Ville Kumpu

Privacy and the emergence of the "ubiquitous computing society": The struggle over the meaning of "privacy" in the case of the Apple location tracking scandal

ABSTRACT

The article studies negotiation and struggle over the meaning of privacy in the context of the proposed emergence of an "ubiquitous computing society" which refers to a vision of a society where computer technology, in the form of cheap microchips and wireless networks, has been seamlessly integrated into everyday objects and activities. As an illustration of the re-negotiation of the concept of "privacy" that emerges with "ubiquity", the news coverage of the 2011 Apple location tracking scandal was analyzed from a discourse analytical perspective. Employing the concept of a mediated scandal, the articulation of privacy was studied in relation to the media as the site for the cultural negotiation concerning privacy. Two competing discourses concerning privacy were identified. In the relational discourse, privacy was understood as negotiable in the changing conditions that technological development produces. In a fundamental discourse, technological development was articulated in relationship to the fundamental and universal right to privacy. The study suggests two differing understandings of how privacy would be re-negotiated in this process of change as an ubiquitous computing society emerges..

Keywords:
Ubiquitous computing
Ubiquitous society
Journalism
Media
Discourse analysis

1. Introduction

The boundaries and content of what is considered as private vary among cultures, eras and individuals. While different dimensions of privacy (such as bodily, territorial, information or communication privacy) may be recognized and analyzed objective, an all encompassing and final definition is unattainable. Any conception of privacy may achieve a hegemonic position as the dominant horizon for social orientation and action in a given context but this hegemony is never total, there is always some room for resistance. Historically, privacy has been intimately linked to technological development. As the abilities to see, hear, detect and record have been enhanced, the rethinking of attitudes towards privacy has been required and the balance between privacy and disclosure has changed [1], [p. 97]. In 1890 the technical progress in the field of photography prompted two US lawyers, Samuel Warren and Louis Brandeis, to state in one of the first publications advocating privacy in the United States [2] that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops'" [1], [p. 102]. Historically, the focus of privacy has shifted from things that are perceivable directly with one's own eyes and ears (bodily and territorial privacy)

The article presents a case study of the research project *Ubiquitous Computing in News Media*, a collaboration project between Department of Communication at the University of Jyväskylä, Research Centre for Journalism, Media and Communication at the University of Tampere, and Finland Futures Research Centre at the University of Turku. The research project is funded by the Finnish Funding Agency for Technology and Innovation (TEKES).

towards more remote forms of privacy invasion, where privacy violations can occur at a distance. Territorial privacy, the limits on intrusion into the domestic and other environments, is the basis of the earliest definitions, as exemplified in the saying "my home is my castle" which dates back to the eighteenth century. Bodily privacy refers to the protection from unjustified medical tests, experiments or strip searches [1], [p. 104]. With the development of information and communication technologies communication privacy and especially information privacy have become more and more important. Communication privacy refers to securing the privacy of mail, telephones, e-mail and other forms of communication. Information privacy was defined influentially by Alan Westin in his groundbreaking book Privacy and Freedom [3] as "the claim of individuals, groups or institutions to determine themselves when, how, and to what extent information about them is communicated to others".

What visions of ubiquitous computing and ubiquitous society suggest is a profound change in all of the four dimensions of privacy. Ubiquitous computing, that is the integration of information processing in the form of miniature sensors, cheap microchips and wireless networks into everyday objects and activities, is an umbrella term describing currently emerging developments [1], [p. 122]. The ubiquitous society or ubiquitous information society, which is sometimes referred to as being the next phase of an information society [4], is a vision of a society where technology is ubiquitous or "everywhere". The result is that information can be accessed from anywhere, at anytime, by anyone and anything [5] and real-world facts and phenomena can be mapped on a computer with an unprecedented reliability and efficiency [1], [p. 122]. The potential threat of ubiquitous computing to privacy was already noted by Mark Weiser who coined the term ubiquitous computing two decades ago [6], [p. 3]: "In addition to showing some of the ways that computers can find their way invisibly into people's lives, this speculation points out some of the social issues that embodied virtuality will engender. Perhaps key among them is privacy: hundreds of computers in every room, all capable of sensing people near them and linked by high-speed networks, have the potential to make totalitarianism up to now seem like sheerest anarchy." [7]. In terms of privacy, information privacy is the dimension most obviously at stake in the emergence of an ubiquitous society. The digitalization of information about our lives and the ability for computer systems to automatically process it complicates the ability of individuals to determine when, how, and to what extent such information about them is communicated to others. Marc Langheinrich has suggested five aspects that help to explain why this is the case [1], [p. 122–128]. Firstly, the scale of data collection is set to explode as our lives will be covered digitally anywhere and anytime. Secondly, the manner of collection will change as potentially any item in our surroundings can have the capability to collect, process and disseminate data. The level of awareness of any kinds of electronic transactions is set to drop drastically as the technology pervades everyday surroundings and neither data collection nor continuous surveillance activities will have recognizable markers that would indicate the publicity of actions. Thirdly, new data types will emerge as the wide array of new sensors and collection mechanisms will potentially allow the use of "hard" facts (e.g. location, shopping preferences, health data) to infer the kind of gossip or hearsay that has thus far been mostly based on an individual's personal observations (often modified in each retelling). Fourthly, the motivations behind data collection will blur as more and more data is being collected by various kinds of players for various reasons. Context awareness, the enabling of "dumb" systems to predict the user's need and intents without involving any actual intelligence, is one of the main paradigms in ubiquitous computing. The more contextual information is available, the better these kinds of systems are predicted to perform. Thus, to maximize their chances for correctly determining the user's context and intent, future ubiquitous systems could easily attempt to collect all possible information available instead of targeted data collections of specific information for a certain purpose. Finally, the accessibility of data can increase greatly as information can travel quickly around the globe, and modern database management systems allow for the efficient retrieval of minute details out of huge, federated databases from a wide variety of sources. In a world of smart cooperating objects, the freedom of movement for personal information is greatly increased both between humans and computers and between cooperating artifacts [1], [p. 122–128]. While information privacy is the dimension of privacy most profoundly at stake in the transition to an ubiquitous society, it as also important to note that bodily and territorial privacy become highly relevant too because of smart appliances, wearable computers, and activity recognition programs.

This investigation studies the struggle over the meaning of privacy in the context of the suggested emergence of an ubiquitous society. While some have suggested that in such conditions privacy is a social norm of the past and that people are now comfortable sharing information about themselves,[1] the recurrent scandals related to privacy and information and communication technologies[2] suggest otherwise. The existence of such scandals implies that some publicly held values, norms or moral codes have been transgressed [8], [p. 11–30]. From this perspective scandals can be considered as "boundary work" concerning what is considered as a transgression and what is not. While technologies easily cross borders in a globalized market economy, the cultural contexts – and among them the conceptions of privacy – in which the technologies are then situated vary significantly. Thus the boundary work that a scandal manifests is situated in culturally and legislatively diverse terrain. To begin to understand this diversity, this investigation studies the struggle over the meaning of privacy prompted by the emergence of an ubiquitous society not only in the US but also in two

[1] Facebook CEO Mark Zuckerberg being perhaps the most prominent example. See e.g. http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

[2] For a list of scandals see e.g. http://www.networkworld.com/news/2012/012612-privacy-scandals-255357.html.

European countries. At a highly generalized level, the US and Europe differ in the cultural approach towards privacy in the sense that in the US, privacy has been traditionally understood as oriented towards the value of liberty, and particularly towards liberty against the state, while in Europe privacy has been understood as an aspect of dignity concerning rights to respect, personal dignity and informational self-determination [9]. One reflection of these cultural traditions is the legal frameworks concerning privacy at use in the US and in the European Union. In general Europeans trust the government more in guarding their privacy and are less distrustful of government intrusions[3] [11]. In the US the protection against unnecessary government searches or seizures is at the very heart of privacy.[4] The legal framework at use in the European Union member states [12] allows the collection of personal information (e.g. name, address, religious views, and location) only upon explicit "opt in" consent of the affected person under government supervision. This is in direct contrast with the US tradition of "opt out" which requires one to specifically indicate in each and every circumstance that one does not wish personal information to be shared [11]; 9, p. 1193; 1, [p. 116–117]. The need for negotiation that global markets and localized legislation is producing is manifested in the "safe harbor" agreement between the US and the EU that permits US companies that voluntary adhere to the EU principles to continue transborder data transfers with EU member states [13]. While cultural and legislative differences suggested in literature justify the research frame used, this investigation does not aim at explaining the struggle over the meaning of privacy through the differences, or, on the other hand, at corroborating the existence of such differences. Rather, the aim of the article is to validate that there are ongoing negotiations concerning privacy and explore these negotiations in the context of the emergence of the ubiquitous society.

2. Material and method

In this study, one of the recent "privacy scandals" related to information and communication technology, the 2011 Apple location tracking scandal, is studied as an illustration of the struggle over the meaning of privacy in the context of the suggested emergence of an ubiquitous society. To investigate the public negotiation and struggle over the meaning of privacy, research material consisting of the news coverage of the Apple case in four newspapers and one technology-oriented web-publication was gathered (Table 1). The *New York Times* and *Wall Street Journal* were chosen because they are eminent daily newspapers based in the US that have substantial influence in setting the agenda of national politics and public discourse. By circulation, the *Wall Street Journal* is the largest newspaper in the United States while the *New York Times* is the third largest.[5] *Helsingin Sanomat* is the largest daily newspaper in Finland, and the only one that can claim a true national reach. The *Guardian* is a British daily newspaper that was by circulation the eleventh largest newspaper in the UK in 2011.[6] It was selected over papers with wider circulation (e.g. *The Sun*, *Daily Mail*) because of its political relevance and the assumption that with its investments in reporting about new technologies it would cover the Apple case more widely than other newspapers. *Techcrunch* is a technology oriented web publication established in 2005. It is currently ranked third in the Technorati "authority" rankings [14]. According to its own announcement it had over four and half million RSS subscribers in February 2010 making it also a relevant source for public discourse. The newspaper material was collected using the ProQuest database.[7] The research material from *Techcrunch* was collected from the web sites archive.[8] The research material is by no means representative of the range of opinions about privacy in connection to the Apple case in the given contexts but rather it is a sample of influential discourse concerning the issue. Given the nature and limitations of the research material, the aim of this investigation is not to present a comprehensive study of how the privacy dimensions of the Apple case were reported, but rather to use the case in illustrating the negotiation and struggle over the meaning of privacy amidst the emergence of an "ubiquitous society".

Table 1
Research material.

Publication	Stories
Wall Street Journal	16
New York Times	8
The Guardian	3
Helsingin Sanomat	1
TechCrunch	10
Total	38

The research material was analyzed from a discourse analytical perspective which views reality and our knowledge and representations of the world as products of our ways of categorizing the world [15]. All objects are objects of discourse, as their meaning depends upon a socially constructed system of rules and significant differences [15], [p. 3]. This is not to deny the existence of a world external to

[3] According to a June 2011 Special Eurobarometer on attitudes on data protection and electronic identity in the European Union, Europeans trust authorities and institutions clearly more than commercial companies on privacy and data protection issues. Least trusted are Internet companies (e.g. search engines, social networking sites) (22% trusts) and phone companies, mobile phone companies and internet service providers (32%). 70% of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected [10].

[4] Illustrative of the differences are the everyday practices concerning privacy like credit reporting practices in the US [9], [p. 1190–1192] and governments authority to interfere with the christening of children in many European countries [9], [p. 1216–1219].

[5] http://en.wikipedia.org/wiki/List_of_newspapers_in_the_United_States_by_circulation.

[6] http://en.wikipedia.org/wiki/List_of_newspapers_in_the_United_Kingdom_by_circulation.

[7] Only stories published in the actual newspapers were considered, (i.e. no stories published in the web only). All stories mentioning Apple published between April 20th and May 23rd were retrieved and relevant stories then selected.

[8] http://techcrunch.com/2011/04/(April) and http://techcrunch.com/2011/05/(May).

thought but rather to highlight the fact that such a world is unattainable; the objects in the external world cannot constitute themselves as objects outside any discursive conditions of emergence [16], [p. 108]. The aim of discourse analytical research is to study the way in which social practices articulate and contest the discourses that constitute social reality [15], [p. 3]. Articulation is any practice establishing a relationship among signifiers. Discourse is the structured totality resulting from the articulatory practice where meaning is constantly negotiated and constructed [15], [p. 7–9]. The aim of the article is to study how privacy was articulated in the context of the Apple location tracking scandal. To reach this aim, the conceptualizations of privacy were first examined in the context of the claim that the widespread adoption of ubiquitous computing will significantly influence the way we handle personal information and understand privacy. The privacy dimension of the Apple case was then studied in light of the taxonomy of privacy violations suggested by Daniel J. Solove [17,18]. Then through close reading of the research material discourses of fundamental and relational privacy, in which privacy was articulated in relation to different concepts, were identified. Finally, employing concept of scandal suggested by John B. Thompson [8] the articulation of privacy in these discourses was studied in relation to media as the site for the cultural negotiation concerning privacy that the emergence of ubiquitous computing is producing.

3. Apple location tracking scandal as a threat to privacy

From the perspective of ubiquitous computing, location is one of the most important components of user context. The ability to determine a user's location enables a variety of applications to provide services and functionality to the specific location and context. A simple example of a context aware application is an electronic tour guide in a museum or at a historical site that automatically senses which exhibit the user is closest to and presents the appropriate information [19]. While location in itself is a useful and potentially profitable (e.g. for advertisers) information it can also be used to infer additional contextual information: for example, spending time at a gym is indicative of exercising, driving someone every morning to and from work is indicative of a close relationship and moving around certain neighborhoods at certain hours may suggest or can be used to corroborate shady activities [20], [p. 286]. As the scale of location data collection is set to explode, the ability of an individual to determine himself when, how and to what extent information about him is communicated, becomes more and more difficult. As potentially any item in our surroundings can have the capability to collect, process and disseminate data, the ability to prevent others parties from learning one's current or past location (and inferring something from that information) is increasingly difficult. In the case of the Apple location tracking scandal in 2011, researchers Alasdair Allan and Pete Warden found an unencrypted file in iPhones containing a record of the phones past locations. The researchers introduced a simple program that allows anyone to visualize the contents of the file to a map.[9] Apple first declined to comment the issue but later published a press release[10] and claimed the recording of the phones' locations to an encrypted file as being a "bug" that would be fixed. The company also stated that the data did not concern the phone's exact location but rather the locations of Wi-Fi hotspots and cell towers nearby that were tracked to create a crowd-sourced database that speeds up calculating a phone's location.

To understand the dimensions location tracking scandal has in relation to privacy, the privacy taxonomy created by Daniel J. Solove is useful [17,18]. Although the taxonomy of activities that might lead to privacy problems was originally drawn up to aid in discussing legal protections, it is useful for analyzing how a piece of software or technology might be problematic [1] [p. 106]. In the taxonomy, activities that might lead to privacy problems are grouped into four sets: information collection, information processing, information dissemination and invasion. Apart from direct invasions, the location tracking scandal is related to all sets of activities. According to the taxonomy, if information collection is hidden or forced it leads to surveillance or interrogation, which violates the data subject's privacy. In the Apple case the fact that people were not aware that their locations were being recorded and stored was one of the primary concerns. The secrecy of the tracking was explicitly mentioned in the beginning of the first news about the researchers' findings in *New York Times*, *Wall Street Journal* and *Guardian*.

> *Apple faced questions on Wednesday about the security of its iPhone and iPad after a report that the devices regularly record their locations in a hidden file.* (New York Times, April 21st)

> *Security researchers have discovered that Apple's iPhone keeps track of where you go - and saves every detail to a secret file on the device which is copied to the owner's computer when synchronized.* (Guardian, April 21st)

> *Two researchers said they have uncovered a hidden file on Apple Inc. iPhones that keeps a record of where the phone has been and when it was there – a database that is unencrypted and stored by default.* (Wall Street Journal, April 21st)

On the other hand the very idea of surveillance was contested. In the press release Apple claimed that "Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so". Rather than the location of the user, the data collected concerned "maintaining a database of Wi-Fi hotspots and cell towers" around the location and the storing of that data stretching months back in time and the fact that this happened even with location services turned off were bugs. From this perspective, the scandal in the Apple case was more related to the possibility of tracking the location of smart phone users rather than the actual disclosure made by the researchers. On the other hand, Apple did not actually engage in killing the speculation around the issue as it

[9] http://petewarden.github.com/iPhoneTracker/.

[10] http://www.apple.com/pr/library/2011/04/27location_qa.html.

declined to comment on the issue for seven days. Partially because of this, Apple was considered a data holder in the news coverage. However, it was not considered as an agent interested in surveying anyone in particular but rather it was some third party that was imagined to use the data.

According to the Solove's taxonomy, while processing or using the data, a data holder may threaten the data subjects privacy trough aggregation (linking multiple information sources that the data subject may prefer to be separated), identification (connecting particular information or activity to a person), acts of insecurity (a failure to properly protect the stored information that leads to improper access), secondary use (using the collected data for a purpose that was not agreed with the data subject) and exclusion (not letting the data subject know what the data holder has on file about her and how it is used). In the Apple case, the fact that the location file was not encrypted was another major concern which in the news coverage led to speculation about what could happen if the phone got into wrong hands such as an ex-partner in the case of divorce, "predators" stalking children or circumstantial evidence in a criminal case which could lead to unsubstantiated conclusions.

> *Got an angry ex trying to prove that you were seeing someone else while the divorce was still in progress? Hope she doesn't have a backup of your iPhone. Taking it one step further into the creep-zone, this seems like something that could potentially be used as evidence in a criminal case. Just don't ever be in the wrong place at the wrong time ever again, right?* (TechCrunch, April 20th)

Identification and aggregation did not emerge in the coverage as major problems, partly because it was usually agents that had physical access to the phone (and thus knowledge of its owner) that were imagined to misuse the data. Exclusion (and implicitly secondary use) was highlighted when the question of whether Apple had notified its customers about location tracking in its terms of use and whether it was possible to avoid the tracking by not using location based services.

> *Some privacy experts said the issue was not the legality of storing this information but whether Apple was playing fair with its customers. "Collecting this data is not illegal, but it does matter whether or not this is explicitly spelled out in Apple's terms of use," said Christina Gagnier, a lawyer specializing in privacy and copyright. "Apple constantly changes their privacy policy, and it's questionable whether most users are aware this is happening."* (New York Times, April 21st)

In Solove's taxonomy activities that threaten the data subjects privacy in information, dissemination include: a breach of confidentiality (breaking a promise of keeping information confidential), disclosure (the publication of truthful facts that might affect the person's reputation), exposure (revealing private details), increased accessibility (publication of telephone numbers or e-mail addresses, for example), blackmail (threat of disclosing information), appropriation (the use of data subject's identity to serve someone else's interest), distortion (the dissemination of false or misleading information about the data subject). Increased accessibility and a breach of confidentiality were implicated in the fact that the file stored on the phone was unencrypted which also rendered disclosure, exposure, blackmail, appropriation and distortion possible but again Apple was not the agent implicated in the possible misuses of the data.

4. Discourses of fundamental and relational privacy

In the newspaper coverage, privacy was articulated through *relational* and *fundamental* discourses. In the relational discourse, privacy was primarily articulated in relation to technological development that was considered to be the driving force changing the ways in which privacy was understood and in relation to the contracts consumers make with companies. The collection of data concerning all kinds of actions and its use and re-use in different contexts was often considered "part and parcel" of living in a society where computer technology was ubiquitous.

> *Others said the discovery of the hidden file was unlikely to have a major practical impact on privacy and security. "It is more symbolic than anything else," said Tim O'Reilly, a longtime technology pundit and founder of O'Reilly Media. "It is one more sign of how devices are collecting data about us and potentially sharing it with others. This is the future. We have to figure out how to deal with it."* (New York Times, April 21st)

> *Cellphones that collect people's locations are only the tip of the iceberg: Auto makers, insurance companies and even shopping malls are experimenting with new ways to use this kind of data. Location information is emerging as one of the hottest commodities in the tracking industry – the field of companies that are building businesses based on people's data.* (Wall Street Journal, May 10th)

Within the relational discourse, the relativity of privacy was articulated in relation to *data security*, *contracts* or *benefits*. In the first example, privacy was articulated through data security. It was not the existence of the data that was problematic but the fact that it could get in the wrong hands because of lapses in securing the data. In *Helsingin Sanomat* this type of an attitude towards privacy was generalized to be a common denominator of the "internet public".

> *Internet users are not usually that bothered about growing databanks. The argument is similar as when grocery store bonus schemes are considered: as long as the information concerning my groceries or my internet searches is only used by faceless apparatus, it is ok. Why would the engineers working for Google, Facebook or Apple be interested in me, many wonder. [...] The internet public mainly revolts when their own data slips unasked to the reach of neighbors.* (Helsingin Sanomat, April 23rd)

When privacy was articulated in relation to the *contracts* made between service providers and customers, the focal point was on the terms and conditions that the customer had agreed on. In this regard, privacy was articulated in relation to contracts between customers and service providers.

> *However, Apple can legitimately claim that it has permission to collect the data. Near the end of the 15,200-word terms and conditions for its iTunes program is an 86-word paragraph that says: "Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used . . . to improve location-based products and services.* (Guardian, April 21st)

When privacy was articulated as relational to benefits, the economic or more general potential of location data was highlighted.

> *Collecting location data "is a legitimate device that helps businesses offer better services," said Kimon Zorbas, director of the Interactive Advertising Bureau, which represents the online industry. "It's like the IP address on computers, which needs to be processed to see where people are coming from, which is crucially important."* (Wall Street Journal, May 13th)

In opposition to the articulation of privacy as relational was the discourse that considered privacy as a basic right that can be violated even if the data was not used or even if neither the data subject nor the data holder protested.

> *To some privacy advocates, the storing of the data was a clear breach. "The secretive collection of location data crosses the privacy line," said Marc Rotenberg, executive director of the Electronic Privacy Information Center, a privacy policy organization based in Washington. "Apple should know better than to track iPhone users in this way.* (New York Times, April 21st)

Within this discourse privacy was most often articulated in relation to privacy legislation. While the material of the study does not allow broad generalizations, it does in a very limited way suggest that privacy (as articulated through legislation) is more politicized in the US than in Europe. The comments made by The European justice commissioner Viviane Reding concerning location data at the time were reported in relation to the Apple case in *New York Times* and *Wall Street Journal* but not at all in *Helsingin Sanomat* or *The Guardian*. In general, the Apple case also got more extensive coverage in the US newspapers than in *Helsingin Sanomat* or *Guardian*. In the US, there were several stories connecting reactions in domestic politics to the issue.

> ***Europe Leads In Pushing For Privacy Of User Data***
>
> *BRUSSELS – As pressure grows for technology companies like Apple and Google to adjust how their phones and devices gather data, Europe seems to be where the new rules are being determined.* (New York Times, May 4th)
>
> ***Corporate News: EU to Say Location Data Private***
>
> *BRUSSELS – The European Union's top advisory body on online privacy will issue an opinion this month saying that information collected by phone and Internet companies on customer locations must be treated like names, birthdays and other personal data, EU officials say.* (Wall Street Journal, May 13th)

When connected to visions about how ubiquitous computing will develop and how the age of ubiquitous computing is different than earlier eras of modern computing, the discourses identified suggest differing ways in which privacy will be re-negotiated in this process of change. In the discourse where privacy is considered as relational, individual agents and ITC companies are the main agents in defining privacy in a society where computer technology is becoming ubiquitous (and where this development is considered inevitable). This was most obvious in the contract discourse where privacy was articulated in relationship to the responsibility individuals as customers have in making contracts. In the benefit discourse, the benefits such as new and useful services were considered to be the currency in the negotiations between consumers and companies (or economic growth in the case of nation states and privacy regulation). In the data security discourse, the currency was trust in the technology company (or the state) to not misuse the data that is inevitably gathered. In general, the relational discourses suggests that in a society where technology is ubiquitous, privacy will more and more be defined by individuals making contracts, weighing potential loss of privacy against the benefits of useful applications and controlling privacy through the trust they have in different agents. In the discourses where privacy is considered as a basic right, the main agent is the nation state (or some multinational institution such as the EU) that regulates privacy. In the fundamental discourse, technological development and privacy are considered subordinate to the will of the people expressed through democracy and civil society.

5. The Apple location tracking scandal as a scandal

According to John B. Thompson [8] scandal refers to "actions or events involving certain kinds of transgressions which become known to others and are sufficiently serious to elicit public response" [8], [p. 13]. The definition implies five characteristics for a scandal. First and the most obvious one is that a scandal involves actions or events which transgress or contravene values norms or social codes. Here scandal occupies a kind of a "middle ground of impropriety" involving transgressions that are sufficiently serious to elicit the disapproval of others but fall short of the most heinous crimes. Secondly, scandal is a necessarily public affair that involves much more than the actions or events which are its principal focus and more than the values and norms which these actions transgress. According to Thompson [8], the necessary elements constituting a scandal are a degree of public knowledge of the actions or events (concealment, disclosure, rumor), a public of indirect-participants (that is, others than those directly involved) and a process of making public or making visible the actions or events so they become known by others. Thirdly, scandal presupposes some degree of public disapproval, some non-participants must feel (or be represented as feeling) that the transgression was a morally discreditable action. Fourthly, not only disapproval of non-participants but also some form of expression of the disapproval is necessary for a scandal. The immediate and performative response of others is integral to the scandal.

Finally, the damage or loss of reputation is a risk which is always present in a scandal [8], [p. 11–30].

At the very heart of the Apple case was a suspicion that new technologies may be functioning in ways that many would not feel comfortable. The disclosure of a ("hidden") file in iPhones that seemingly holds a record of the phone's past locations was a concrete event that activated this suspicion. This helps to explain why the scandal expanded despite the fact that when studied in detail the Apple case was not a straightforward violation in any sense. The suspicion that new technologies may violate privacy was articulated through the Apple case. What was interesting in the news coverage of the issue was that there was no effort to invoke narratives related to the idea of a "big brother" type of surveillance. The (mis)user of the data, the uses of the data and the individual whose privacy was violated were all ambiguous in the coverage. In addition, there were no easily identifiable victims or culprits. Despite this ambiguity, the suspicion towards new technologies allowed the "scandalization" of the issue. What the Apple case then first and foremost illustrates is that there is a need to negotiate what privacy means in relation to new technologies. If privacy would be a social norm of the past, or if there was no suspicion that new technologies might somehow facilitate violations, there would be no scandal. Although the research material is limited, it tentatively suggests that such a negotiation is more topical in the cultural and legal context of the US compared to Europe. In addition, the Apple case also suggests that the issues related to privacy invasions are changing. In the coverage, no one suspected Apple of collecting the data to be sold or released to organizations or nation states interested in spying on some individual citizens. Technologies for spying are already so mundane that the fact that those in need of such information could spy is no scandal. Rather, the ways in which such data is routinely collected of practically everyone and how this data is used, are the primary ingredients of the Apple scandal.

The mediated nature of most contemporary scandals, that is, they are in varying ways and to some extent, constituted by mediated forms of communication (e.g. disclosure through the media, commentary in the media), was clearly evident in the Apple case. From this perspective, the most interesting dimension in the Apple case was the representations of the public disapproval which are a necessary ingredient in a scandal. In *Helsingin Sanomat* (April 23rd), for example, it was stated that "the findings of the British researchers created a stir in the Internet on Wednesday". The vague reference functioned as evidence of public disapproval and its expressions which in turn legitimized the writing of the story. As is often the case, civic organizations were also used to exemplify the disapproval. From this perspective, scandals can also be interpreted as manufactured by the media. The negative judgments in the press can easily become a self referring discourse, and the extent to which the moral climate generated by it corresponds to the attitudes of the recipients is an open question [8], [p. 68]. Claiming something as scandalous legitimizes the position of the transgression as scandalous. This "media logic" that magnifies things out of proportion or functions as a self-fulfilling prophecy was also commented on in the research material.

> *In that regard, it reminds me a lot of "Antennagate" last year. It was the biggest deal ever. It was the death of the iPhone. It was the end of Apple. …in the press. The reality of the situation was the vast majority of actual consumers didn't give a shit — and rightly so. Apple sold more iPhones than ever last year — by a wide margin. The device is now the source of the majority of revenues for the company.* (TechCrunch, April 27th)

6. Conclusions

The privacy dimensions of the Apple case were more ambiguous than clear. The collection of information was hidden and forced in the sense that users were not aware their location was constantly tracked and data concerning it was stored in a file in their phones which fulfilled the essential elements of surveillance. On the other hand, it was not clear whether this type of surveillance was mentioned at all or clearly enough in the terms and conditions of use, whether anyone misused the data or whether the data concerned the precise location of the phone. The only uncontested violation in the case was related to data security. The file stored was unencrypted and thus it could be accessed by anyone who was aware of it. In the newspaper coverage of the case, this led to speculation of what predators or ex-spouses could do with the data, which is of course deeply paradoxical given the fact that the file was hidden or secret and that this was highlighted at the same time. The location tracking scandal was more of a "lightning rod" through which the lack of trust regarding new technology was highlighted rather than a clear violation of privacy. This lack of trust in relation to privacy is evident for example in the June 2011 Special Eurobarometer on attitudes on data protection and electronic identity in the European Union where the least trusted were internet companies and phone companies, mobile phone companies and internet service providers. In the study, 70 per cent of Europeans were concerned that their personal data held by companies might be used for a purpose other than that for which it was collected [10]. While the recurrent privacy scandals related to technology might be considered symptomatic of this lack of trust, the mediated nature of the scandals that clearly calls for further research. There is no research available on how journalists writing about technology relate themselves to technological development. The ways in which the logic of scandal (i.e. attention legitimizing further attention and the ways in which public disapproval is represented to legitimize the attention given to the issue) govern the coverage of privacy and new technologies also calls for further research.

When studied as an illustration of cultural struggle or negotiation over privacy, the news coverage of the Apple case, pointed to two competing understandings of privacy and technological development. In the relational discourse, privacy was understood as negotiable in the changing conditions that technological development produces. The currencies to be used in these negotiations identified in the coverage were trust, contracts and benefits. In this case, the trust in data security was the primary dimension of privacy. In the second case, privacy was articulated in relation to contracts consumers make companies. In this instance, it was the benefits available (e.g. useful services, social contacts or economical gains) that were represented as a governing privacy. In the fundamental discourse, it was technological development that was articulated as relational to the fundamental and universal right to privacy. Privacy was thus articulated in relation to laws that were represented as guarding privacy that were considered static. The ways in which privacy is negotiated or struggled with will continue to call for further research. In a more extensive study, the existence of cultural and legislative differences could be examined through privacy scandals and the negotiation or struggle over its meaning understood better in the light of these differences.

Privacy issues are one of the most important dimensions in the suggested emergence of ubiquitous society. The study suggests two differing understandings of how privacy would be re-negotiated in this process of change. In the relational discourse or understanding of privacy, it is individual consumers that are controlling the change. The right level of privacy is defined in the markets where consumers trade their privacy for useful or interesting services or other advantages. Here data security is important because it maintains the trust between consumer and service providers concerning the degree if disclosure of an individual consumer. In the fundamental discourse, ubiquitous society is understood as emerging in the supervision of nation state (or some inter-national institution like the EU) that regulates privacy. Finally, what is clear based on the research is that privacy is not just considered a “thing of the past” but is instead vocally re-negotiated in public discourse.

References

[1] Langheinrich Marc. Privacy in ubiquitous computing. In: Krumm John, editor. Ubiquitous computing fundamentals. Boca Raton: Chapman & Hall/CRC Press; 2010. p. 95–160.

[2] Warren, Samuel & Brandeis, Louis. The right to privacy. Harvard Law Review 4:5, p. 193–220.

[3] Westin Alan. Privacy and freedom. New York: Atheneum; 1970.

[4] Mannermaa, Mika. Living in the European ubiquitous society. Journal of Futures Studies.11:4, p. 105–20.

[5] Mannermaa Mika. Jokuveli: elämä ja vaikuttaminen ubiikkiyhteiskunnassa. Helsinki: WSOYpro; 2008.

[6] Want Mark. An introduction to ubiquitous computing. In: Krumm John, editor. Ubiquitous computing fundamentals. Boca Raton: Chapman & Hall/CRC Press; 2010. p. 1–35.

[7] Weiser, Mark. The computer for the 21st century. Scientific American 265:3, p. 94–104.

[8] Thompson John B. Political scandal: power and visibility in the media age. Cambridge: Polity; 2000.

[9] Whitman, James. The two cultures of privacy: dignity versus liberty. The Yale Law Journal 113: 6, p. 1151–222.

[10] Special Eurobarometer 359: Attitudes on data protection and electronic identity in the EU. See http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf [accessed 07.11.11].

[11] Hoofnagle Chris. Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments. Country studies: United States of America. European Commission: General Justice, Freedom and Security. See http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf [accessed 07.11.11].

[12] Directive 95/46/EC. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ: L: 1995: 281: 0031: 005 0: EN: PDF [accessed 07.11.11].

[13] Commission decision 26th July 2000. See http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A32000D0520%3AEN%3AHTML [accessed 07.11.11].

[14] Technorati Top 100 as ranked by “Technorati authority”. See http://technorati.com/blogs/top100/ [accessed 07.11.11].

[15] Howarth David, Stavrakakis Yannis. Introducing discourse theory and political analysis. In: Howarth David, Norval Aletta, Stavrakakis Yannis, editors. Discourse theory and political analysis: identities, hegemonies and social change. Manchester: Manchester University Press; 2000. p. 1–23.

[16] Laclau Ernesto, Mouffe Chantal. Hegemony and socialist strategy: towards a radical democratic politics. London: Verso; 1985.

[17] Solove Daniel J. Understanding privacy. Cambridge: Harvard University Press; 2008.

[18] Solove, Daniel J. A taxonomy of privacy. University of Pennsylvania Law Review 154:3, p. 477–560.

[19] Dey Anid K. Context-aware computing. In: Krumm John, editor. Ubiquitous computing fundamentals. Boca Raton: Chapman & Hall/CRC Press; 2010. p. 321–52.

[20] Varshavsky Alexander, Patel Shwetak. Location in ubiquitous computing. In: Krumm John, editor. Ubiquitous computing fundamentals. Boca Raton: Chapman & Hall/CRC Press; 2010. p. 285–319.