ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Nagata, Junji; Kunishi, Teruo; Idota, Hiroki; Shinohara, Takeshi

Conference Paper

Emerging location based services and its privacy control

23rd European Regional Conference of the International Telecommunications Society (ITS), Vienna, Austria, 1st-4th July, 2012

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Nagata, Junji; Kunishi, Teruo; Idota, Hiroki; Shinohara, Takeshi (2012) : Emerging location based services and its privacy control, 23rd European Regional Conference of the International Telecommunications Society (ITS), Vienna, Austria, 1st-4th July, 2012, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/60352

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

Emerging location based services and its privacy control

Junji Nagata
Otemon Gakuin University
junji.nagata@gmail.com

Teruo Kunishi
GIS Research Institute
kunishi@gissoken.org

Hiroki Idota
Otemon Gakuin University
idota@res.otemon.ac.jp

Takeshi Shinohara
Otemon Gakuin University
takshino@res.otemon.ac.jp

Keywords

GIS, location based service, privacy protection, stealth rights, granularity control

Introduction

Location based technology is one of the fastest developing information technology area. In recent years, Mobile phones are equipped with positioning sensors such as GPS devices. Its accuracy becomes increasingly higher and the cost is decreasing. Location based services are also emerging. One good example are "navigation services" where system guide the user to the destination, or guide the taxi to the place where you are. Manufacturing industry today is shifting toward more service oriented approach such as maintenance services. It is often inevitable to grasp the physical place of the product to provide quick and sufficient maintenance associated the product.

It becomes important issue to protect individual's privacy information in our modern society. Location based information of individual is often critical privacy information because it tells when and where you are or you were. Location information on each device can be also privacy information when the devices are linked to each individual. User receives the full benefit of

location based service in exchange of its own location information necessary for the service. This privacy information are to be accumulated in the service provider and/or platform provider. If privacy information were once accumulated to a certain level, It becomes threat. Concatenation of many privacy information would reveal unanticipated result. And it is difficult for individuals to recognize the consequences beforehand.

Location based information is increasing as the ICT power progress. In fact, accuracy and frequency of the positioning data will increase. The number of equipments will also increase and thus the amount of relevant information will increase very rapidly. That is to say "Information explosion" of location based private information come about. This information is accumulated in the service providers and platform providers. These providers must be trustworthy. However, the privacy information is often leaked in reality and abuse of those information happens in certain level even if maximal attention were to be paid. If certain level of leakage were to occur, "information explosion" of those leakage and abuse would happen in anyway.

Concern for each individual is how to control those accumulations of privacy information and abuse of them. Existing technological and regulatory framework of privacy protection for these issues has its own limits. Recent emergence of new global overwhelmed platform provider other than conventional telecommunication carrier makes this problem even more difficult. To build a sound market for location based service, consumer must feel confidence and new technological and regulatory framework must be build.

Understanding above mentioned background and problem consciousness, following argument are developed in this paper.

1. We propose the metric model for leakage and accumulation of location based privacy information. Each elements consists of the model are identified and degree of increase is also identified. Model shows that degree of increase is the order of exponential.
2. A concept "Stealth rights " is proposed to define the right to control the exposure and provision of one's own location based privacy information.
3. We also propose the model to realize this concept. For this, we also defined granularity of location based information and also proposed system model to implement this concept. In this model, user set up his policy to control service adaptation and granularity of the information necessary for the service. This provides users with the ability to minimize the risk associate with the accumulation of privacy data.
4. We verified the effectiveness of the model by using the above mentioned metrics model and

confirmed the effectiveness. The risk associated the accumulated privacy data can be controlled.

Finally, we overview the problem remained. To establish sound market for location based application and industry, it is inevitable to establish the comprehensive and effective framework for privacy control.

2. The framework for the problem solving

2.1 previous research

The idea of " Anonymity Set" was proposed by Chaum (1988) who is famous for his digital money based on the blind signature technology. This idea has been developed by Pfitzmann (2000) etc. to the following research theme. That is, based on the anonymity of each users, "how could the risk of users to be identified "could be reduced even the service providers collude.
Nakanishi (2005) etc proposed, as a development of this approach, the method to protect anonymity by controlling the granularity of positioning data. These research area reflects the Chaum's philosophy and display academic excellence. But same time does not always fit in the real service situation mainly because many services does not promised on anonymity.

Peterson (2005) propose RFC4119 which controls "to whom", "at where", "when", "the acknowledgement and acceptance" and the "granularity" etc. Natsubori (2006) proposed the method for disclose the location information according to the disclosure policy which are specified according to the set of user's situation and the target to whom the information is disclosed.
Jocha (2004) proposed the schema where service provider define the control of anonymization in addition to the users policy. These research are practical, but does not mentioned total risk where privacy information is accumulated and how to control the situation. This paper attempts to focus these points.

3.2 "right to be stealth" and the framework

The term "stealth " is often used meaning something to spy others. But here " right to be stealth" or " stealth right" is defined as the individual's right not to be monitored his own behavior namely location information. Right to be stealth is considered to be one of

"self-information control right" and provide individual to involvement in collection, use, provision, etc. of his own privacy information. Thus, the stealth right is in the broad sense belongs to the self information control right. (Kunishi, Shinohara).
The framework of the "stealth rights " includes the model where user set up the policy and the Intermediate between control the delivery and granularity between user and location based service provider. The Granularity is defined as information amount calculated by sampling frequency and degree of precision of location information.

First characteristics of our framework is to consider the "explosion of personal data " for location information. Second characteristic of our framework is to propose the "stealth right" as is a right to be unknown individuals' location information. As the third characteristics, we propose the metric model to explain policy and the effect of stealth right.

This model is based on the assumption that,
(1) A certain rate of leakage and ill-use of personal information is unavoidable.
(2) Accumulation of these personal data leakage is proportional to the risk associated.
(3) There exists the threshold that the risk becomes obvious.
(4) We can control the speed of accumulation of personal data and thus control the time period until the risk actualized. And if the period is long enough, the risk will not realize.

4. A proposal of service models

4.1 the trusted third party model

This model set up the intermediary between user and the location based information service provider as is shown in Figure.1.

The intermediary is presumed to be trusted. This model is based on the fact that mobile phone carriers are always monitor the users location and it is the natural assumption that mobile phone carrier becomes the trusted third party.
This model however became not effective anymore for several reasons. Because last few years, terminals have equipped with more capacity and the implementation of HTML5 have progressed. Thus tracking technology which bypasses the carrier became realized and this model is not effective anymore.

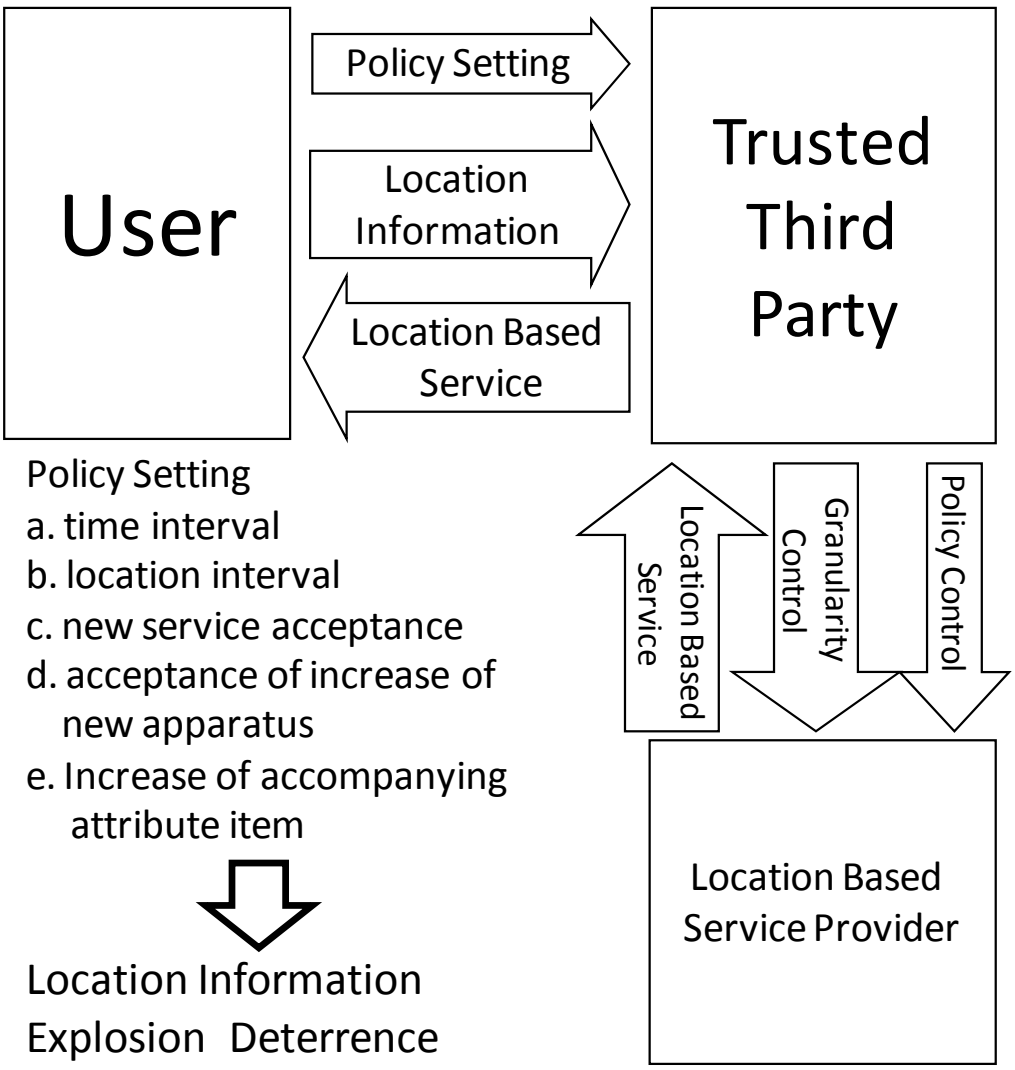


Figure.1

4.2 Local proxy model

In this model set up the local proxy between user and the Location based service provider. The Local proxy monitors and controls the inappropriate acquisition and storage of the information which are the matter of concern caused by HTML5 (Goth, 2011) (Schmidt, 2011)(Ferraro 2011). Implementation model is shown as Figure 2.

Acquired data includes not only location data but also other privacy data for the purpose of data mining.

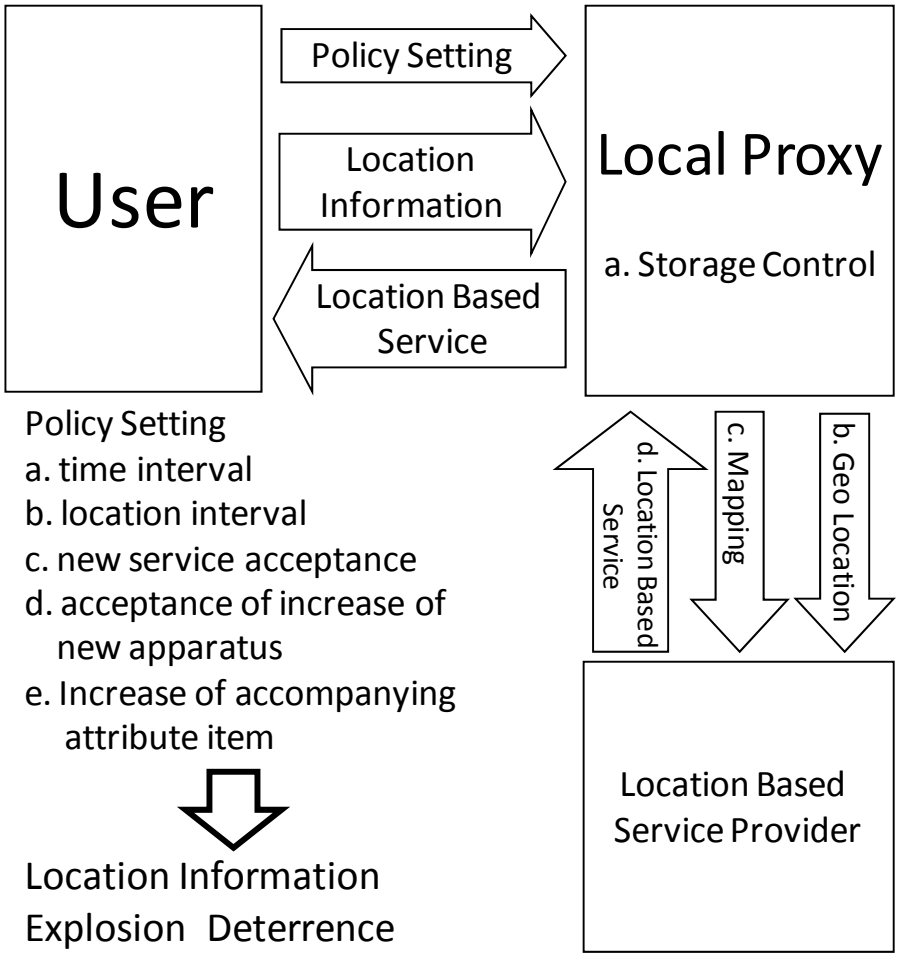


Figure.2 Implementation of Stealth Rights using Local Proxy

The Proxy controls gratuity of location information according to the policy defined by the user as follows.

(1) The User set up policy for provision of location information
   a. Time interval
   b. location interval
   c. new service acceptance
   d. acceptance of increase of new apparatus
   e. increase of accompanying attribute item
(2) User provides location information and requests location based services.
(3) Local proxy controls followings.
   a. Storage (control the information stored)
      1) Session Storage control cookies (include HTML5, Flash)
      2) Local Storage control the local accumulation of data

3) Global Storage control the storage of data to the server
4) Database Storage control the store of data to the database (ex. Web SQL Database API)

b. Geo Location (control reference of location data, GPS, IP address, RFID, Wi-Fi station, Cell phone station, Google Maps JavaScript API , etc.)
c. LBS (control information delivered to the Location-based Service Provider) (Holdener, (2011), Lubbers, (2010))

Above (a) reduce the risk that the information is used for preparation of intended data collections. (b) ,(c),(d) control the granularity of location information before handover to the location-based service providers.

d. Location based service provider provide results to the Local Proxy.
e. Local Proxy provide the service results to the user.

User's policies are defined as follows. The purposes of these policies are to prevent the "Information explosion" related to the location. The factor of the explosion must be identified and controlled.

Chart 1 Policy level

	Policy1	Policy2	Policy3
Allowance	Absolute Value	Fixed Quantity	Fixed Ratio
Approximate Function	Constant	Linear	Exponential
Time Interval	Max Value	Steady Value	Fixed Ratio
Location Interval	Max Value	Steady Value	Fixed Ratio
New Service Acceptance	Don't Allow	Steady Value	Fixed Ratio
Increase Position Acquisition Apparatus	Don't Allow	Steady Value	Fixed Ratio
Increase Accompanying Attribute Item	Don't Allow	Steady Value	Fixed Ratio

Sweeney (2001) empirically analyzed the personal information treated in the public services in U.K. He pointed out that the factors of increase of data are, (1) increase of items collected, (2) data become collected more individually rather than just as a group, (3) more services

emerges which requires personal information in turn.

For these reason, we set up the item " new service acceptance ", "Increase Position acquisition apparatus" and " Increase accompanying attribute item" as factors to be controlled as is shown chart 1. Increase in performance of the equipments leads the factors "Time interval of data acquisition " and " Granularity of the location information acquired"

We also set a policy level as policy1, policy2 and policy3. The contexts of each policy are as follows.

Policy1 intend total volume control which means to limit the personal information to the designated fix volume.

Policy 2 limits the degree of increase not to exceed linear increase.

Policy 3 permits the exponential increase.

To realize these policies, Local Proxy must have the historical data related to the personal data exposure for each user, and controls the disclosure according the policy and the history.

We emphasize that the control of total volume of the location based information is unavoidable to reduce the risk in the "personal data expansion age".

5. Metric model of accumulation of location based information.

5.1 Acquisition of location based information

We define α as a exponential increase ratio, E_0 as a initial accumulated data, and t as time.

Assuming the increase ratio is constant,

$$\frac{df(t)}{dt} = \alpha f(t) \quad \text{.....(1)}$$

Chart 3　　Acquisition of location based information (exponential)

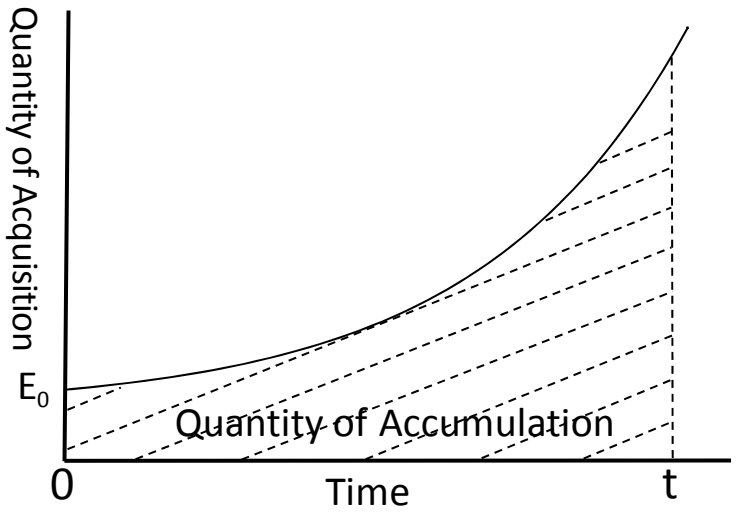


Chart 4　　Acquisition of location based information (linear)

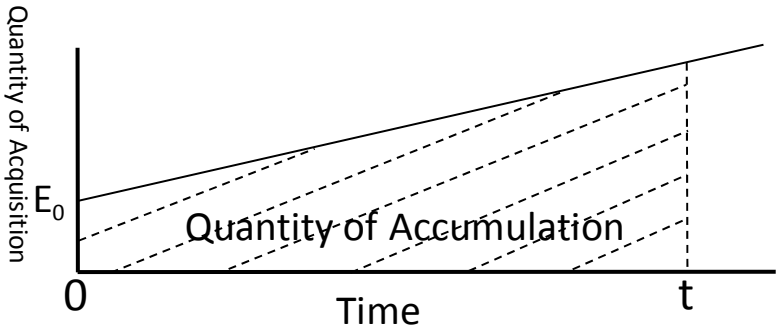
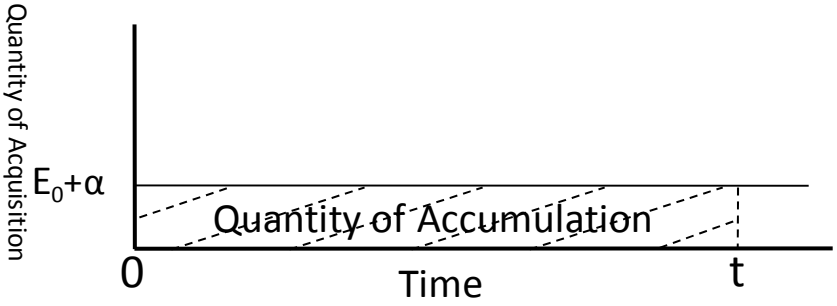
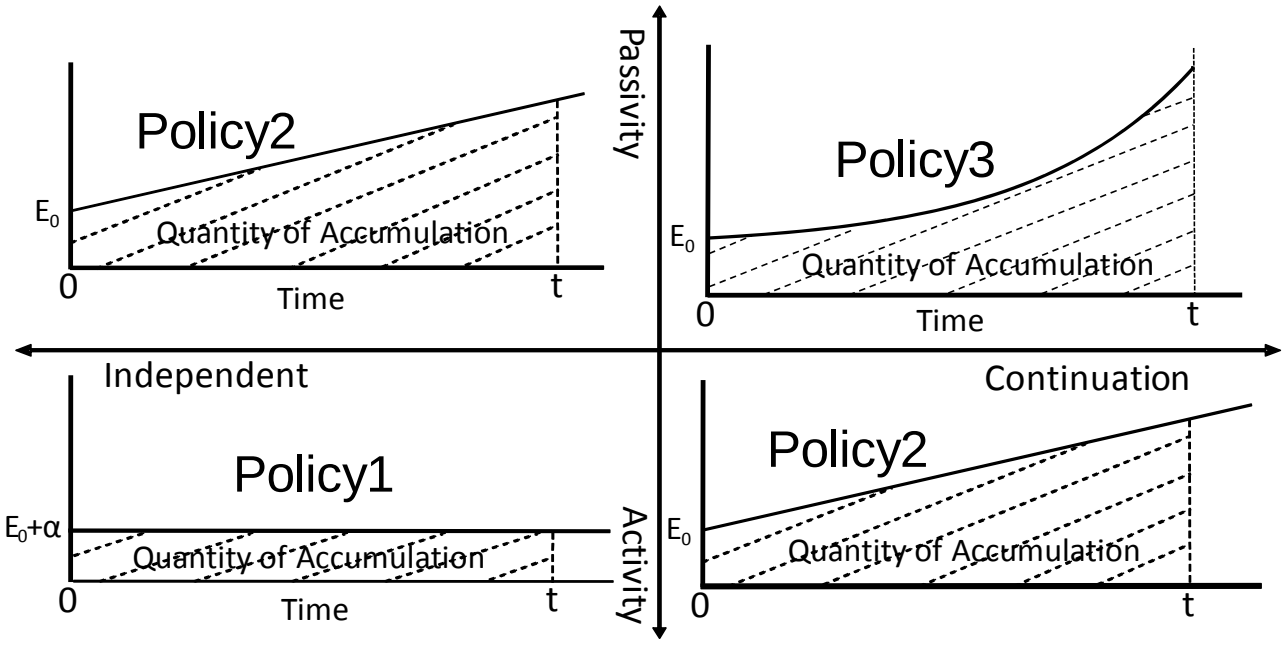


Chart 5　　Acquisition of location based information (constant)



We will position these policies X-Y chart. Where X means independent to continuation, and Y means passive and active.

Chart 6 policy and the increase of acquisition of data



First quadrant is based on the increase of all factors listed. The third quadrant is the most restricted case where the total volume of location information is limited to be constant.

5.2 Estimation of the value of factors

Information explosion ratio is approximately estimated as $e^{0.6t}$ (kunishi 2010)

If we assume the Location based information expand with the same ratio. It also expands as the ratio $e^{0.6t}$ We will divide α into two factors. α_1 represent the factor corresponds to the granularity and α_2 correspond to the acceptance of services.

$$\alpha = \alpha_1 + \alpha_2 \quad (6)$$

α_1 is farther divided into the granularity of time and granularity of space. α_2 is consists of several factors. First one is the increase of convenience due to the increase of new services. Second one is the increase of equipment due to the increase of service providers. And the third one is the increase of data collected associated the new service.

α_1 is caused by the performance of computation capacity.

Moor's law is a experimental rule in computer industry and say twice for 24 months. This leads α_1=0.346

We will assume here both α_1 and α_2 are 0.3 under the rough assumption.

6. The effect of the policy

Policies to realize the stealth right are defined in chart 1. We will visualize the effect of the each policy using the above mentioned metrics model. The results are shown at Fig 7.

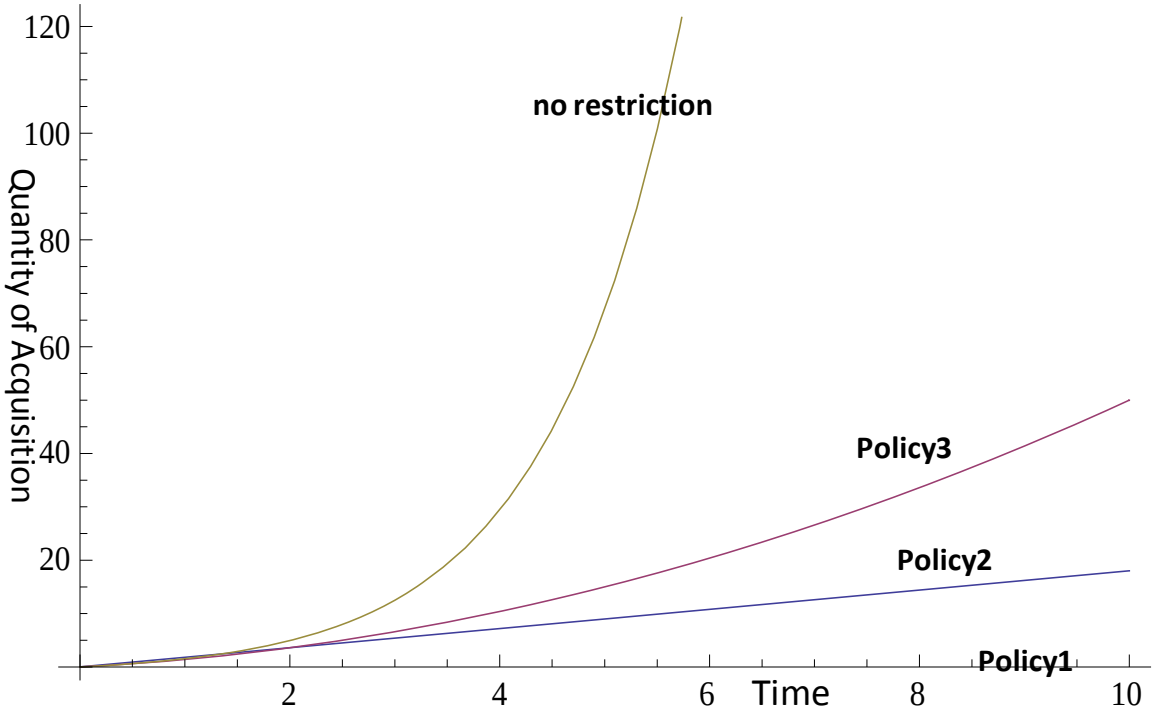


Fig 7 policy and the volume of acquired location based information

Chart 2 shows the policy level and the effect of policy and the values of α_1 and α_2

Chart2 policy and the factor of increase of acquisition of location based information

	Policy1	Policy2	Policy3
Time+Location Interval	α_1=0.003	α_1=0.030	α_1=0.300
New Service Acceptance	α_2=0.003	α_2=0.030	α_2=0.300
Total=α_1+α_2	0.006	0.060	0.600

7. Conclusion

In this research the “stealth rights” are defied and implementation model are also discussed. In this model user can set up own policy and the proxy control the delivery of location based information. Recently implementation of HTML5 is ongoing and appropriate levels of countermeasure are considered in this model. However situation regarding privacy data issue are becoming hot issue. In near future, HTML5 is expected to include more privacy data control mechanism. Then the model we proposed would be more dedicated to the location based information control.

8. References

[1] Kunishi,T., Shinohara.T., (2008a) “Proposal of Stealth-Rights as Right to Control Personal Information in Location Information-Explosion Era” Japan Association for Social Informatics Proceedings of Kansai Branch Study Group 16th, pp.17-23 (in Japanese)

[2] Kunishi,T., Idota,H., Kurome,T., Shinohara.T., (2008b) “ Proposal of Stealth right concerning Location Information in Information Explosion Era” Japan Association for Social Informatics Proceedings of Kansai Branch Study Group 17th,pp.29-36 (in Japanese)

[3] Kunishi,T., Idota,H., Kurome,T., Shinohara.T., (2010) “ An Implementation Method Realizing Self Information Control Rights in Location-Information Explosion Era” Japan Association for Social Informatics Academic journal (2), pp.23-33, 2010-03-31 (in Japanese)

[4] Jocha,T., Hirano,M., Kurokawa,A., (2005) “A privacy-control method for location-based services” Technical Report of IEICE, Information network 103(692), pp.267-270 (in Japanese)

[5] Nakanishi,K., Takashio,K., Tokuda,H., (2005) “A Concept of Location Anonymization” Journal of Information Processing, Vol.46,No.9, pp2260-2268 (in Japanese)

[6] Natsuhori, S., Kawarasaki,M., (2006) “A Study of Location Information Platform realizing Self-Information Control “Technical Report of IEICE, Information network 106(358), pp.43-48 (in Japanese)

[7] EUROPEAN COMMISSION(2010) ”Opinion 2/2010 on online behavioural advertising”, ARTICLE 29 DATA PROTECTION WORKING PARTY

[8] Chaum,D., Fiat, A., Naor, M. (1988) Untraceable electronic cash Proceedings of CRYPTO

[9] Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=EN&guiLanguage=en, Referenced March 13, 2012

[10]EUROPEAN COMMISSION(2012)”on the protection of individuals with regard to the

processing of personal data and on the free movement of such data (General Data Protection Regulation)" Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Brussels, 25.1.2012 COM(2012) 11 final
[11] Federal Trade Commission, Protecting Consumer Privacy in an Era of Consumer Change: A Proposed Framework for Businesses and Policymakers (December,2010)
[12] Ferraro,R., Aktihanoglu,M. (2011) Location-Aware Applications, Manning, pp.214-232
[131 Goth, G. (2011)"Privacy Gets a New Round of Prominence," Internet Computing, IEEE, vol. 15, no. 1, pp. 13-15, 2011.
[14] Holdener III,A.T. (2011) HTML5 Geolocation, O' Reilly,pp47-58
[15] Lubbers, P. (2010)Pro HTML5 Programming Powerful APIs for Richer Internet Application Development, Apress,pp89-90
[16] Lyman, P., Varian, H. R., Dunn, J., Strygin, A. and Searingen, K.(2000) How much information?
http://www2.sims.berkeley.edu/research/projects/how-much-info/how-much-info.pdf , Referenced March 13, 2012
[17] Lyman, P., Varian, H. R., Searingen, K., Charles, P., Good, N., Jordan, L. L. and Pal, J. (2003) How much information? 2003
http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/, Referenced March 13, 2012
[18] Moore, G.E. (1965) Cramming more components onto integrated circuits, Electronics, Volume 38, Number 8, April 19,pp.114-117
[19] Peterson, J.(2005) A Presence-based GEOPRIV Location Object Format RFC4119
http://www.ietf.org/rfc/rfc4079.txt, Referenced March 13, 2012
[20] Pfitzmann,A. Kohntopp, M.(2000)Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology, Lecture Notes in Computer Science 2009, Springer, pp.1-9
[21] Schmidt, M. (2011) HTML5 web security V1.0, December 6th, 2011, Compass Security AG, pp.27-28
http://media.hacking-lab.com/hlnews/HTML5_Web_Security_v1.0.pdf , Referenced March 13, 2012
[22] Sweeney, L. (2001) Information Explosion. Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies, Urban Institute, pp.12-24
[23] Westln,A.F. (1967) Privacy and Freedom Bodley Head, 1970, p7