DOI: 10.1145/1610252.1610283

BY SUN SUN LIM, HICHANG CHO, AND MILAGROS RIVERA SANCHEZ

Online Privacy, Government Surveillance and National ID Cards

THIS STUDY EXPLORES WHETHER INTERNET USERS' CONCERNS for personal information privacy, principally manifested as online privacy, are related to their attitudes to government surveillance and national ID cards (often perceived as a surveillance tool). This is a relationship which needs to be explored in-depth because of three concurrent trends – first, the push towards e-government, where citizen-government transactions are increasingly conducted online; second, the growing use of smart cards, RFID tags and other portable information collection and transmission devices by governments and businesses; and third, calls for greater government surveillance, both online and offline, to counter terrorism in the post 9/11 environment.

While prior research has dealt with individual concerns about online privacy and individual concerns about government surveillance, studies exploring the relationship between the two are limited. This study seeks to fill that gap by surveying Internet users across five cities which vary in their experience of government surveillance and the use of national ID cards – Bangalore, New York, Seoul, Singapore and Sydney.

Personal information privacy is the individual's ability to personally control information about him/herself. Such information could include anything from one's birth registration details, to the identities and coordinates of one's next-of-kin, income and expenditure patterns and even health records. In countries where day-to-day transactions with commercial and government entities are increasingly being conducted online, involving the electronic collection of personal information, online privacy is the principal manifestation of personal information privacy.

As e-commerce and e-government services become more pervasive, Internet users' concerns about online privacy are likely to grow. Individual online privacy concerns have been classified into improper acquisition, improper use and privacy invasion.[12] Concerns about improper acquisition relate to unauthorized access to personal information, improper collection of one's private information and improper monitoring of consumers' online activities. Concerns about improper use cover unauthorised analysis of consumers' online shopping behavior and the subsequent business-to-business transfer of such analyses. Concerns about privacy invasion refer to the transmission of information to Internet users without their prior consent, such as spam, as well as the improper storage of personal information. To maintain their online privacy, Internet users can engage in self-protective behaviour such as opting out, using privacy enhancing technologies, reading privacy policies, or checking trust marks.

Studies have been conducted to test

concern about online privacy as a function of demographic variables. Sheehan[10] found that gender was a significant factor in that female consumers were generally more concerned about their personal privacy than male consumers. In general, older consumers[2] were also more concerned about online privacy. The relationship between consumers' experience with the Internet and online privacy concerns has also been explored. Bellman et al.[2] reported that consumers' online privacy concerns diminished with Internet experience. As more consumers use the Internet and the average level of experience rises, online privacy concerns should gradually diminish. In general, studies have demonstrated that demographic variables and Internet-related experiences significantly affect Internet users' concern about online privacy.

Online Privacy, Dataveillance and Government Surveillance

Dataveillance has been defined as the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."[4] While the relationship between concerns about online privacy and attitudes to government surveillance may not be immediately obvious, the concept of dataveillance may provide some links.

Surveillance is essentially institutionalised intrusion into privacy and governments worldwide engage in surveillance of their citizens to varying degrees. Government surveillance can incorporate a range of activities – from extreme physical intrusions to day-to-day gathering of personal information, for example, dataveillance. Dataveillance is the most common and pervasive form of government surveillance as governments worldwide collect information for social services, taxes, voter registration, birth, death, marriage records, utilities, education etc. With the growth of Internet based e-commerce and the proliferation of e-government services, dataveillance will be increasingly conducted online. Consequently, Internet users may become more conscious about how their online privacy will be affected. In this regard, Internet users' attitudes to government surveillance may affect their level of concern with online privacy as a whole.

Adding depth and complexity to this issue is the fact that while Internet users desire online privacy, they also see the benefits of government surveillance in enhancing national security, especially in the post 9/11 environment.[5] However, the value of national security vis-à-vis online privacy varies from country to country and from person to person. Emphasis on individual rights is arguably stronger in the West. In the US for example, privacy is seen as a basic human right and entrenched in the Bill of Rights. In contrast, Asian legal systems have tended to overlook the individual's interest in favour of the collective: "The importance of national goals to life in say, Singapore or Japan, has no equivalents in other parts of the world, and can permit much higher levels of intrusive surveillance than would be countenanced in surveillance-conscious regions such as Scandinavia."[8] On an individual level, those who see the advantages of government surveillance in stamping out crime and terrorism may have a higher threshold for privacy intrusions. They may therefore accord a higher priority to national security than to individual privacy. Hence, we ask: *Do attitudes to government surveillance influence online privacy concerns?*

Online Privacy and National ID cards

National ID cards are often perceived (and criticised) as instruments of surveillance. Indeed, the introduction of national ID cards has been resisted in countries such as the U.S. and Australia. Australia's attempt to launch the "Australia card" national identification scheme between 1986 and 1987 met with such severe public opposition that it was not granted parliamentary approval. Indeed, studies have found that the way in which an identity card is introduced into a community impacts on the level of public acceptance. The level of compulsion and the existence of a centralised database can raise privacy concerns[7] while transparency and public consultation can alleviate them.[1]

While some countries are contemplating the adoption of identity cards, many European and Asian countries already issue and use them. Citizens/residents of these countries are routinely asked to provide national ID card numbers when using governmental and business services, thus enjoying the convenience of completing a range of transactions by utilising only that one number. Aside from convenience, it has also been noted that national ID cards can aid in the prevention of terrorism and identity theft, and serve as documentary proof of one's identity.[6]

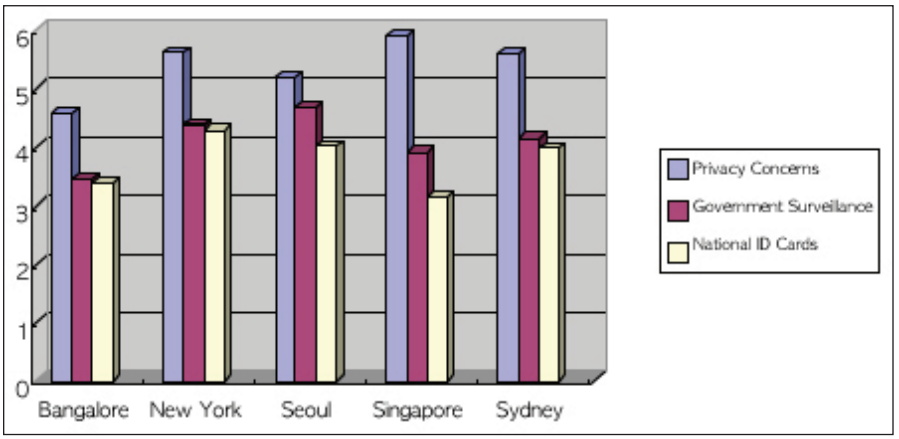
However, critics argue that such benefits are greatly outweighed by security risks such as overzealous surveillance.[9] One study concluded that while the post 9/11 atmosphere has made Americans more amenable to the idea of a national ID card, they are still concerned about the possible loss of privacy through authorized or unauthorized use of personal information.[6] Yet another study predicted that with the increased use of smartcards, RFID tags and other such information collection devices, there will be more demands for government regulation of such technology so that individual privacy is protected.[11] Therefore, we ask: *Does experience with using national ID cards influence online privacy concerns?*

However, attitudes to national ID cards are not contingent upon experience with using them. Individuals in countries which do not issue identity cards may still hold the opinion that such cards are beneficial to society. Similarly, individuals in countries which do issue identity cards may have negative opinions towards their use. Therefore, we recognise that a distinction should be made between experience with using national ID cards and attitudes towards national ID cards. Hence, we additionally ask: *Do attitudes to national ID cards influence online privacy concerns?*

Research Method

Sample and data collection. An online survey was conducted amongst Internet users in Bangalore, New York, Seoul, Singapore and Sydney. Seoul and Singapore were selected because globally, they rank high in Internet penetration and broadband connectivity, and they issue national ID cards to their citizens and residents. While national ID cards are not issued in India, voter registration cards which are issued nationwide are often used and widely regarded as identity cards. These three Asian cities were then counter-balanced by Sydney and New York, both of which do not issue national ID cards.

Figure 1. Five-city comparison of levels of online privacy concern, attitudes toward government surveillance and attitudes to national ID cards



* Based on 7 point Likert scales (1=less concerned/positive attitudes, 7=highly concerned/negative attitudes)

The survey, conducted in 2003, took the form of an online, self-administered questionnaire comprising 47 questions, most of which contained 7-point Likert-scale items. The same English language survey was used for Bangalore, New York, Singapore and Sydney, and translated into Korean for administration in Seoul. To ensure consistency of survey implementation, a research company with branches in all five cities was hired to conduct the surveys. Survey respondents were randomly selected from the company's panel database for each city. Email invitations were sent out continuously until the required sample size (300 Internet users per city) was attained. The total number of respondents for each city was 300. However, after eliminating unreliable answers, the final sample size per city was: Bangalore: 244, Sydney: 280, Singapore: 277, Seoul: 196 and New York: 264.

Measure. Internet users' online privacy concern was measured by a 5-item scale covering various dimensions such as concerns about online privacy in general, concerns about data collection by online entities, and control over online privacy (α = .759). Internet users' attitudes toward government surveillance and national ID cards were measured by 6-item Likert scales (see Table 1). To control for the effects of other relevant variables, we also measured national culture (individualism), demographics (age, gender, education, and income), and Internet-related experiences (the lengths and frequencies of Internet use and online shopping, SPAM mail received, and online shopping spending).

Data Analysis

National variances in online privacy concerns, attitudes to government surveillance and national identity cards. Figure 1 shows the differences in online privacy concerns, attitudes toward government surveillance and attitudes toward national ID cards across the five cities.

ANOVA tests showed that the differences in online privacy concerns [$F(4,1256)=81.331$, $p<.001$], attitudes to government surveillance [$F(4,1256)=33.642$, $p<.001$], and attitudes to national ID cards [$F(4,1256)=60.706$, $p<.001$] across the five cities were all significant (see Table 2). Internet users in Seoul had the most negative attitude towards government surveillance, while those in Bangalore were the most positive. Interestingly, Internet users in New York and Sydney, the two cities which do not use or issue national ID cards, had the most negative attitudes towards these cards. Another point of note is that across all five cities, while Internet users held somewhat high levels of concern for online privacy (M=5.41), attitudes to government surveillance (M=3.89) and the use of national ID cards (M=3.75) were more neutral. This trend is suggestive of the ambivalence which individuals feel about these two practices – that on the one hand, government surveillance and the use of national ID cards may compromise one's personal information privacy; on the other hand, they could help to enhance national security.

How attitudes to government surveillance and National ID cards affect online privacy concerns. Table 2 summarizes the results of regression analysis. To test the relationships between the variables, multiple regression analysis was conducted. Given that cultural attitudes may influence consumer

Table 1. Scales for measuring attitudes to government surveillance and national identity cards

The Government's ability to monitor the activities of its citizens...

- Keeps my country safe
- Infringes my personal liberty
- Is important for maintaining national security and social stability
- Is intrusive
- Makes it easier to arrest criminals, terrorists and illegal immigrants
- Is unnecessary

National identity cards....

- Are necessary for maintaining national security
- Enhance the Government's power of surveillance over its citizens
- Help to guard against terrorism and illegal immigration
- Enable the Government to monitor the activities of its citizens
- Help to enhance personal security
- Infringe on personal liberty

Table 2. Comparison of attitudes toward government surveillance and national ID use across five cities showing means and standard deviations

	Sydney	Singapore	Seoul	Bangalore	New York	Total	F
Online Privacy Concern	5.60 (.97)	5.91 (.86)	5.20 (.86)	4.57 (.93)	5.62 (.91)	5.41 (1.01)	81.331**
Government Surveillance	4.15 (1.42)	3.92 (1.31)	4.69 (0.89)	3.46 (0.87)	4.39 (1.36)	3.89 (1.06)	33.642**
National ID card use	3.99 (1.24)	3.15 (0.87)	4.01 (0.60)	3.39 (0.87)	4.29 (1.14)	3.75 (1.07)	60.706**

( ): Standard Deviation
** p <.01

adoption of smartcards,[1] we included national culture in the model as a control variable. Other control variables included were demographics and Internet-related experiences. The association between government surveillance and privacy concern was significant (b= -.179, p < .001), indicating that Internet users with positive attitudes to government surveillance are less concerned about online privacy. Arguably, Internet users who regard government surveillance positively are likely to have higher thresholds for privacy intrusions and thus, it stands to reason that they have lower levels of online privacy concern. One would therefore expect that Internet users with positive attitudes to national identity cards would also have lower levels of online privacy concern. Instead, our findings show that attitudes to national ID cards had a positive association with online privacy concern ((b= .133, p < .001), that is, Internet users with more positive attitudes to national identity cards have higher levels of online privacy concern.

This apparent inconsistency may be due to the fact that while government surveillance can be an abstract concept, national identity cards are an observable instrumentation of government surveillance practices. Envisioning the use of national identity cards in daily transactions accentuates the practical implications of government surveillance, dataveillance and potential privacy intrusions. Hence, while people can hold positive attitudes to national identity cards, they can be concurrently more concerned about online privacy because they anticipate the potential adverse effects of these cards on their online privacy.

How experience with national ID cards affects online privacy concerns. We ran a separate ANCOVA analysis to test the effect of national ID cards experience on online privacy concern. Interestingly, Internet users from countries which issue national ID cards exhibited lower levels of privacy concerns (M=5.26) than those from countries which do not (M=5.61). The difference is statistically significant (F=9.25, p<.01), after controlling for the effects of the same control variables as noted above. Viewed in tandem with the previous findings about attitudes to national identity cards, it seems that while positive attitudes to national identity cards raises online privacy concerns, actual experience with using national identity cards may lead to a decline in online privacy concerns. Actual experience with using national ID cards appears therefore to desensitise Internet users to privacy intrusions, due possibly to three reasons. First, their online privacy concerns are neutralised by the convenience which using such cards can bring. Second, from their experience of using identity cards, they realise that the potential for privacy intrusions is not that significant; or third, they become accustomed/resigned to the online privacy intrusions which accompany the use of national identity cards.

Limitations and Managerial Implications

Please note that our findings are based on correlational analyses, making it difficult to establish causality. For instance, it could be argued that online privacy concerns can influence individuals' attitudes toward government surveillance and national ID card use, suggesting that the causal direction can go the other way.

Internet users' concerns about online privacy can have negative consequences for the broad-scale adoption of the Internet and e-commerce. Surveys show that Internet users who are most concerned about threats to their online privacy are least likely to engage in online shopping, and many Internet users who have never made an online purchase cite privacy concerns as a key reason for their inaction. Indeed, the perceived risks of shopping online, such as vulnerability to credit card fraud, have been found to outweigh its perceived convenience.[3] Furthermore, online privacy concerns can negatively influence Internet users' online behavior, such as, Internet users with stronger online privacy concerns are more likely to provide incomplete information to Web sites or to request removal from mailing lists, thereby adversely impacting online consumer relationship management activities.

It is important to note though that online privacy is but one facet of an individual's overall privacy concerns, which persist whether the individual is online or offline. Hence, factors which influence an individual's overall privacy concerns are likely to influence his/her online privacy concerns a well. As our findings show, factors which are ostensibly extraneous to the Internet, such as, attitudes to government surveillance and experience with national ID cards, can also influence an individual's online privacy concerns. Managers of Internet sites should therefore be aware of such factors when formulating their privacy policies.

As fears of terrorism mount in the post 9/11 environment, the nature and extent of government surveillance and dataveillance is likely to change. This will in turn affect individuals' concerns about personal information privacy and specifically, online privacy. Concerns about dataveillance are also likely to increase with the growth of e-government services and smart card technology. Hence, in trying to gauge their potential target audience, managers of Internet sites have to consider the entire environment shaping individuals' privacy and online privacy concerns, and not just focus only on Internet-based factors. In addition, they should also be cognisant of trends in e-government because individuals' concerns about dataveillance by public and private organisations may mutually influence each other and together, influence online privacy concerns. C

References

1. Bailey, S. and Caidi, N. How much is too little? Privacy and smart cards in Hong Kong and Ontario. *Journal of Information Science, 31*, (2005), 354-364.
2. Bellman, S., Johnson, E., Kobrin, S. and Lohse, G. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society, 20*, (2004), 313-324.
3. Bhatnagar, A., Misra, S. and Rao, H. R. On risk, convenience, and Internet shopping behavior. *Commun. ACM 43*, 11, (Nov. 2000), 98-105
4. Clarke, R. Information technology and dataveillance. *Commun. ACM 31*, 5 (May 1988), 498-512.
5. Gould, J. B., Playing with fire: The civil liberties implications of September 11th. *Public Administration Review*, 62, (2002), 74-79.
6. Hiltz, S. R., H. J. Han and Briller, V. *Public Attitudes Towards a National ID "Smart Card": Privacy and Security Concerns*. IEEE Computer Society, 2002.
7. Joinson, A. N., Paine, C., Buchanan, T. and Reips, U.-D. Watching me, watching you: privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom. *Journal of Information Science*, 2006. 334-343.
8. Lyon, D., *Surveillance Society: Monitoring Everyday Life*. Open University Press, 2001.
9. Neumann, P. G. and Weinstein, L. Risks of national ID cards. *Commun. ACM 44*, 12 (Dec. 2001), 176.
10. Sheehan, K. B. An investigation of gender differences in online privacy concerns and resultant behaviours. *Journal of Interactive Marketing 13*, 4, (1999), 24-39.
11. Strickland, L. S. and Hunt, L. E. Technology,

security, and individual privacy: New tools, new threats, and new public perceptions. *Journal of the American Society for Information Science and Technology*, 56, (2005), 221-234.
12. Wang, H. Q., Lee, M. K. O. & Wang, C. Consumer privacy concerns about Internet marketing. *Commun. ACM 41*, 3, (Mar.1998), 63-70.

This study was supported by a grant from National University of Singapore (R-124-000-006-112). The authors thank the editor and the anonymous reviewers for their helpful comments.

Sun Sun Lim (sunlim@nus.edu.sg) is an assistant professor at the Communications and New Media Programme, National University of Singapore.

Hichang Cho (cnmch@nus.edu.sg) is an assistant professor at the Communications and New Media Programme, National University of Singapore.

Milagros Rivera Sanchez (mrivera@nus.edu.sg) is an associate professor and head of the Communications and New Media Programme, National University of Singapore.