2012

MOBILE PHONES AND USER PERCEPTIONS OF PRIVACY AND SECURITY

Elizabeth Fife
University of Southern California, fife@marshall.usc.edu

Juan Orjuela
Annenberg School of Communications, University of Southern California, jdorjela@gmail.com

MOBILE PHONES AND USER PERCEPTIONS OF PRIVACY AND SECURITY

Elizabeth Fife, Sr. Lecturer, Viterbi School of Engineering & Associate Director, Industry Studies, Institute for Communication Technology Management (CTM), Marshall School of Business, University of Southern California, fife@marshall.usc.edu

Juan Orjuela, Annenberg School of Communications, University of Southern California, CTM Graduate Researcher, jdorjela@gmail.com

Abstract

As smartphones proliferate, new technologies including facial recognition, sensors and Near Field Communications (NFC) are expected to produce everyday services and applications that challenge traditional concepts of individual privacy. The average person as well as the "tech-savvy" mobile phone user may not yet be fully aware of the extent to which privacy and security are relevant to their mobile activities and how comparable it is to personal computer usage. We investigate perceptions and usage of mobile data services with privacy and security sensitivities: social networking, banking/payments and health-related activities to see if there is a relationship to usage behavior. Nationally representative survey data collected in 2011 from two markets: the US and Japan are presented to show demographic and cultural differences.

Keywords: mobile phone, privacy, security, m-commerce.

1 Introduction: Privacy and security perceptions and current risks on the mobile Internet

As people have come to relish the convenience, immediacy, enjoyment, and possibilities of online shopping, the gathering of health-info and social networking, the volume and frequency of these activities has grown rapidly. Much of the debate surrounding unintended consequences of this activity: namely breaches of personal identity, financial risks, and negative consequences of personal information becoming public is countered by continued growth in "risk-sensitive" activities involving money, health, location and personal identity. If people were truly afraid of what might happen when they volunteer personal information "in exchange" for an online service, the argument goes, they would not make this trade. Thus, many of the mobile services that are predicted to have potential future value, include social media, location based services, mobile commerce and healthcare are at the moment based on the continued willingness of customer's to opt in to the trade-off. Given that most people probably do not understand exactly what is done with their personal information and the potential consequences, the situation is complex and changing.

Definitions of online privacy have emerged from concepts discussed over the past two hundred years in conjunction with other technologies seen to threaten private life, beginning with possible privacy threats posed by newspapers and cameras (Warren & Brandeis, 1890). Perspectives of what constitutes privacy have changed through the years, particularly as a result of information and communication technologies (Lee, 2007). Privacy is generally defined as the right to control access to one's person and to personal information about oneself with the implication that consent is a part of the equation (Hartmann, 2011). The advent of the Internet has brought in the topic of intrusion as an added dimension of privacy and the topic of surveillance as well is considered an additional category in definitional boundaries of privacy (Lee, 2000). Increasingly, however the central issue in online privacy discussions is the collection, transfer and reuse of personal information and the individual's control of their information after it has been received by others (Lee, 2000, 2007, Lin & Atkin, 2007). The growth of computer databases and possible misuse of information is seen as the central threat to individual privacy in the modern age (Wu, Lau, et.al 2011). Daniel Solove characterizes privacy issues in cyberspace today in Kafkaesque terms in that many people know that their information is held by unseen entities but they have no control over how the information is used. In addition, much of the information that is passed to databases is not necessarily sensitive information, but concerns daily activities, preferences and hobbies (Kaplan, 2001). Whether this is a problem, or how exactly third parties profit from this kind of information is not generally clear to the average person. Granting consent in the mobile world is apparently difficult, given the need for unobtrusiveness as a design choice. Users will necessarily be unaware of possible privacy breaches, although this wasn't necessarily intended (Beckwith, 2003).

The mobile device and mobile Internet present a new platform of uncertainty for the user in terms of understanding how their personal information may be transmitted to marketers, other companies and institutions. The mobile context and social media and location based services present added privacy issues. Facebook for instance has offered a service called "Deals," allowing local businesses to offer promotions; based on the user's location. The privacy implications were not clearly presented to potential users (Hartmann, 2011). This example illustrates how individual responsibility is a core issue in the current mobile environment. While users may have some apprehension that their privacy has been might be diminished when using their mobile phone, the full picture is not apparent.

The *Wall Street Journal* carried out a study of apps available for Android and the iPhone platform finding that the majority in fact, collect personal information ranging from age, gender and location to phone identifiers which is sent to other companies without the user's knowledge or consent (Thurm, 2010). It is difficult if not impossible for smartphone users to stop being tracked as they can on computers by deleting or blocking "cookies" which are small files that track use. Many apps included in the *WSJ* study did not offer written privacy policies at the time they were tested. The piece of

information most often shared was the unique ID number assigned to each phone which cannot be deleted. Overall, standard practices for handling information do not yet exist; neither Google nor Apple requires permission to access some forms of the device ID or to send it to outsiders. Assembling this information into profiles of mobile phone users is a burgeoning area, and developers are often encouraged to release more data about customers. Some ad networks provide "kits" that insert ads into an app or track where users spend their time in the app itself. From the *Wall St. Journal* test apps, Google was the largest recipient of data through its companies like AdMob, AdSense, Analytics and Doubleclick. Apple uses knowledge about its users gained through iTunes and its App Store and includes the kind of music and video a person uses and apps that are downloaded. There are signs that Apple is targeting people more intensively through social-networking sites such as Ping, a service within iTunes that lets users share music choices with friends (Thurm, 2010).

The debate around privacy/security and online services often focuses on the trade-offs that users make when they decide that they want something like information, entertainment or discounts and make the decision to supply personal information in return for value or access to services. Eric Schmidt, CEO of Google has phrased it in terms of a line that should not be crossed; the use of facial recognition and real-time tracking are two examples. He has said, "What we have learned is that people disagree on where that line is..." (2012, Kapko). A reluctance to pay for electronic services and content, present in the mobile as well as the online world suggests a degree of willingness on the part of the consumer to provide personal information as the cost of doing business; at least for some kinds of services like music and other entertainment. Downloads of free apps, which for the most part have unclear policies and privacy protections are used more frequently and downloaded more often than apps that require payment. From all apps downloads on Android, nearly 100% are free which compares with around 92% of iPhone apps in December 2011 (Cutler, 2011).

1.1 Literature Review: Factors governing decision making to use mobile devices for transactions, social interactions and other activities that suggest a level of risk

The dimensions of privacy and definitions vary across disciplines, but at their core, most acknowledge the role of the individual in controlling access to their own information as central (DeCew, 1997, Laufer and Wolfe, 1977, & Lee, 2007). The theft or misuse of personal information is the basis of discussions of online privacy given the value that this data has when collected, mined, categorized and shared (Wu, 2011). A growing literature on information privacy and its diminishment resulting from information and communications technologies (ICTs) exists that analyzes how people make decisions about revealing their personal data. An individual's concept of privacy is changeable depending on the benefit they expect to return for revealing their information. This privacy "calculus," essentially a cost-benefit analysis has been used to help explain how users balance decisions to adopt and use technologies. For example, Gupta (2011) et. al. study the privacy balance with utility and adoption of location-based services (factoring in other conditions such as how easy it is to use the service, how well it performs, and other facilitating conditions that have been examined and modeled in other research. They find that adoption models need to consider the role of this "negative utility" as a factor for usage behavior. Gupta, et. al's study found that privacy concerns did influence use of LBS services, but varied depending on the type of LBS, suggesting that the degree of control an individual had was important. Other factors like cost, quality of the service and dependability are other factors that need factoring in to the complete equation (Gupta, et.al, 2011).

1.2 Perceptions of privacy and security: cultural differences

Although all cultures share at least a minimal conception of personal privacy, there is no coherent global conception of privacy. What is considered personal information that should not be passed along in one culture may be completely acceptable in another (Mizutani, et. al., 2004). Communications technologies like the Internet and mobile devices have created new situations that specific traditional cultural norms may not be able to accommodate.

Comparing US and Japanese cultures, the practices surrounding privacy are different, in large part due to the emphasis on the individual in the US vs. the importance of group association in Japanese life. As conceptions of privacy are often associated with individualism rather than group loyalty, it is sometimes assumed that there are fewer concerns about privacy in Japanese culture (Mitzutani, et. al., 2004). Public baths, the construction materials of Japanese homes that include thin walls that are opened during the day are examples that suggest minimal privacy. The connotations of "public" and "private" are different in Japanese culture relative to the U.S. with individual private concerns considered subordinate to the public domain (Hayashi, 2012). However, similar to the U.S., Japanese also have privacy customs and restrictions on access to places, people and objects; fundamental situations that define privacy (Moor 1997). Because the privacy of an individual will be considered to be protected within a group, in addition to other subtleties of practice, there may in the end be less protection in terms of regulation and protection for new situations like the Internet and mobile devices (Mitzutani, et.al, 2004). In terms of individual perception of privacy and security when using electronic networks, both U.S. and Japanese users face a similar situation of not being able to see definitively how their personal information is collected and perhaps aggregated and who has access to this data. Thus, attitudes are difficult to measure until awareness of consequences is apparent. In terms of the "road map" for mobile services and privacy, areas needing attention have been identified, including raising users' awareness and finding ways to automate an adaptive means to address privacy preferences for people using mobile services (Wishart, et.al., 2012).

1.2 Hypotheses:

We analyze the survey data to address the following hypotheses:

1. Users with the highest degree of privacy/security concerns will also have the greatest sensitivity to using services that make them vulnerable.

2. Users with the least degree of concern will have the greater confidence in using services that could also risk privacy and security breaches.

3. Users with greater experience with mobile services will also have more understanding of privacy/security issues and thus confidence (higher frequency of usage) compared to those with less experience.

4. Users with less experience accessing mobile services will have less understanding of privacy/security issues and thus more difficulty making a cost-benefit calculation which will result in lower use.

2 Methodology - Global Mobile Survey

The data presented here is based on analysis from a nationally representative survey of US smartphone users and Japanese users carried out in June 2011. This effort was part of a global project called the Global Mobile Survey (GMS) a loosely organized consortium of universities and research entities that has collected survey-based data on mobile users in Europe, the US and Asia over the past 8 years using a standard survey instrument. The US survey is a representative sample of the population by age, gender, education level and income and is carried out online. The sample size was 1,114 and all respondents were smartphone users. The Japanese survey data was collected in August 2011 with a sample size of 2,000 respondents. Distribution of the respondents corresponds to national population statistics for population, age and gender. We thank the Japanese members of the GMS group, (Yoshihisa Takada, Keio University, and Ichiro Kawamura and Yoshiharu Fujita, Institute for Information and Communications Policy (IICP), Ministry of Internal Affairs and Communications) for their 2011 data collection efforts.

3 Results

Survey questions were asked to gauge the respondent's level of concern about privacy and security when using mobile applications and services for financial transactions, health-related activities and overall general perceptions of this issue. A series of statements were ranked on a five point scale gauging high to low levels of concern. We use a sample in which we have users with both the highest and the least degree of concern about privacy/security on mobile devices.

Table 1 below shows the first question that is examined:

Table 1. Global Mobile Survey Question: To what extent do you generally agree with the following statements about your use of the mobile Internet and your privacy?

Question
1 I'm worried about companies having access to my profile
2 I'm worried that my information can be more easily accessed by others through a mobile device than other means
3 I'm worried about the privacy of my health records if I were to use mobile health applications
4 Sharing my health information on my social network is not a concern
5 Privacy issues and my mobile data activities are not a concern
6 Making transactions on my mobile phone is not a concern
7 I'm more comfortable using my computer for things involving my personal information than using my cell phone

The first four statements reflect a high degree of privacy/security concerns on mobile devices; the last three show a low degree.

Table 2. Global Mobile Survey Question: To what extent are you concerned about the following security issues when using your cell phone to make financial transactions?

Questions
1 my financial information could be vulnerable
2 I'm concerned about losing money if something goes wrong during a transaction
3 I would be confortable using my cell phone as a payment tool
4 I would be interested in paying for things with my cell phone only if there was a benefit like price cuts
5 I would use my phone to scan and pay for goods if it made store check out faster

The first two statements reflect a high degree of privacy/security concerns on mobile devices; the last three show a low degree of concern.

We look at demographic variables including age, education and income to measure the different degrees of concern of these groups. We then compare the privacy/security questions to use of different mobile services. First the results are compared to three key demographic variables: age, income and education level. Next we analyze the degree of privacy/security concerns with high usage (daily or more) of various means of accessing the Internet services, ranging from the most simple and frequently used method: email to the more sophisticated, connecting remotely such as through a VPN. These access methods are listed in Table 3 below:

Table 3. Global Mobile Survey Question: How often do you access the Internet from your cell phone in the ways that are listed below?

Questions
1 Communication by email (e.g. Outlook, Hotmail, Yahoo, Gmail)
2 Communication by other means (e.g. Twitter, chat, MMS, blogging)
3 Communication by SMS or IP telephony (e.g. Skype)
4 Synching my device or updating an app
5 Sharing or exchanging files by any means

6 Streaming media content: TV, radio, video
7 Playing online games
8 Using my cell phone as a mobile hotspot to tether other devices to the Internet
9 Connecting from a remote site to my office or home computer, including use of a VPN

Finally, we look at high usage (weekly or more) of m-commerce services. These services are listed in Table 4 below:

Table 3. Global Mobile Survey Question: How often do you access the Internet from your cell phone in the ways that are listed below?

Questions
1 Downloaded free apps
2 Purchased apps
3 Bought or ordered physical goods
4 Performed an online banking activity
5 Made reservations (e.g. movie, bus train)
6 Checked stock info
7 Used a coupon

3.1 Privacy/security concerns and demographic variables

The first result shown below in Figure (1) is the age breakdown issues surrounding privacy for US respondents.

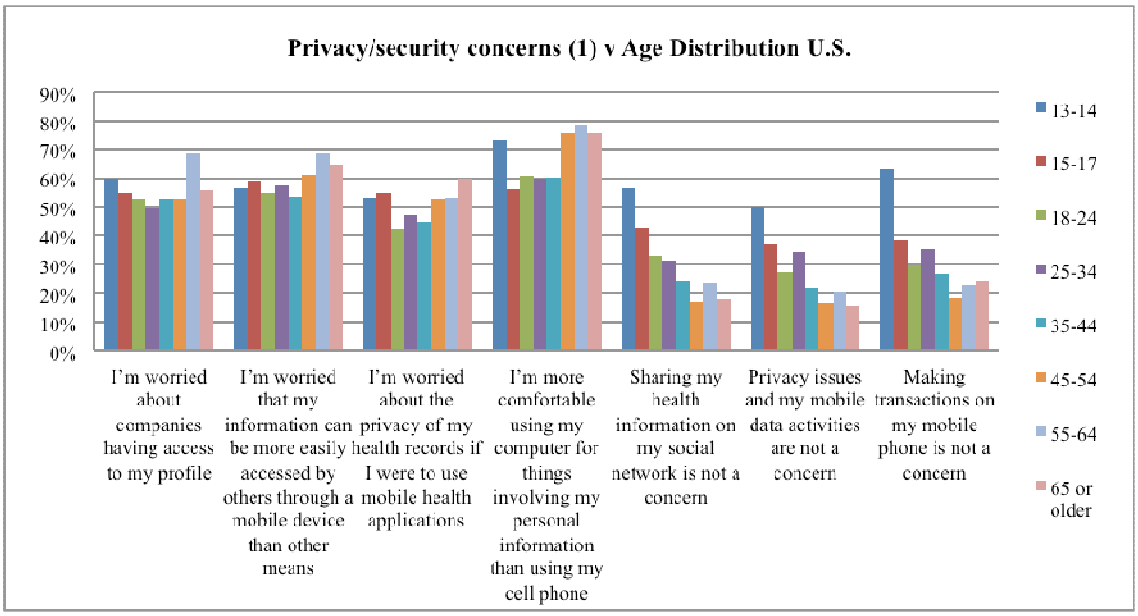

Figure 1. Age breakdown of survey responses for privacy/security (1) related to mobile online activities for the U.S.

We observe that for the first four statements with users older than 18, as age increases the proportion of users with a high degree of privacy/security concern also increases. Viewing the last three statements which describe a low degree of concern, as age increases there is less agreement. These results show that as age increases the proportion of users with high degree of concern also increases. This could be expected as people in higher age demographics tend to have less experience with mobile

services and therefore perhaps less understanding of the associated privacy/security issues and more apprehension. This finding is consistent with other studies that have found that adults over the age of 55 tend to have higher sensitivity to privacy and security concerns in an online environment (Quinn, 2010)

The exception to this analysis is users under 18 years old, who seem to have at the same time high and low degrees of privacy/security concerns. This result might be explained by a lack of understanding of privacy/security issues on mobile devices leading to inconsistent results.

Looking at the results for Figure (2) below we see the percentage of respondents for each age group asked about the extent to which they agree with the following statements about their use of the mobile Internet and their privacy. We observe that for the first four statements which refer to a high degree of concern, the results are similar to the U.S.; as age increases the proportion of users with a high degree of privacy/security concerns increases. On the other hand, with the low degree of concern statements, as age increases the extent of agreement decreases except for respondents older than 65 who seem to have a higher proportion of low level concern. These results show that as age increases the proportion of users with high degree of concern increases and similarly users with low degree of concern decrease. Again, this is expected as older people tend to have less experience accessing mobile services and therefore perhaps less understanding or focus on privacy/security issues. A notable exception again users older than 65, who seem to have even less concern than some younger age groups.

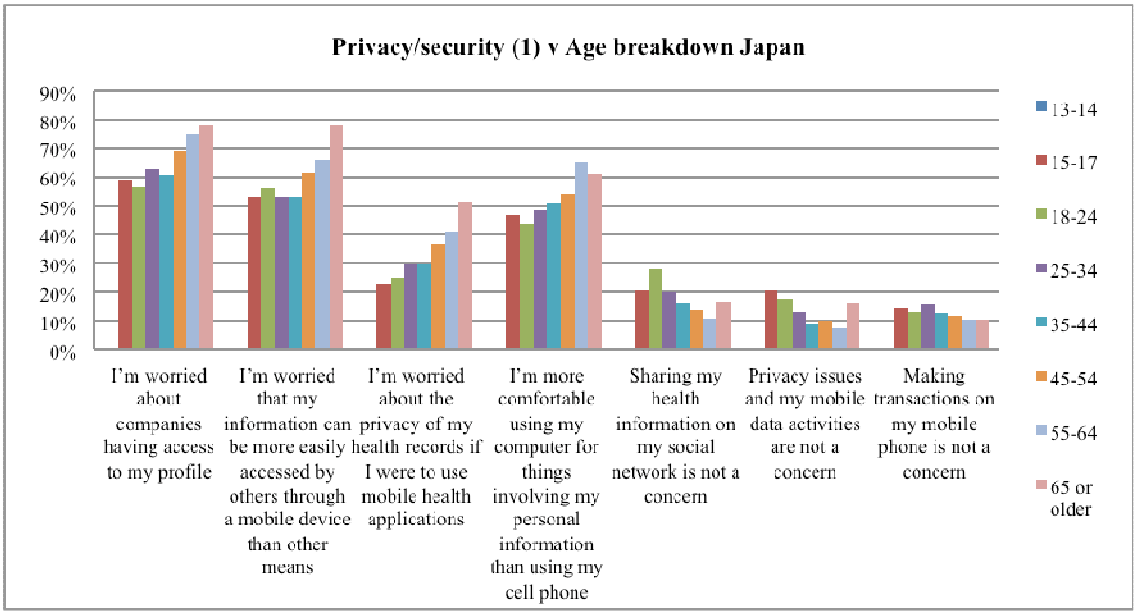

Figure 2. Age breakdown of survey responses for privacy/security (1) on related mobile online activities for Japan.

Overall, more than half of the respondents are worried about companies having access to their profiles (at least 50% of every age group). Additionally, at least 50% of every age demographic have the impression that their information can be more easily accessed by others on a mobile device than by other means. This is an interesting finding given that there are generally far fewer reports about people's information being taken from a mobile device (other than when the device itself is taken without permission) relative to other means ranging from online to physical mail. Surprisingly, unauthorized access to personal health information, which many consider to qualify as sensitive, does not appear to be as great an issue, although degree of concern clearly increases by age.

The next relationship of interest is *privacy/security (1)* versus income distribution. For the U.S. Figure 3 shows the relationship. It can be seen that for those with the highest degree of concern there isn't any

specific trend except for respondents with income over $150,000 a group that seems to have a higher percentage of users with concern than the other income groups. For the low degree concern statements both the people with the lowest income (lower than $15,000) and the highest income have a higher proportion of users with low degree of concern than the other groups.

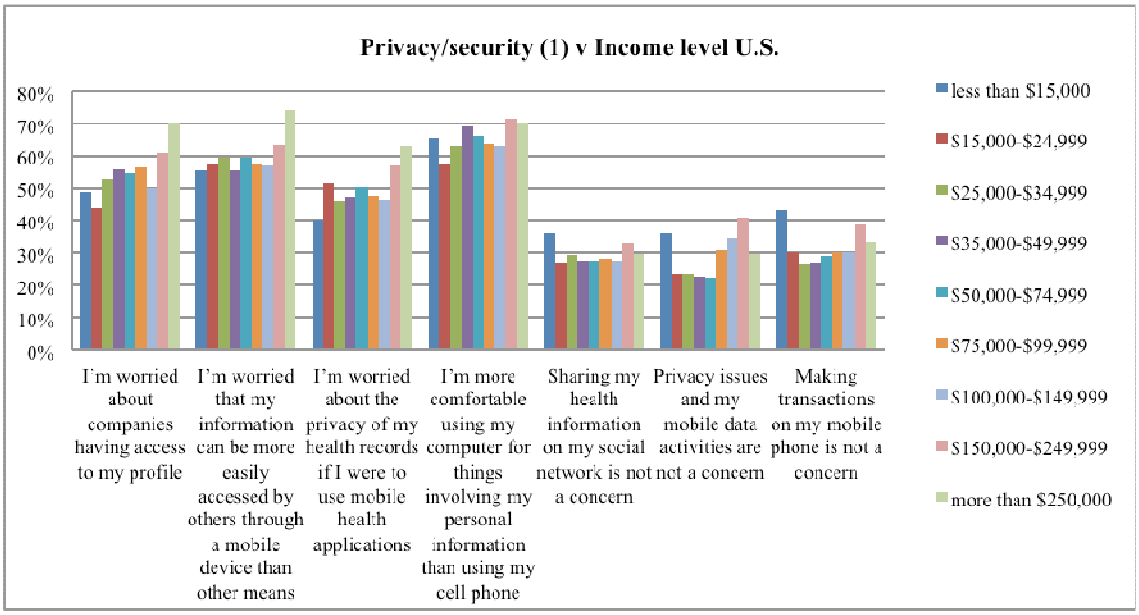

Figure 3. *Income breakdown of survey responses for privacy/security (1) on related mobile online activities for the U.S.*

Now we turn to the income level breakdown for Japan. Below Figure 4 shows the income level breakdown of users for the *privacy/security question (1)*. In terms of a high degree of concern there isn't any specific trend except for respondents with incomes over $150,000 who seem to have a higher percentage of users with a high degree of concern compared to other income groups. For the low degree of concern statements, there is a definite trend.

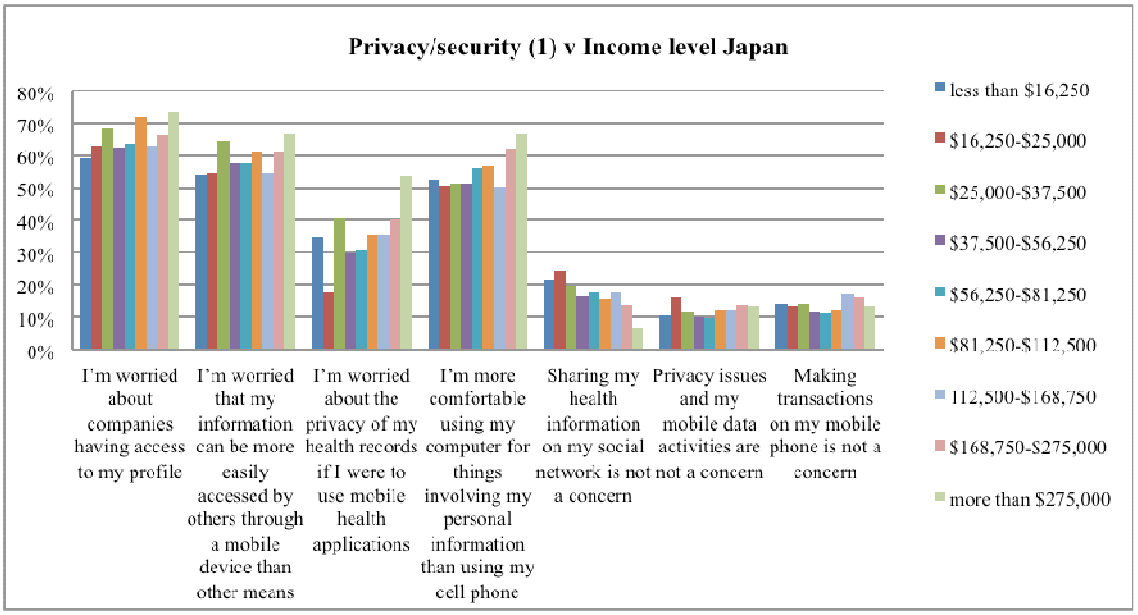

Figure 4. *Income breakdown of survey responses for privacy/security (1) on related mobile online activities for Japan.*

Finally, we compare the *privacy/security (1)* question with level of education. For the U.S. there isn't any definitive trend for the statements reflecting a high degree of concern. For the low degree statements, the only visible pattern is the proportional increase for the lowest levels of education. On the other hand, the Japanese respondents show a clear pattern of increased concern corresponding to higher educational attainment. For the low degree of concern statements, there isn't a specific trend.

Overall, a similarity is seen between Japanese and US respondents in their degree of concern about privacy and security relative to age and income. However, even though, the trend is similar, there is an important difference: for the U.S. there is a higher general proportion of users with low degree of concern than in Japan.

3.2 Privacy/security concerns and Internet service use /access and m-commerce

Next, we examine Internet service usage/access and m-commerce. This analysis uses responses that were highest on the scale for Internet service use/access (daily or more) and highest for M-commerce activity (weekly or more). First we look at high use/access to Internet services and *privacy/security (1)* in Figure 5. This figure shows the privacy/security perspective of respondents with high levels of access/use of Internet access/services. For almost all the items listed, the proportion of users is high in agreeing or strongly agreeing with the statements related to a high degree of privacy/security concerns. Also, it is important to note that for almost all the Internet services the proportion of users with a high degree of privacy/security concern is more than 50%. It is also significant that for more advanced services like playing online games, tethering or using a VPN, the proportion of users with a lower degree of privacy/security concerns increases, but this proportion is still slightly lower than that of high concern. This is unexpected as we anticipated that frequent use of more advanced methods of mobile Internet access and services would reflect a greater comfort level with mobile security and privacy.

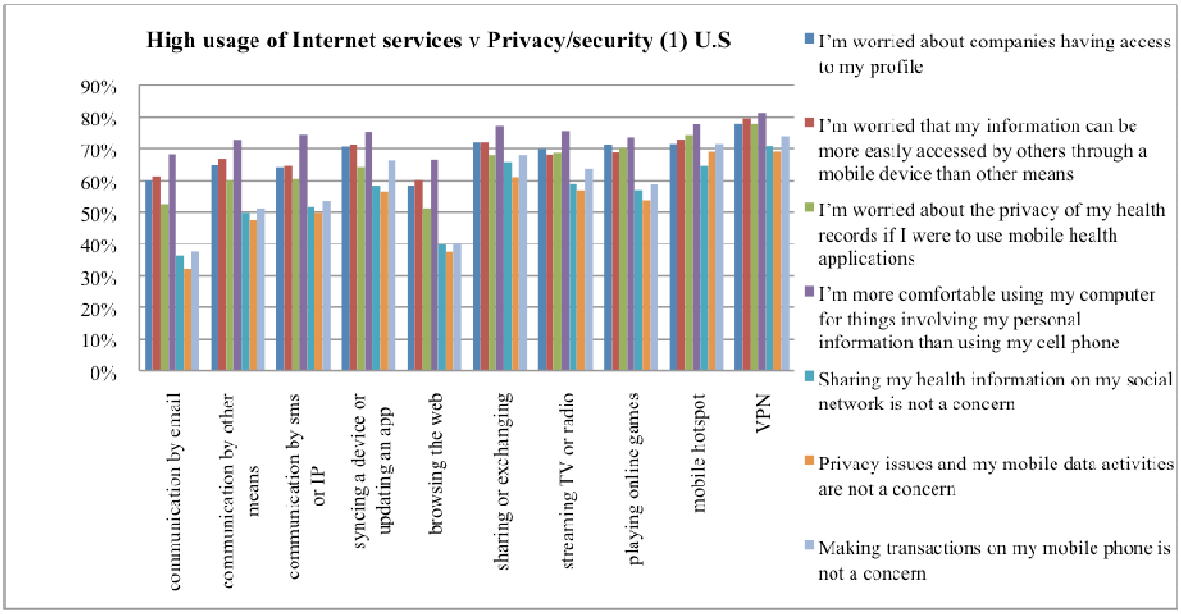

Figure 5. *High (daily or more) usage of mobile Internet services for privacy/security (1) for the U.S.*

Now we look at the high use of Internet access/services and the *privacy/security (1)* question in Japan, shown below in Figure 6.

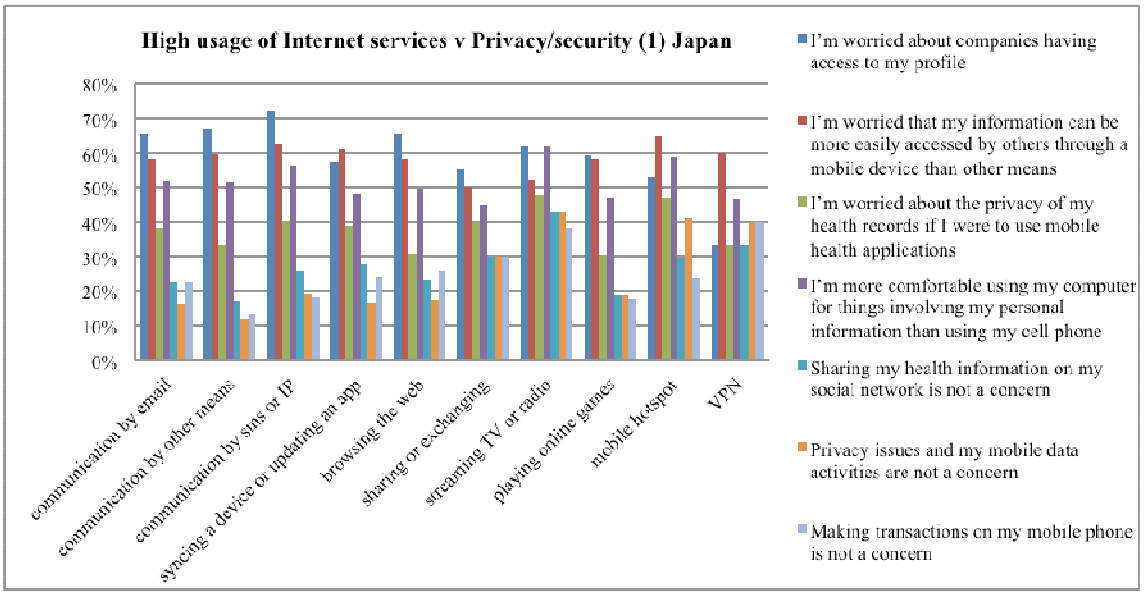

Figure 6. High (daily or more) usage of mobile Internet services for privacy/security (1) for Japan.

For most categories of Internet access/services, the proportion of users that agree or strongly agree with the statements about having a high degree of privacy/security concerns are high, the exception being the statement "high degree of concern for the usage of health care applications." This statement has a general lower proportion of agreement than the other statements expressing concern. Also, it's important to note that in Japan there seems to be less concern about health care applications than in the U.S. Also, it is important to note that for almost all the Internet access and services the proportion of users with high degree of privacy/security concerns is consistent throughout all services that are listed. These trends don't apply however for VPN services. This finding could have several explanations, but the most likely is that for this service the sample is small, therefore the results are not reliable. It is also interesting to compare these results to the U.S. results where the low degree of concern statements are in higher proportion that those in Japan, indicating that in Japan there is a higher degree of concern than in the U.S.

Next we look at m-commerce use in Figure 7 below. Attitudes towards privacy and security for downloading free apps and performing online banking seem to be very similar, compared to the other categories. There happens to be an ease of use quality as well as popularity (measured by frequency of use) for these services. It is interesting that that for these two services, the trend is different from the other categories. On the other hand, for the services that are more advanced, like making stock transactions, using coupons or buying physical goods, the trend is also similar and a greater level of concern about privacy and security is visible. It is worth noting that respondents that have high use of M-commerce have at the same time a high degree of concern about privacy/security. Also, for the activities that are popular and that people are more likely to use, such as downloading free apps and online banking, the difference in proportion between the low and the high degree of concern is significant. In other words, the degree of privacy and security concerns are great. On the other hand, when the activity is more advanced, like making a stock transaction or buying physical goods, the difference in proportion between the two degrees is almost insignificant, suggesting a lower level of concern overall. Our hypotheses that people with greater experience using mobile services will have less concern about privacy and those with less experience have more concerns appears to hold in these findings. Furthermore, it's important to point out the behavior of people with low levels of m-

commerce service usage. The results show that this group has a lower degree of concern for privacy/security. This behavior can be explained by the fact that non-use of m-commerce probably isn't due to security/privacy issues but other factors, like lack of experience or interest in using mobile services.

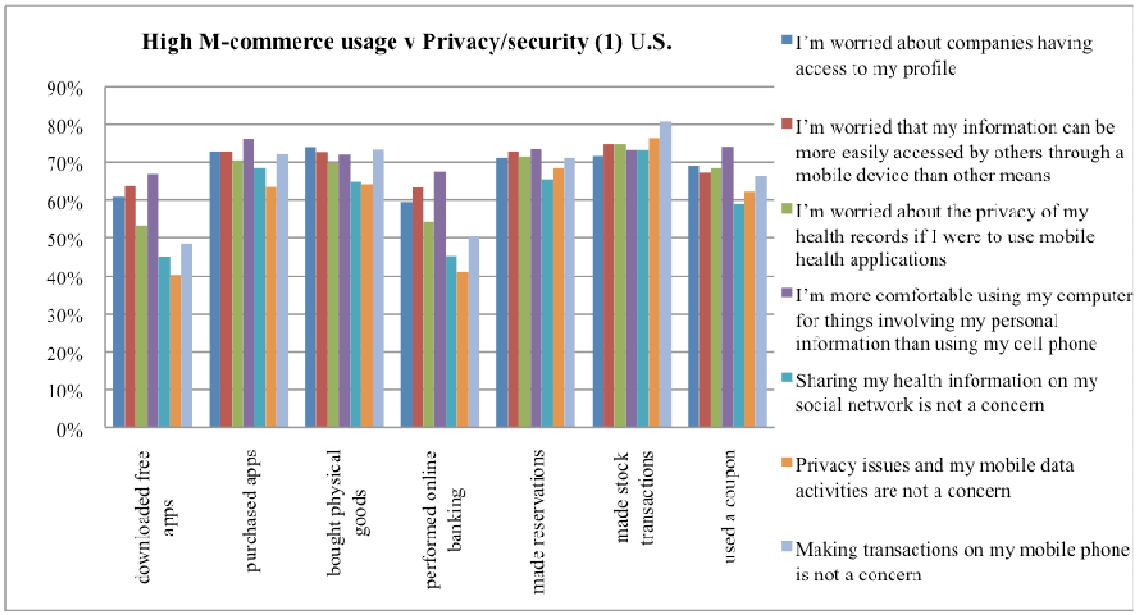

Figure 7. High (weekly or more) usage of M-commerce services for privacy/security (1) for the U.S.

Finally, M-commerce usage is shown in Figure 8 for Japan. Again, the proportion of users of M-commerce that have high degree of concern is higher than those with low degree for all statements, except for 'concern about health records for the usage of health care applications.' This is also a characteristic seen in Figure 6. It is also interesting to compare these results to the U.S. user's behavior regarding privacy of health records. As in the previous figure we can see that compared to the U.S., Japanese users have a lower proportion of users who have a low degree of privacy/security concerns Thus, Japanese users appear actually to have more concerns about privacy/security issues than U.S. users. This finding is unexpected given conventional wisdom that concepts of privacy in Japan are minimal. In addition, this concern with privacy and security is worth noting when we look at the general use of m-commerce services in the U.S. and Japan. See table below:

Table 1. Global Mobile Survey Question: How often do you use the wireless data services listed below? Frequencies for high (weekly or more) usage for the entire sample of U.S. and Japanese users

	downloaded free apps	purchased apps	bought physical goods	performed an online banking activity	made reservations	made stock transactions	used a coupon
U.S.	30.0%	14.2%	14.5%	27.5%	14.3%	12.1%	16.0%
Japan	6.2%	0.9%	1.4%	2.7%	1.3%	1.5%	3.2%

This table shows that U.S. usage of m-commerce services is higher than it is in Japan where there is also a higher degree of privacy and security concerns, consistent with hypothesis 4 that higher concern results in lower use of services.

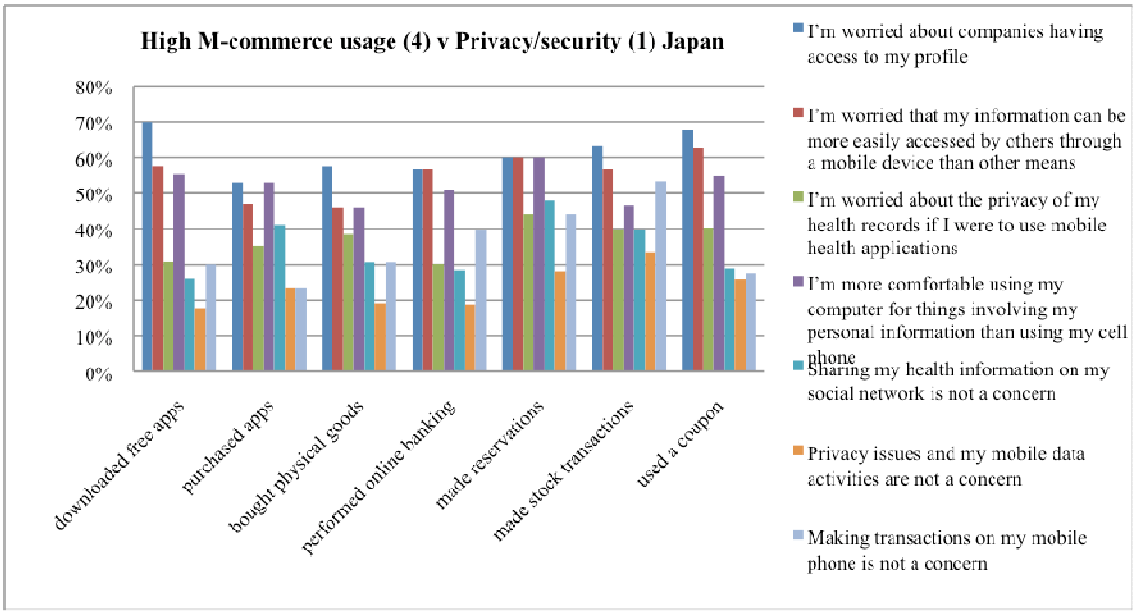

Figure 8. *High (weekly or more) usage of M-commerce services for privacy/security (1) for Japan.*

3.3 Privacy/security concerns for financial transactions and m-commerce

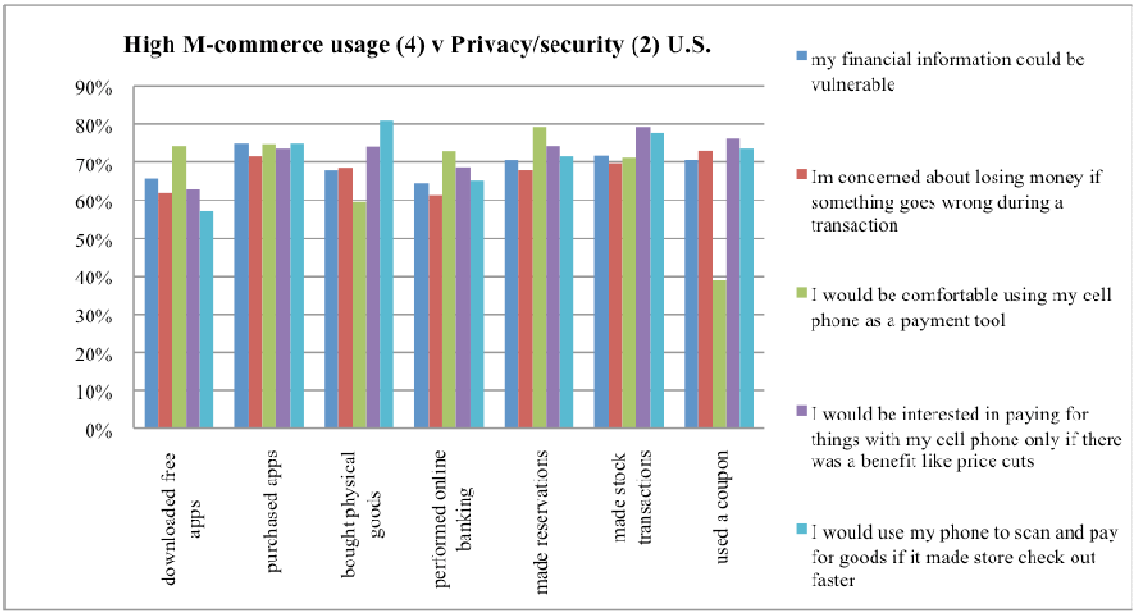

Figure 10. *High (weekly or more) usage of M-commerce services for privacy/security (2) for the U.S.*

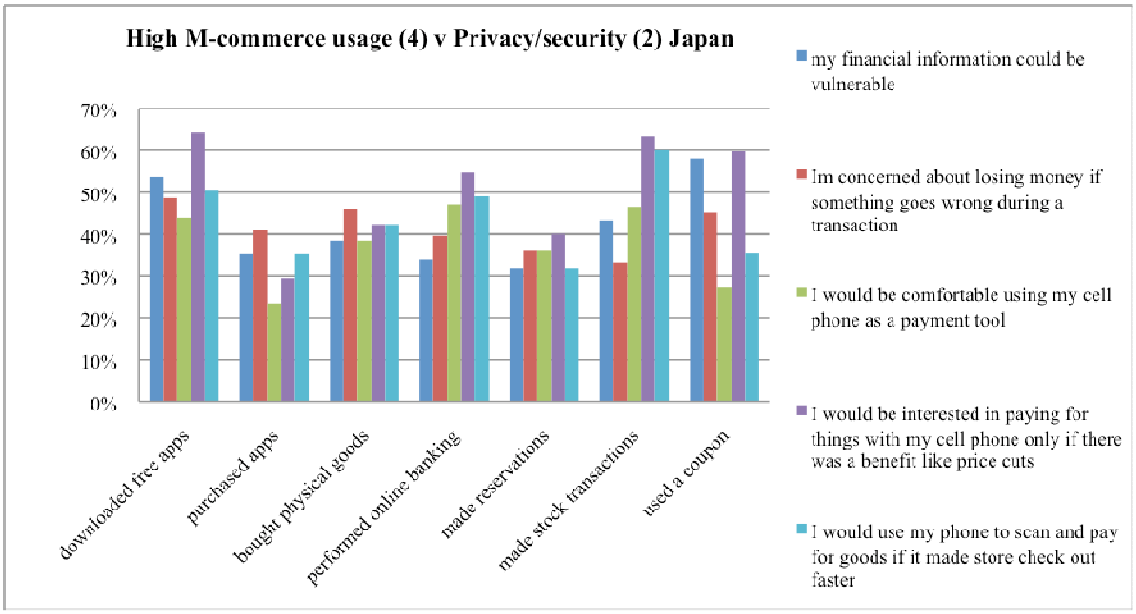

Figure 11. High (weekly or more) usage of M-commerce services for privacy/security (2) for Japan.

4 Discussion: Implications

A prevailing concept about privacy at the moment in the consumer sphere uses the idea of trade-offs made by the individual who willingly divulges personal information in exchange for something of value in return such as use of services or discounts (Crovitz, 2011). This trade-off presumes knowledge on the part of the individual who makes a rational decision to take part in this bargain. It is clear that users are not fully aware when their data such as age, gender, habits, address, and other items are collected, aggregated or sold to a third party. The expectation in some cases may be that the individual's privacy is protected; for example, Apple has a privacy policy, although enforcement of this policy is currently in question. Privacy and security concerns may not be based entirely on fact, but rather habits, expectations and cultural practices. As our survey data indicates, (Figure 1) privacy and security concerns are present when substituting the mobile phone for a task rather than using a computer. People are more comfortable using their computer for things involving personal information and also feel that their information is more vulnerable on a cell phone than a computer.

While the survey data reveals in general that older people are more concerned with privacy and security – in particular related to health information, younger people are also concerned about these things. Our survey data shows that despite many claims that younger people are not concerned about privacy, substantiated often by use of social networking sites like Facebook, where personal information is readily shared to connect with others; in fact younger people do have concerns about companies having access to their information and using it without authorization. Well over 50% of those between the age of 13 and 45 have this sensitivity. Interestingly, people who buy apps have a higher concern than those who download free apps, perhaps reflecting a choice in which the perception is that payment provides more privacy and security.

Our first hypothesis is that users with a high degree of privacy/security concerns would also have sensitivity to using services that increased this risk, and we did find that some services were associated with higher degrees of concern, (i.e. health related matters seem to be a sensitive area for all US users). Surprisingly, other services that used frequently, are used in spite of the fact that there is

concern. The second hypothesis that users with less concern will also have greater confidence using services that could risk privacy and security breaches seems to be supported for online banking and downloading free apps. Hypothesis 3 and 4 is likewise supported by the survey findings for m-commerce use in that more advanced users (defined in terms of the difficulty of using the service) have lower levels of concern and users with less experience have greater concern and use the services less. Finally, in comparing cross-nationally, we found more agreement between the US and Japanese users in terms of privacy and security concerns than differences in spite of the clear distinctions in social views and traditions in these two countries. In particular both cultures are sensitive to the possibility that companies are able to collect their information and utilize it without informing the user. To conclude, it seems clear that users are not yet completely aware of the privacy and security issues surrounding the use of mobile devices, yet to a large extent it is up to the individual to take precautions and make decisions in the face of incomplete knowledge. As users become more knowledgeable about how their data is collected and used, it will be interesting to see how use patterns and attitudes evolve towards either greater acceptance as some have argued is already evident or to increased vigilance and caution.

References

Beckwith, R. (2003). "The human experience. Designing for ubiquity: the perception of privacy," Pervasive Computing, 2(2): 40-46.

Corey, S.M. (1937). "Professed Attitudes and Actual Behavior," Journal of Educational Psychology. 28, 271-280.

Crovitz, G.L. (2011). "Information Age: Are we too hung up on privacy?" Wall Street Journal, New York: Oct. 3., pg. A.15

DeCew, J. (1997). In pursuit of privacy law: law, ethics, and the rise of technology. Ithaca, NY: Cornell University Press.

Deloitte. (2012) Open Mobile: The growth era accelerates: The Deloitte Open Mobile Survey.

Dyson, E. (2008). Reflections on Privacy 2.0. Scientific American, Sept. 50-55.

Gupta, S. Xu, H., et al. (2011). Balancing privacy concerns in the adoption of Location-Based Services: an empirical analysis, International Journal of Electronic Business, Vol.9, Nos. 1/2, 118-137.

Hartmann, M. (2011). "Mobile Privacy: contexts" Ch. 14 in Trepte, S. and Reinecke, L. (eds), Privacy Online, Springer-Verlag Berlin.

Hayashi, K. (2006). 'The Public' in Japan" Theory, Culture & Society, 23:615.

Kapko, M. (2012). The Quest for Security in Mobile. Feature Report, Juniper.

Kaplan, C. (2001). Kafkaesque? Big Brother? Finding the Right Metaphor for Net Privacy., New York Times.

KPMG, (Dec. 2011). Privacy, Security Issues Hamper Wider Growth of Mobile Banking, Despite Increasing Consumer Acceptance: KPMG Survey, Dec. 21, 2011 /PRNewswire, http://www.prnewswire.com/news-releases/privacy-security-issues-hamper-wider-growth-of-mobile-banking-despite-increasing-consumer-acceptance-kpmg-survey-135994438.html

Kutler, K,M. (2012). Even Android's Top Developers See a Scant Number of Paid Downloads in US, Inside Mobile Apps, (online blog) accessed: Feb. 5, 2012, http://www.insidemobileapps.com/2011/01/25/android-paid-downloads/

Laufer, R. & Wolfe, M. (1977). Privacy as a concept and a social issue: a multidimensional development theory. Journal of Social Issues, 33(3), 22-42.

Lee, L.T. (2000). Privacy, security, and intellectual property. In A.B. Albarran, & D.H. Goff (Eds.) Understanding the web: Social political, and economic dimensions of the Internet (pp. 135-164). Ames, IA: Iowa State University Press.

Lee, L.T. (2007). Digital media technology and individual privacy. In C. Lin, & D. Atkin (Eds), Communication technology and social change (pp.257-280).
Lin, C. & Atkin, D. (2007). Communication technology and social change. Mahwah. NJ: LEA.
Mizutani, M., Dorsey, J. et.al. (2004). The Internet and Japanese conception of privacy. Ethics and Information Technology. 6: 121-138.
Moor, J. (1997). "Towards a Theory of Privacy in the Information Age," Computers and Society, 27(3): 27-32.
Nissenbaum, H. (2011). "A contextual approach to privacy online," Daedalus. Fall. Vol 140, p.32-49
Quinn. (2010). "Methodological Considerations in Surveys of Older Adults: Technology Matters" International Journal of Emerging Technologies and Society, 8: 2, 114-133.
Warren, S. & Brandeis, L. (1890). The right to privacy. Harvard Law Review, 4, 193-220.
Wishart, R. & Mancini, C. (2012) Privacy Management in Mobile Applications: A report on PriMo 2011, J. Network Systems Management, 20: 149-153.
Wu, Y., Lau, T. Atkin, D. & Lin, C. (2011). A comparative study of online privacy regulations in the U.S. and China. Telecommunications Policy, 35, 602-616.