pretoria, South Africa.

E-mail: ringtingting@gmail.com, martin@mo.co.za

Abstract. In certain circumstances an individual may not be in control of their private location information and thus vulnerable to a privacy violation. In this paper, we ensure location privacy through the establishment of a prohibitive contract in a situation where an individual wishes to minimize privacy loss and a service provider aims to maximize profits. Given the possible strategies we show that a privacy equilibrium can be found. This equilibrium, expressed in the form of a prohibitive contract, is established with the intention of preventing a possible privacy violation. Should within the constraints of the prohibitive contract, a violation occur, a suitable and efficient outcome for both parties presents itself. We further investigate how such violations may affect a user-centric location privacy system. Emphasis is placed on the economic and contract aspects of the parties' relationship, rather than specific technical detail of location privacy. Utilizing the utilitarian paradigm approach, we evaluate the overall efficiency of the prohibitive contracts which we show postulates convergence towards an overall balanced system.

Keywords. Privacy, Location Privacy, Game Theory, Utility

1 Introduction

Location can be defined as the knowledge of the position of an object or an individual. Variations of location-based services offer subscribers the convenience of finding nearby restaurants using their mobile phone, or locating and tracking friends from social networks. In each instance, their precise location is identified and recorded.

Location privacy is a particular type of information privacy. It is defined as the ability to prevent other parties from learning one's current or past location [2]. Usually position is computed and maintained by an external source, such as the underlying network [3]. In a mobile communications network, this is necessary in order to route calls to and from subscribers within the network. Location is determined mathematically by calculating the distance using a time interval approach between an object and a fixed known location point or simply by the entry point of a subscriber to a network. The problem is clear: how is location privacy possible when location information is necessary in connecting communicating parties and while under the control of a service provider?

The custodian of private location information is obliged to protect the individual's personal information. However, if a decision is made by the network service provider to

monetize their subscriber's location information, there is little option available for the individual subscriber to prevent such an action nor recoup any compensation for this privacy violation. The only available option for an individual whose privacy has been infringed upon is an attempt to pursue legal action against the perpetrator. In fact, in the generic case, where an individual's private information is divulged by a controlling third party, the individual currently has ***no*** means of reinstating their privacy and has few options for compensation in this regard. On the other hand, if reasonable recourse is an available option, some individuals may feel apathetic towards their private information and content with collecting some economic compensation. In most cases it is assumed that the vast majority of individuals would opt for privacy assurance over the option of a privacy violation compensated with some economic gain. It is thus this paper's intention to focus on preventing privacy loss and seeing any recourse value as a penalty incurred rather than a reward received.

Our purpose in this paper is to define a privacy location system which maintains equilibrium between the competing objectives (privacy prevention and profit generation) of the parties. The emphasis being on the economic and contract aspects of parties' relationship, rather than technical detail of location privacy. An equilibrium is expressed in the form of a prohibitive contract which both the subscriber and service provider are bound by and is of no benefit to anyone if violated.

In this paper, a prohibitive contract describes the constraints necessary in order to prevent the interaction between parties achieving any of their competing objectives. In other words, a prohibitive contract prevents engagement between parties which may lead to a privacy violation. Should the prohibitive contract be compromised by one party, the other party is presented with a mechanism for calculating a suitable recourse value.

Our aim in this paper is to define a location privacy prohibitive contract which defines a suitable recourse mechanism, should a violation occur. Furthermore, the goal is to show an overall system outcome resulting from any violations of the prohibitive contracts (between individuals and the service provider) is a desirable one for *all* parties concerned. The objective is thus best represented in the notion of efficiency. Efficiency is an important criteria for evaluating systems and public policies. Efficiency, in this paper, is the measure of the quality of a location privacy system which leaves no one in the system economically strictly better off.

Utilitarianism is the idea that the moral worth of an action is solely determined by its contribution to overall utility, that is, its contribution to happiness or pleasure as summed among all users. Utility, the good to be maximized, has been defined by various thinkers whose classic proponents were Jeremy Bentham [25], John Stuart Mill [23], and Henry Sidgwick [24]. Together these claims imply that an act is morally right if and only if that act causes "the greatest happiness for the greatest number".

Although, our prohibitive contract may apply to general types of data, we choose location data for the instantiation of the proposed approach and for illustration purposes via a real-world numerical example.

This paper is structured as follows: Section 2 covers location privacy concerns and examines previous location privacy work. Section 3 finds a location privacy equilibrium between the individual subscriber and the service provider through the establishment of a prohibitive contract defining privacy, efficiency and recourse. To demonstrate that the proposed method can be used practically, a simulated example is presented in Section 4. This section is devoted to the rational argument that some users may be apathetic towards their private information thus affecting the overall efficiency of the system. Finally Section 6 concludes this paper. This paper forms part of a mobile network privacy project, some

other works included are [10, 11, 12, 13, 14, 15, 16, 17, 18].

2 Background

2.1 Previous Work

Various approaches have been proposed in gathering user location information. They differ in measurement namely: accuracy, range, units, time and cost. Technologies include Global Positioning Systems (GPS), Radio-Frequency (RF) tags and various other wireless based methods. These systems provide location management operations but rely on privacy-enhancing technologies (PETs) in order to protect the unauthorized misuse of location information.

Some solutions and frameworks have been proposed for handling location privacy. A vast majority are based on the existence of a Trusted Third Party (TTP). IETF Geopriv Workgroup [4] provides a framework for TTPs by introducing a Location Server (LS) to manage subject location. Due to the fact that LS is a centralized storage, user location information is prone to eavesdropping and attacks. Geopriv's goal is to allow the tracking of user location through location (data) objects while maintaining some user controls. Users define rules both on the location server and embedded in the location object which restrict how the data can be redistributed.

Marias et al. [5] propose a new technique in ensuring location privacy through secret sharing techniques where location information is seen as a secret divided into n pieces and all pieces are required to restore the original information. This proposed architecture enables privacy location without relying on the existence of a TTP. Instead it uses "Share the Secret" (STS) servers, which are untrusted entities, to distribute portions of anonymous location information, and authorizes other entities to combine these portions and derive the location of a user.

Kesdogan et al. [6] propose the use of temporary pseudonymous identities to protect the identity of subscribers. However, anonymity and pseudonymity are not complete answers to privacy concerns because:

- Anonymity presents a barrier to authentication and personalization, which are important for a range of applications [7].
- Pseudonymity and anonymity are vulnerable to data mining, since identity can often be inferred from location [2].

Duckham et al. [9] and Ardagna et al. [1] address the location privacy problem through a formal framework using obfuscation, obfuscation-based techniques and negotiation. Obfuscation concerns the practice of deliberately degrading the quality of information in some way, so as to protect the privacy of the individual to whom that information refers. It protects location privacy by artificially inserting into measurements some fake points with the same probability as the real user position. Such techniques may degrade system performance particularly in a network where latency affects the quality of communication. Others like [26, 27] simply take obfuscation a level further and suggest encryption and masking as means to ensuring location privacy.

Zhong et al. [8] introduce three protocols (named *Louis, Lester* and *Pierre*) for solving the nearby-friend problem (a variant of the location privacy problem). The *Louis* protocol requires a semi-trusted party which does not learn any location information. The Lester

protocol does not need a third party, but has the drawback that a user might be able to learn a friends location even if the friend is in an area that is no longer considered nearby by the friend. The Pierre protocol does not have this disadvantage at the cost of not being able to tell the user the precise distance to a nearby friend. Although each of these protocols may have specific application in solving the nearby friend problem, there remains some pertinent privacy issues around friends knowing location information which may be disseminated without the consent of the individual.

In all the aforementioned location privacy approaches and frameworks (TTP, secret sharing, temporary pseudonym, obfuscation), achieving location privacy has specific application and purpose. Their privacy-enhancing capability, effectiveness and practicality remains open for debate. Should a privacy location violation occur, none of the previously presented techniques allow for a suitable privacy conflict resolution and recourse for the individual should a privacy violation occur.

We describe, at the outset, the importance of game theory in understanding techniques available for finding an equilibrium in a system. This forms the basis when establishing a prohibitive contract.

2.2 Game Theory

Game Theory [19, 20] is concerned with analyzing the interactions of decision makers with conflicting objectives. Game theory thus studies the choice of optimal behaviour when costs and benefits of each option depend upon the choices of other individuals. In strategic games, individuals choose strategies which will maximise their return, given the strategies that other individuals choose. Although game theory has been the focus of attention in years gone by, there has been a renewed interest in the applications of its principles. One example of this is Mackey et al. [28] who applies game theory to understanding statistical disclosure of events.

Combinatorial game theory (CGT) is a mathematical theory that only studies two-player games which have a position which the players take turns changing in defined ways or moves to achieve a defined winning condition. CGT does not study games of chance, but restricts itself to games whose position is public to both players, and in which the set of available moves is also public. Applying CGT to a position attempts to determine the optimum sequence of moves for both players until the game ends, and by doing so discover the optimum move in any position. In practice, this process is notoriously difficult unless the game is very simple. CGT should not be confused with game theory which is traditionally used in the theory of economic competition and cooperation; however similar operations and principles apply. CGT is not usually associated in establishing collaboration where private information is concerned, however, given the existence of conflicting objectives between decision makers it is conceivable that CGT is a perfect mechanism to determine the conditions which define a prohibitive contract.

2.3 Finding Equilibrium and determining Efficiency

The most important equilibrium concept in game theory is the concept of Nash Equilibrium [22]. A Nash Equilibrium is a strategy profile such that no user may gain by unilateral deviation. Thus Nash Equilibrium is a *stable operating point* as no user has incentive to change strategy. More formally, a Nash Equilibrium is set in game (S, f) where S is a set of strategy profiles and f is the set of payoff profiles. When each player ($i \in \{1, \ldots, n\}$) chooses strategy x_i resulting in a global combined strategy profile $x = (x_1, \ldots, x_n)$ the

player i obtains payoff $f_i(x)$. Note the payoff depends on the strategy chosen by player i as well as those chosen by all the other players. A strategy profile is a Nash Equilibrium if no unilateral deviation in strategy by a single player is profitable. Thus a strategy profile $x^* \in S$ is a Nash Equilibrium if:

$$\forall i, x_i \in S_i, x_i \neq x_i^* : f_i(x_i^*, x_{-i}^*) \geq f_i(x_i, x_{-i}^*) \quad (1)$$

In other words, by changing strategy, the player will not benefit in any way. We do not use Nash Equilibrium directly but rather apply the principles in finding under what conditions a stable operating point can be found so as to maintain location privacy.

Finding equilibrium, where location privacy is concerned, is comparable to finding suitable constraints such that no party may gain by unilateral deviation. More formally, our goal is to find the constraints under which a stable operating point exists such that the conditions prohibit any party from becoming strictly better off. For our purpose, a privacy equilibrium is finding a balance in the following situation: private information is preserved by the presence of a suitable deterrent (monetary loss) should the custodian divulge the individual subscriber's information, causing a privacy violation. Collectively, such conditions affect the efficiency of the entire location system.

Recall that utilitarianism is often used to gauge levels of "happiness" amongst users, it is also used to represent the total benefit (in monetary terms) to all in a system. We choose utilitarianism as a means to present a numerical example depicting a practical world where apathetic users exist and privacy infringements do occur.

3 Finding a Location Privacy Equilibrium

Determining the intrinsic value of private information is a subjective process and evidently hard. This can be attributed to the fact that privacy and privacy violation is dependent on the individual, the degree of violation, time, circumstance and situation.

Private information has a perceived value proportional to the demand for it by others and the amount of anguish it causes the owner should privacy be infringed upon. Information which may be deemed private today may have "less" or even "more" of a privacy implication in the future. Take for example a mobile telephone number which over time, may form part of an individual's identity, used for social and business purposes or alternatively may be used briefly for a specific purpose and then be discarded by the individual. We see private information as information with some inherent value which is influenced by social, economic and environmental factors. This information has the distinct possibility of being relinquished to others without the owner's consent.

Laudon et al. [21] suggests one possibility of valuing private information is through the creation of a National Information Market (NIM). The concept of a NIM is best described as a place where information about individuals is bought and sold at a market clearing price freely arrived at, in which supply for this information is equaled by its demand. Similar to financial markets, an "Exchange" would bring together buyers and sellers of private information for the purpose of transacting at a market clearing price. NIM, in our case, is used as a hypothetical construct, used only as a mechanism to get an associated value. It may be argued that everyone possesses information about themselves that would be of some value under some circumstance, to others, for commercial purpose.

If there is a monetary gain through the sale of private information, the individual currently does not receive any compensation for this *loss*. In many cases, there is an imbalance in the

tradeoff of a custodian protecting private information against the desire from benefits derived from relinquishing this information to others. Remember the premise in this chapter is that the individual's primary concern is privacy protection rather than the prospect of the individual deriving benefit from sold private location information.

3.1 Current Location Privacy Imbalance

Currently, divulgence of private location information is at the sole discretion of the service provider. We use the notation $(individual; service\ provider)$ to indicate the utility of each party. Traditionally in a mobile environment, the individual derives benefit from using the service provider's infrastructure (e.g. making a call). The service provider charges the individual and derives profit. In other words, the utility describes the benefit to each party given a set of circumstances. Generally, an individual is happy to engage in a service, provided the benefit gained is offset against the charges incurred.

If m_i represents the value (in monetary terms) of private information as perceived by i then the utility of the individual should private information be sold or divulged, for some benefit to the service provider, is shown as $-m_i$. Should the service provider SP divulge private location information, the utility for SP is a divulgence payoff, denoted by u.

Should a privacy violation occur, there are a number of legal options available to the individual should SP divulge private information; we briefly discuss two of these. The first is a state-pursued criminal case against SP on behalf of aggrieved individuals. The state prosecutes and fines SP if it is found guilty of a privacy violation. The second is a civil case brought against SP by the individual in order to pursue a degree of compensation for a privacy infringement.

We focus our attention on a civil case, and choose $P(sue)$ to denote the probability i successfully takes legal action against SP for a location privacy infringement. A recourse value, denoted by r, is awarded by the court to the plaintiff should there be sufficient evidence proving a privacy violation. r may include punitive damages, again awarded by the court, as further compensation for losses as a direct result of the privacy violation.

If the costs involved in the individual suing the service provider are greater than the potential recourse value r issued by the court, then the probability of i pursuing any legal action against the service provider diminishes to zero, thus $P(sue) \times r = 0$. In the case where private information is managed correctly, the utility of i and SP is represented as $(\Delta_i; \Delta_{SP})$. In other words, the SP does not gain unilaterally at the individuals expense and the individual does not loose.

If *no* civil case is opened by i against SP, the result is that SP simply gains the divulgence payoff u while i looses his perceived value, m_i. This scenario is indicative of a situation where costs incurred negate any legal option available to i. Thus, there is a clear affinity towards SP divulging i's location information, thus creating an imbalance, as shown in Equation 2.

$$(\Delta_i - m_i; \Delta_{SP} + u) \tag{2}$$

In summary, the individual wishes to enjoy a service while private location information is protected. Should a privacy violation occur, determining and receiving any recourse is an arduous task and the individual has **no** guarantee of being successful. On the other hand, in knowing the service offering is not bound by any privacy contract, SP is confident that if $u > P(sue) \times r$ (the divulgence payoff exceeds the probability of being sued and

being forced to pay an "admittance of guilty" fee) then the individual's private location information is "sold" in order to maximize profits.

3.2 Privacy, Efficiency and Recourse

A possible solution to solving the privacy imbalance is to create a prohibitive contract outlining the basis for privacy equilibrium including a privacy violation payoff. Recall, a prohibitive contract is seen as the constraints necessary in preventing the interaction between parties trying to achieve their competing objectives. Finding equilibrium is comparable to finding a stable operating point in which no player may gain by unilateral deviation and where the overall location privacy system is considered efficient. In establishing a prohibitive contract, we hope to achieve a desirable equilibrium where the individual maximizes privacy confidence while the service provider provides a consistent and private service.

It is interesting to note that SP is subject to lose a degree of trust from i should a privacy infringement occur. However, trust is inconsequential in establishing a prohibitive contract as the strategy profiles are public and the payoff profiles known. Thus, in this case, trust does not form part of any utility.

Take the following scenario; a service provider divulges private location information (causing a privacy violation) where there is a prohibitive contract is in place. In this case, the individual's utility is made up of a privacy loss (expressed as the individual's associated perceived monetary value) and a recourse value gained $(r - m_i)$. The SP's utility is made up of a divulgence value gained and a recourse value lost $(u - r)$.

In the service offering is bound by a prohibitive contract and $r > u$ then there is a clear affinity towards the SP not revealing (selling) i's personal information. In other words, there is a clear affinity towards a stable operating point. Likewise, if $x_i > r$ it is highly unlikely that i will knowingly be enticed to relinquish private information in order to gain recourse value r.

It is clear that constraints are necessary in the establishment of a prohibitive contract. Indeed, if a prohibitive contract is in place, the utility shown for i and SP respectively should private information be divulged is:

$$(\Delta_i + r - m_i; \Delta_{SP} + u - r) \tag{3}$$

where m_i symbolizes the value that i associates with its private information. m_i, r, and u are considered partial variables, meaning these variables are subjective and influenced by various factors. Finding values for these partial variables, which tend towards a stable operating point, in many cases is only possible after a violation has occurred. However, the conditional constraints for i and SP in the establishment of a prohibitive contract are $r - m_i < 0$ and $u - r < 0$ respectively. If the prohibitive contract acts as a successful prediction then there exists a sufficient deterrent to act. This is possible if the penalties inflicted are equivalent to the compensation for the loss resulting from a privacy violation. In other words, we tend towards an ideal utility for i and SP, $(\Delta_i; \Delta_{SP})$.

In summary, the service provider is prohibited from divulging private location information while the individual is secure in the knowledge that there is a prohibitive contract safeguarding against the possibility of a privacy violation.

3.3 Defining a Privacy Location Prohibitive Contract

We define a prohibitive contract as a strategy profile such that each user is constrained to deviate unilaterally. Thus a prohibitive contract is a *stable operating point* as no user has incentive to change strategy as there is a significant deterrent to do so. More formally, a prohibitive contract is set of strategies with conflicting and competing objectives (S, f) where S is a set of strategy profiles and f is the set of payoff profiles. Strategies in this case are constrained by a recourse value $r^{'}$, where $r^{'}$ is a prediction of the recourse value.

Each player has only one strategy x_i resulting in a global combined strategy profile $x = (x_1, \ldots, x_n)$. In our location privacy example, i's strategy is to protect private information, while SP's strategy is to take profit from the sale of private location information. Thus a strategy profile $x^* \in S$ represents a **prohibitive contract** if:

$$\forall i, x_i \in S_i, x_i \neq x_i^* : f(x_i^*, r_i') \geq f(x_i, r_i') \tag{4}$$

By changing strategy, no player will benefit in any way. In other words, a prohibitive contract is used to dissolve conflicting strategies through recourse constraints. Should a player choose to engage (breach the prohibitive contract), how can the efficiency of the system be determined? Under what circumstance can a prediction of the value of $r^{'}$ ensure efficiency?

4 A Numerical Example

Our example investigates a communications network where a service provider is responsible for a number of users. In this approach, a service provider and user system interaction is itself modeled as a game. Recall that utilitarian theory is concerned with the greatest benefit to the greatest number. We use this approach to measure the cooperation and for evaluating our location privacy system for efficiency.

Apathetic users presents the service provider the opportunity to benefit directly. Taking this into consideration, an efficiency evaluation method can be used in simulating location privacy systems, given the utility of the service provider and utility of all its users. In other words, finding this balance is best described as finding the association between the divulgence and recourse values given different system scenarios. This utility function evaluates system cooperation in the sense that no player benefits at the other's expense and overall system outcome is considered efficient.

4.1 Evaluation

We assume the network service provider values all its users equally and all user's private location information is valued by a NIM. Furthermore, it is assumed that the vast majority of users seek privacy assurance while a small proportion are apathetic towards their private information.

In setting up our numerical example, we choose the most significant factors which may influence a location privacy system. We assign variables influencing our privacy location game as follows:

- u - Divulgence value
- $r^{'}$ - Recourse value

- a - Number of apathetic users where the service provider is likely to sell their information
- b - Number of privacy-seeking users where the service provider is likely to sell their information
- c - Percentage users don't claim the allocated recourse value
- d - Percentage privacy-seeking users defect due to service provider violation
- v - Value of single user to the service provider
- n - Number of users in the system
- α - efficiency value (ideal divulgence to recourse value)

The service provider bases the value of its operation on the number of users and the associated value of each user. The values of a, b, c and d may be determined using sample data from a subset of the population n. The system value is calculated as follows: $SystemValue = v \times n$. In establishing overall system efficiency, the costs incurred must equal incomes received for both the service provider and its users. For the service provider this is expressed using the following equation:

$$\begin{aligned} Income - Expenses &= 0 \\ ((u - r^{'})a) + (ar^{'}c) + ((u - r^{'})b) + (br^{'}c) - (bvd) &= 0 \\ ua - r^{'}a + ar^{'}c + ub - r^{'}b + br^{'}c - bvd &= 0 \end{aligned} \tag{5}$$

For the user this may be expressed as the satisfaction in the knowledge that the maximum possible recourse value (determined using utilitarian theory) is received should a privacy violation occur. In addition, it is generally accepted that the service provider does not benefit from infringing upon privacy.

Through elementary mathematical equation manipulation, the divulgence value for our numerical example is calculated as follows:

$$\begin{aligned} 0 &= ua - r^{'}a + ar^{'}c + ub - r^{'}b + br^{'}c - bvd \\ u(a+b) &= r^{'}a - ar^{'}c + r^{'}b - br^{'}c + bvd \\ &\dots \\ u &= r^{'}(1-c) + \frac{bvd}{a+b} \end{aligned} \tag{6}$$

We define an efficiency value for our system which is the relationship between the divulgence value and the recourse value. This is used in evaluating a location privacy system's efficiency to maintain balance. In our numerical example, the efficiency value showing the ideal divulgence to recourse ratio is shown below:

$$\alpha = (1-c) + \frac{bvd}{r^{'}(a+b)} \tag{7}$$

Both Equation 6 and Equation 7 directly corresponds to the manipulation of the Equation 5 ($Income - Expenses = 0$).

Now that we are able to calculated an efficiency value for our numerical example, let apply this to the following example. Suppose we have a communications environment where there are 1000 (n) users each with a associated value of 10 (v). Assume 10% of the users are apathetic towards their private information and 5% of users who are awarded a recourse value, do not claim the recourse value. Assume the likelihood the service provider is presented with an opportunity to sell private information is 50%. If a privacy-seeking user's information is sold, we assume that 50% of these users will defect to another service provider. This defection is based on insufficient recourse value or due to significant anguish caused by the service provider privacy violation, resulting in the service provider losing system value. We tabulate the values of the given variables and using Equation 7 we calculate the efficiency value such that the system best employs the theory of utilitarianism and the end result is an efficient system. From Table 1, assuming the recourse value ($r^{'}$) is set to 1, the efficiency value (α) calculated is 5.45.

α	a	b	c	d	v	n
5.45	50 (1000x10%x50%)	450 (1000x90%x50%)	5%	50%	10	1000

Table 1: Numerical Example - Calculating the efficiency value

If the service provider sells information, other than at a value of $u = 5.45r^{'}$, then we have a system imbalance which defies the principles of efficiency. Table 2 shows the summed payoff profiles for the service provider and users and the costs incurred by the service provider, given $u = 5.45r^{'}$.

	Apathetic	Privacy-Seeking	Total
User Claim	47.5	427.5	475
SP Claim	225	2025	2250
SP Cost of User Defecting	0	2250	2250

Table 2: Case Study - Income and Expenses

The figures show that the maximum possible recourse value is received by the privacy-seeking users offset against the apathetic users, should a privacy violation occur (in our example this occurs 50% of the time). In addition, the sum of the service provider utility and all its users utilities is zero.

5 Privacy Analysis

If we consider previous location privacy solutions, all exude preventative measured approaches in protecting private information. However, none consider the scenario where a violation does occur and for the consequences and consideration for recourse thereafter. A privacy preserving location system which maintains equilibrium between the competing objectives of the parties is defined by a prohibitive contract which binds both such that no benefit is gained to anyone if violated. In other words, this approach provides a built-in (possibly pre-determined) safety net governed by a utilitarianistic viewpoint. Privacy is enhanced due to the presence of a deterrent to engage in a privacy violation.

6 Conclusion

This paper defines a privacy preserving location based system which maintains equilibrium between the competing objectives of the parties involved in a service-based environment. Through investigating the current location privacy imbalance, we were able to determine constraints necessary to find a suitable equilibrium. This was expressed in the form of a prohibitive contract which either the subscriber or service provider must not violate. If the prohibitive contract, is compromised by one party, the other party is immediately presented with a recourse option.

With a prohibitive contract in place, it is evident that no player should ever move. We investigate a possible scenario where the allure of perceived benefit causes a system imbalance. In our example, we model adversaries through simulation. We adopted the utilitarian paradigm, which provides a means of finding overall system efficiency, where the sum of all utilities is zero. An efficiency function finds the ideal divulgence to recourse ratio for the evaluation of the location privacy system for efficiency.

Acknowledgements

This paper is dedicated in loving memory of Nobuhle.

References

[1] Ardagna C.A., Cremonini M., Damiani E., De Capitani di Vimercati S., Samariti P. (2007) Location Privacy Protection through Obfuscation-based Techniques, ISSA.

[2] Beresford A.R., Stajano F. (2003) Location privacy in pervasive computing, volume 2 46-55.

[3] Mouly M., Pautet M.B. (1992) The GSM System for Mobile Communications, Telecom Publishing, ISBN:0945592159.

[4] Peterson J. (2004) A presence-based GEOPRIV location object format, Web Reference: http://www.ietf.org/internet-drafts/draft-ietf-geopriv-pidf-lo-03.txt.

[5] Marias G.F., Delakouridis C., Kazatzopoulos L., Georgiadis P. (2005) Location Privacy Through Secret Sharing Techniques, WoWMoM '05: Proceedings of the 6th IEEE International Symposium on a World of WirelessMobile and Multimedia Networks, IEEE Computer Society.

[6] Kesdogan D., Reichl P., Junghärtchen K. (1998) Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks, Fifth European Symposium on Research in Computer Security, Springer-Verlag, Louvain-la-Neuve, Belgium 1485 295-312.

[7] Hong J.I., Landay J.A. (2004) An architecture for privacy-sensitive ubiquitous computing, 2nd International Conference on Mobile Systems, Applications and Services, ACM Press, 177189.

[8] Zhong G., Goldberg I., Hengartner U. (2007) Louis, Lester and Pierre: Three Protocols for Location Privacy, Seventh Privacy Enhancing Technologies Symposium (PET 2007), Ottawa, Canada.

[9] Duckham M., Kulik L. (2005) A Formal Model of Obfuscation and Negotiation for Location Privacy, PERVASIVE, LNCS, Springer-Verlag, volume 3468 152-170.

[10] Croft N.J., Olivier M.S. (2004) Using a Trusted Third Party Proxy in achieving GSM Anonymity, South African Telecommunication Network and Applications Conference, SATNAC, Stellenbosch, South Africa.

[11] Croft N.J., Olivier M.S. (2005) Using an approximated one-time pad for securing Short Message Service (SMS), South African Telecommunication Network and Applications Conference, SATNAC, Drakensburg, South Africa.

[12] Croft N.J., Olivier M.S. (2006) Anonymous Mobile Conference Calls, South African Telecommunication Network and Applications Conference, SATNAC, Stellenbosch, South Africa.

[13] Croft N.J., Olivier M.S. (2007) A Silent SMS DoS Attack, South African Telecommunication Network and Applications Conference, SATNAC, Maritius.

[14] Croft N.J., Olivier M.S. (2005) Using compatible keys in achieving subscriber privacy channelling for billing in GSM Networks, INC, Samos, Greece.

[15] Croft N.J. (2003) Secure Interoperations of Wireless Technologies, University of Pretoria, School of Computer Science, Masters Dissertation.

[16] Croft N.J., Olivier M.S. (2005) Codec-Hopping: Secure and Private Voice Communication in Bandwidth Constrained Networks, SecPerU, Workshop on Security an Privacy in Pervasive Ubiquitous Computing, Santorini, Greece.

[17] Croft N.J., Olivier M.S. (2005) A Model for SPAM Prevention in IP Telephone Networks using Anonymous Verifying Authorities, Fifth South African Security Conference, ISSA, Midrand, South Africa.

[18] Croft N.J., Olivier M.S. (2006) Sequenced Release of Privacy Accurate Call Data Record Information in a GSM Forensic Investigation, ISSA, Sandton, South Africa.

[19] Fudenburg D., Tirole J. (1991) Game Theory, MIT Press, Cambridge.

[20] von Neumann J., Morgenstern O. (1980) Theory of Games and Economic Behaviour, Princeton University Press, Princeton.

[21] Laudon K.C. (1996) Markets and Privacy, Communications of the ACM, 39 9 92-104.

[22] Nash J. (1951) Non-Cooperative Games, The Annals of Mathematics, Second Series, volume 54 number 2 286-295.

[23] Mill J. S. (1998) Utilitarianism, edited with an introduction by Roger Crisp, New York: Oxford University Press, Originally published in 1861.

[24] Sidgwick H. (1907) The Methods of Ethics, London: Macmillan, Seventh Edition, First Edition 1874.

[25] Bentham J. (1961) An Introduction to the Principles of Morals and Legislation, Garden City: Doubleday, Originally published in 1789.

[26] Solanas A., Martinez-Balleste A. (2007) Privacy Protection in location-based services through a public-key homomorphism, Lecture Notes in Computer Science (LNCS) EuroPKI '2007 volume 4582 362-368.

[27] Domingo-Ferrer J. (2006) Microaggregation for database and location privacy, Lecture Notes in Computer Science (LNCS) Next Generation Information Technologies and Systems-NGITS '2006, volume 4032 106-116.

[28] Mackey E. (2009) An application of game theory to understanding statistical disclosure events, Joint UNECE/Eurostat Work Session on Statistical Data Confidentiality.