Date submitted: 03/07/2010

Controversies of the new information environment – kiss goodbye for privacy

Päivikki Karhula
Library of the Finnish Parliament
Helsinki, Finland
E-mail. paivikki.karhula@eduskunta.fi

Meeting: **140. FAIFE with Information Technology**

WORLD LIBRARY AND INFORMATION CONGRESS: 76TH IFLA GENERAL CONFERENCE AND ASSEMBLY
10-15 August 2010, Gothenburg, Sweden
http://www.ifla.org/en/ifla76

Abstract :

The car has traditionally been a symbol of freedom and private space. Where you go is nobody's business. This situation is rapidly changing. Over the next 5 years tracking and monitoring technologies, like black boxes, GPS-tracking devices and remote control tools, will be installed in all new vehicles. These tools enable tracking of drivers' location and route, but also provide capabilities to remotely control certain functions of vehicles.

What this has to do with libraries? Pretty much, actually. Same kind of tracking and monitoring functions may be applied for searching of information or for use of appliances and spaces within a library. Your every move, every item you touch, every site you open and every search you do on the net may be tracked and analyzed. Tracking, locating and remote control capabilities will be embedded into the architecture of the ubiquitous society – and they will create a new information environment.

Restricted access alone is not the major future threat to freedom of information on the net. The core problem lies on a large scale data collection and invisible tracking of users' everyday actions, which may be used later in unexpected contexts. In an increasingly integrated information environment, this set of tools and their data management practices will establish very powerful structures of control – a perfect panopticon on users' data. If these intrusive qualities are not questioned and if no adequate privacy protection solutions will be in place, we will soon kiss goodbye for privacy and witness a gradual erosion of freedom of information.

The new information environment – what it is about?

The new information environment proceeds under different titles – in some context it may be called ubiquitous society, in some other occasions Internet of Things, Smart Planet,

Intelligent Web or Ambient information. All these efforts refer to such large scale technology developments which are in significant extent based on implementation of ubiquitous technologies. Practically, these efforts bring forth data collection of individual objects and persons and their location and enable further integration, sharing and use of this data for different purposes.

Ubiquitous as a term refers to something which "exists in every place and in every thing". Accordingly ubiquitous technologies are used to describe such forms of information processing which is integrated into everyday objects and activities. Adam Greenfield (2006) speaks about “everyware” – which distinctively reveals the immanent character of this information environment. The aim of ubiquitous projects is to spread antennas of technologies everywhere to cover everything and include everyone.

One of the first users of the concept of ubiquitous computing was Marc Weiser (1991), who expected already in early 1990s that computers will be distributed everywhere in a physical space, they will become invisible and they will be able to communicate with each others wirelessly. He also predicted that in this environment, new kind of user interfaces will be developed and they are going to be very different from the text-based interfaces. He called such kind of technologies as ubiquitous computing.

American amusement park, Alton Towers, offers a good small scale example of ubiquitous applications. Their visitors use a wristband with RFID-tag. RFID-tag makes a visitor recognizable for hidden sensors which are installed around in the amusement park. These sensors activate cameras to take photographs of the visitor when he walks around in the amusement park. In the end of his visit, he may buy a CD including photos taken on his path in the amusement park.

Ubiquitous data collection works same way. However, it is less likely, that people who become a target for data collection, will see where this data collection takes place, how this data is stored, linked and shared, and who is going to use data on their activities and for what purposes.

Ubiquitous society

Ubiquitous environment is not only an amusement park – it is a serious business - and it is not limited in small scale projects. Ubiquitous society projects are going on in Japan, South Korea, Singapore, Taiwan and Finland under concepts like U-society, ubiquitous society or smart or intelligent technology projects. These kinds of efforts indicate that ubiquitous technologies will be taken in use as nationwide implementations.

Ubiquitous technologies are used to build a new technological infrastructure into society. This development also seems to set forth reformulation of several laws, rules and principles of society, which go beyond technological changes. These implications are explicitly expressed in ubiquitous society projects.

However, the scale of these efforts is in many sense global – it aims at reaching anywhere, anytime, anyone and anytime. Global dimensions or urge to extend the scale of the projects is reflected in ubiquitous efforts many ways: 1) These efforts are often based on international standards or aim at global compatibility. 2) Their target is in integration or distributed use of data.

Ubiquitous technology projects also tend to extend their depth of data collection and accuracy of user recognition. Accordingly, small scale projects may expand to state or nationwide efforts and some of these projects may have a national or global scale as their goal from their origin.

American crime data integration project describes well how accuracy of data and scale of data collection may extend when the project proceeds (McKay, 2006). A local crime data project extended to state wide project – which now has a global data sharing as a target. Also if new type of ubiquitous data collection approaches like face recognition are integrated into this setting, the project has proceeded far from its' local uses and ways to support crime investigation. As a global application and with extended functionality and increased accuracy, it is going to have a very different kind of social and political impact and context.

Since the implementation process of these technologies is still going on and we have not seen yet wide scale impacts of system integration, data sharing and depth and extensiveness of their data and accuracy of user recognition, their possible uses may not be largely understood yet. However, it is necessary to understand intentions, scalability and possible extensions of ubiquitous projects already from their starting point to be able to estimate their possible impacts.

What does it mean?

How proceeding of ubiquitous society projects is reflected in information environment? They introduce several practices which tend to become commonplace and which support their information architectures including:

- user recognition
- user locationing
- extended data collection
- data integration / distributed access
- "always on" information environment

What does this mean? Your presence, location and actions will be recognized in domestic sphere, at work and on your free time. Transaction data of all these life situations will be collected in increasing extent. Collected data will be stored, linked and shared for third parties to use. And data collection devices are going to be always on.

Identity is going to be a key issue in the ubiquitous environment (Fontana, 2006). Unique identifier is required for personalized and context related services offered by ubiquitous technologies to be able to gather identifying data and to deliver data to the right person. Locating services require user recognition and locating to work efficiently and support navigation or traffic monitoring. Data collection and integration from distributed data sources also requires a key – to link all related data together. Unique identifier may also provide a passage and key to integrate data between and within applications and databases.

This course of development may also have undesired future implications which have been foreseen already in late 1990s by Lawrence Lessig. According to him "identity is going to be an organizing principle of the next generation Internet". He also has expressed his concern about this development by saying that the architecture of identity will fundamentally transform regulability of the Internet. (Lessig, 2006)

New data collection practices seem to change the quality of information processing. What it means in simple terms, is that forced authentication and its' use as a key to integrate user relate data will bring control over the use of internet. Do we see it now? Yes, in certain extent. However, the structures of ubiquitous environment tend to introduce new forms of authentication, set their practices commonplace and in the course of their public adaptation they will minimize space of anonymity.

When new forms of data will be combined and integrated to the previous forms of data they facilitate significant changes in information process. Firstly the amount of information will not only increase, but will multiply. Secondly, these new forms of data and their integration will open up a new sense on information: the integrated views based on transactional data, location data, biological data and historical coverage give completely new kinds of pictures of people's life with accuracy, extensiveness and history.

The scale, intensity and concept of data collection will extend when we proceed towards ubiquitous society. There is already a tendency to extend storage time, coverage and uses of collected data. Good examples of these kinds of developments relate to data retention practices. At first only user recognition data was to be stored and for a relative short period. Now it looks like there are pressures to extend both storage period and include data from the use of search terms in search engines (e.g. 0029-2010, 2010, European parliament, Written declaration 29).

It will become hard to predict possible outcome for a given person from massive, cumulative and integrated data collection and data sharing, since there is a range of possibilities. It is also going to be hard to predict how your profile looks like – especially in relation to others and what kind of consequences this data will have. Altogether, this is a setting which brings forth a range of serious vulnerabilities for us and into whole society.

How it is created?

Ubiquitous information environment is based on integration of several technologies which mainly already exist. These tools include user recognition technologies (RFID, radiofrequency identification) for identifying of persons and things, locating technologies (such as GPS), wireless networks and mobile devices, distributed information systems and rapid and intelligent analysis and distribution tools of data.

RFID is a key technology in the ubiquitous environment creating a basis for user and object recognition and tracking. When RFID-chips are embedded to any object – it becomes as a source (and a target) of communication process. By identifying individuals it becomes possible to deliver personalized data to a certain person - and collect data about a person.

Locating information is another key element of the ubiquitous environment. Personalized and context sensitive services, like navigation tools, require identification, but also locating of an individual person or thing. By combining identification and locating technologies new kinds of services has been developed e.g. as navigation tools - but also for tracking location or routes of people/things.

Data collection extends to new data types. This concerns especially person and object related data, transactional data, location data and environmental data. Data may be collected from the net, as well as from real-life activities. We will see new types of data and their integration to existing information resources. Finally, the ultimate target of data collection is human body.

Adam Greenfield in his presentation has taken up as an example a personal biometric monitoring system. It is a bandage like thing which your body heat activates. It will gather sixteen channels of biometric information and broadcast them to a base station. And a variety of data visualisations are performed on information.

Data integration/data distribution practices may be described as a “data puzzle”, which brings together pieces of data from different sources and enable creation of broader and historical pictures of target person’s behaviour and interests.

Larger and integrated public sector databases or databases intended to distributed use, have been implemented, especially concerning personal data which covers basically whole population, like DNA-databases, fingerprint-databases.

In private sector, personal data has become as a successful product: US. data aggregators like Axciom and ChoisePoint, have databases which cover data of 220 million people – their data may have been collected from private and public sources and data may be sold basically for anyone who is willing to pay for it (Lace, 2005).

The complexity of data integration and distribution methods is also evident: person related data may be sold, shared (e.g. for cross-selling) or exchanged (in public sector there are several international contracts concerning e.g. travellers' data or crime detection data sharing practices).

Analyzing tools for large amounts of data – like data mining have been around already decades, but their intelligence, capacity and speed has changed. New data collection approaches give way to create profiles of target persons/groups, benchmark their data against other persons/groups, apply biographical analysis or predict one’s behaviour – and use integrated personal data frequently on a basis for this. In ubiquitous information environment the capacity of these tools will go far beyond that what we have seen before with intensity we have not experienced before.

Finally, person related data may be used in variety of contexts. It may be available for any party being able to pay for it. Users may include banks, insurance companies, car rental companies or security officials may use the data for checking the credibility of the person. Personal background data can be checked in recruiting or by renting an apartment. Also, there are commercial applications available for surveillance purposes: even to domestic sphere to track children, teens, partner or spouse. And work related and security applications are completely a different story.

New vulnerabilities

Ubiquitous applications are widely marketed as tools of transparency. However, the real picture does not fully support these statements. Within a setting of invisible data collection and uncontrollable data sharing, it is obvious that we become less aware of how our data is collected, how it will be used, who is going to use it and for what purpose. Indeed, ubiquitous data collection practices imply a range of new vulnerabilities for individual people and impose tensions in society.

These structures of ubiquitous society are expected to have deep, far-reaching, longstanding and violent impact on society. Threat of surveillance society is one of the main concerns, since ubiquitous technologies establish structures which can be described as "architecture of

control" or ”architecture of surveillance” (Schermer, 2009). These structures facilitate both very detailed and large-scale perspective of ”super-panopticon” to people's everyday life and activities – and offer extreme capabilities for population control. Their risk potential will extend in relation to their penetration, level of integration and extensiveness and accuracy of the data they cover. In a journey towards global ubiquitous society, panoptical risks and political sensitivity of these tools also will increase.

Ubiquitous data collection, data processing and use of data are mostly invisible processes for the users. Their character as such enables invisible use of power, power transferences and social sorting behind the scenes. Ubiquitous infrastructures will pose a serious threat for democracy if hidden control mechanism and practices take place in a society. In addition, if people lose their means to check when their rights have been violated based on their personal related data and who has done it, their juridical position is weakened.

User recognition and data integration make individuals and minority groups as accurate targets for both beneficial and abusive uses of technologies. The same features which may be useful for targeted advertising and navigation tools may become destructive for minority groups and activists if their political opponents use these facilities to oppress them. Ubiquitous technologies can also misused e.g. for domestic violence to pressure family members or ex-partners or to find out targets for different criminal acts.

Beneficial or abusive uses of these technologies are also strongly dependent on political, economical and religious context. If there are pressures against certain type of opinions or abuse for minority groups is common, these circumstances are likely to become supported with the help of ubiquitous technologies. This has unfortunately been the development path in many countries during penetration of Internet – internet may have increased transparency in some extent, but it has also given way to strengthened censorship and oppression (Kalathil, 2003, Kalathil & Boas, 2003).

Even in democratic countries these tools are likely to change social behaviour and atmosphere in society due to their more intensive control mechanisms. Tools of control constitute both direct discipline and indirect discipline (Schermer, 2009).

Power of direct discipline by using ubiquitous tools is based on tracking, monitoring and analyzing subjects to create a basis for factual consequences and decision making. These conclusions and decisions can define our rights, applicability, access, benefits and restrictions.

Indirect discipline may be described according to Michael Foucault as an internalized impact of surveillance: when subjects are aware that data on their activities is constantly collected, they may alter their behaviour accordingly. This may lead to increased conformity, reduced creativity and unwillingness to express opinions which are not welcomed.

If this kind of social and political atmosphere develops, it may have a detrimental impact on democracy. People may not dare to speak up for themselves, take up social problems or progressive ideas before there is a larger group of people to support their standpoints. Also, within a very target group based information environment, which ubiquitous technologies provide, it may become as a punishment as itself to be labelled as a member of a minority group.

One significant character of ubiquitous technologies is their intrusiveness. Since their data collection tools are often invisible and aim to reach home (smart home), workplaces, traffic, consuming and environment by large, cover activities on the net and on a physical environment, it becomes impossible for any individual to avoid sphere of their influence. They also intrude into intimate areas of life - into social relationships and into the body.

There is no place to hide, as Robert O'Harrow (2005) describes ubiquitous environment. But it is not only question about hiding, but about human rights values and rights which a private space without interference offers: intimacy, nurturing and space for self-reflection and relaxing - all of them very necessary for our wellbeing, development of self and ability to creative acts. Do we have in a future any space for such moments of life which do not need to be broadcasted?

If no limits are set to these data collection practices and their impacts on civil rights are superficially studied, erosion of free speech, privacy, anonymity and self-determination, will be ahead. This development is likely to take place unnoticed and step-by-step, since changes of the information architecture are well on their way.

And how does this relate to libraries?

Libraries are not separate islands in a changing information environment. Structural changes of the information environment are already visible in search and use of information on the net. Some of them also relate to such control tools which regulate access and use of library space and devices.

In search and use of digital information, data collection of user's steps and behaviour on then net and data distribution for third parties has gradually extended. Google, Facebook, Amazon are major sources for information for library users today. Their data collection and data sharing practices and controversial privacy protection principles have raised a lot of discussion (e.g. Fortt, 2010). Library principles of anonymity and privacy do not mainly work within the use of search engines and social media. We should understand it – and let library users also understand their conditions as users of these services.

Ubiquitous data collection practices are likely to take place within library systems, digital libraries, use of e-books and new data sharing practices (”open data”). The questions for libraries are: How open we are going to be with user activity data and user data – and who will decide about it? What ever policies we take, we would better let our users know, what is done with their data?

Just doing a search on the net by ”people search” and ”background data” gives a view how easy it is to dig masses of person related data on any given person in USA, when data protection regulations are not very strict. This example also demonstrates well dangers of open data. It would be valuable for libraries to consider in which respect ”open data” is for good and in which conditions it may not bring forth desirable end-results.

What is user related data in libraries? It may be user data or user activity data. User data is collected to identify a library user. User activity data may cover e.g. loans, used search terms, visited websites, used information resources, pages read, time used for reading or path on a certain page.

What are the key elements in ubiquitous practices which create new vulnerabilities for libraries and their users? User recognition and locating capabilities, tracking of library patron's use of information resources, library devices and spaces as well as sharing of user related data are the major decisions. In ubiquitous setting user recognition will not identify user within a library context alone, but may also become a key element to link user activity data from library in other linked applications. Sharing of user activity data would pose users vulnerable for any undesired searches or misuse of information of their interests and loans.

If libraries push their users into the setting of ubiquitous practices and extend their sense on user behaviour, they easily become partners of ubiquitous surveillance society. Do we want to integrate identifiable data on use of our information resources, services, spaces and devices into structures of control? I hope we wouldn't make these choices - at least without users' consent.

Users' rights

There issues related to users' rights on information which become challenges in a ubiquitous environment. The first concern is right to collect data. Is it possible for anyone to take a Google's street view -like rides with a reader device and gather data in their neighbourhood or in a given area? Even Google's project was not only related to taking pictures, but they also captured data on non-protected WiFi-networks (Paczkowski, 2010). What is the next step of data collection –tours?

The other concern relates to data ownership. In certain countries personal data is in target persons' ownership – in other countries it may be very lightly protected. Controversial policies also concern misuse of data: e.g. in Finland identity theft has not been criminalized.

Invisibility of ubiquitous data collection and processing structures as itself creates favourable conditions for misuse of personal or person related data. Misuse of your data cannot be recognized. User does not normally know what kind of integrated, captured or manipulated data has been used as a basis for decisions. They may not either have a possibility straighten out their faulty interpretations.

Misleading or faulty interpretations may cause significant practical consequences for a given person by regulating his access, applicability, role and benefits or by creating interceptions for him. Practical consequences may also cover identity theft which has already gained epidemic dimensions – in USA alone there was 11 million victims of identity theft in 2009 (IdentityTheftLabs, 2010).

Altogether, access on the net does not alone solve the key problems of ubiquitous environment. It is about collection of our footprints which may be utilized later in any desired form or used as a basis for decisions.

Finally, several questions can be raised concerning library users' rights in a future:
Do libraries support free and anonym search and use of information? Anonymity is already lost and narrowing with a use of many information resources. What about free and anonym use of library space and devices? These questions need to be asked, since the concept of "free access" will change from the perspective of privacy and anonymity in a new information environment? Also, do we have a plan to let our users know that our concept of free access and privacy has changed?

Traditional concept of freedom of information has included ideas of seeking, receiving and producing ideas freely and without inference. IFLA statement on Libraries and Intellectual Freedom (1999) also clarifies conditions of freedom as a right on private and anonym use of information, without a need or force to share information about one's interests and readings. If we want to stay with this concept, we need to understand sensitivity of user activity data sharing, data collection practices and ownership statements within major services we give access to.

How to promote intellectual freedom?

As a last issue, how do we promote intellectual freedom in a changing information environment?
Firstly, it is necessary to understand the threats and possible solutions within ubiquitous environment. It is a prerequisite for being able to recognize problem issues of technologies and their context in present and future information environments.

Secondly, these issues should be taken into public discussion. This already has happened by many civil rights advocacy groups, like Electronic Frontier Foundation (EFF). These groups often have in depth information and educational material about technical and legal concerns and their controversial features, and experience on advocating intellectual freedom and privacy related issues.

It may be possible to impact on functional principles of technologies and their implementation strategies and require that they support privacy protection and regulate or deny involuntary data sharing. Defining data sharing policies for an organization would be one step forward.
And it is possible to support user's abilities to make their own choices with their privacy protection and data sharing practices. This would likely require both staff and user training.

However, users' choices seem to get more limited because several involuntary practices have become commonplace. These include user recognition by using smart cards (*traffic, access, payments*) and locating tools embedded in mobile phones, in GPS-devices and black boxes of vehicles. What can we do about it: use cash, buy an old car, not use mobile phones and use public transportation – these choices are not very practical even today and the space for alternative models is becoming narrower in a future. Altogether, functional practices in ubiquitous environment may be political decisions or individual decisions – and they may turn out to become voluntary, involuntary and risky solutions.

Data collection and data sharing practices in major search engines (*Google*) and social media services (*Facebook*) are mainly contractual. Contracts tend to give one and only choice – you basically need to accept their terms as such if you want to use a service. Service provider may also become owner of your data based on contract.

And there is even less choice within environment of wireless sensor networks - you often do not see their reader devices or related tools, they may activate.

Whatever position libraries take in use in a future, their users' would need in increasing extent strengthened understanding and training about their options in search and use of information. They also would need data protection and privacy protection skills for ubiquitous environment –

Ubiquitous literacy training could include information on data collection and processing principles and on tools and approaches which support privacy protection (e.g. open source – applications, open access information resources, search engines). There are also more specific privacy protection technologies, such as anonymizers and use of encryption, which could be useful in certain circumstances. Often use of privacy protection approaches is not the easiest and most convenient solution for a user. However, there may be conditions, in which these instructions may turn out even life saving.

Supporting users' awareness and training is easiest to do in co-operation with parties with expertise and experience on intellectual freedom issues on the net. These include civil right organizations, data/consumer protection bodies and advocates, technology experts and educational organizations.

Author Michael Chabon puts concerns of privacy of reading nicely together by saying…

"If there is no privacy of thought — which includes implicitly the right to read what one wants, without the approval, consent or knowledge of others — then there is no privacy, period."

I hope privacy of reading will stay valuable also for future libraries.

References

0029-2010 (2010), European parliament, Written declaration: pursuant to Rule 123 of the Rules of Procedure on setting up a European early warning system (EWS) for paedophiles and sex offenders.
http://smile29.eu/doc/DS29_EN.pdf

Fontana, John (2006), Setting the foundation for identity management. NetworkWorld, 03/20/06
http://www.networkworld.com/supp/2006/ndc1/032006-ndc-identity-management.html

Fortt, John (2010), Don't like Facebook's privacy controls? Try anyone else's. Fortune, May 28, 2010.
http://tech.fortune.cnn.com/2010/05/28/dont-like-facebooks-privacy-policy-try-anyone-elses/

Greenfield, Adam (2006), Everyware: the dawning age of ubiquitos computing.
Berkeley, California, New Riders.

IdentityTheftLabs (2010), Identity theft statistics.
http://www.identitytheftlabs.com/identity-theft/identity-theft-statistics-2010/

Kalathil, Shanti (2003), Dot Com for Dictators, Foreign Policy, Marc/April 2003.

Kalathil, Shanti & Boas, Taylor C. (2003), Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule. Washington D.C., Endownment for International Peace, 2003.

Lace, Susanne (ed.) (2005), The glass consumer: life in a surveillance society. Bristol, Policy.

Lessig, Lawrence (2006), Code version 2.0. Basic books, New York.
http://codev2.cc/

McKay, Jim (2006), Completing data puzzle. Government technology, Nov. 6, 2006
http://www.govtech.com/gt/102123

O'Harrow, Robert, Jr. (2005), No place to hide. Free press, New York.
Paczkowski, John (2010), Google Street View Cars Collected Wi-Fi User Data for Three Years.
Digital Daily, 14.5.2010.
http://digitaldaily.allthingsd.com/20100514/google-street-view-cars-collected-wifi-payload-data-for-3-years/

Schermer, Bart (2009), Surveillance and privacy in the ubiquitous network society.
https://openaccess.leidenuniv.nl/bitstream/1887/14394/1/schermerALF.pdf

Weiser, Mark (1991), The Computer for the 21st Century.
http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html