Research Note

Comparison of Survey Findings from Canada and the USA on Surveillance and Privacy from 2006 and 2012

Emily Smith

David Lyon

Queen's University, Canada. smithea@queensu.ca

Queen's University, Canada. lyond@queensu.ca

Abstract

This research note highlights the comparative findings of a recent repeat survey of surveillance and privacy. It also draws attention to the usefulness of public opinion surveys for scanning popular responses to surveillance in different contexts and between different countries. The findings from a survey administered in Canada and the USA in 2006, then repeated in a 2012 poll, indicate some continuities and some relevant changes in mood over time. Knowledge of the internet and of software such as GPS is relatively high in both countries and this is accented among younger groups, especially males. Similarly, while a higher proportion than previously think they have a say over what happens to their personal data, the younger, the more so. In both countries, more people than before believe that camera surveillance is effective. Curiously, knowledge of laws regulating responses to workplace surveillance has declined while a greater proportion now consider security-surveillance intrusive. And although responses to workplace surveillance are basically similar, the idea that employers may share data with others is censured. At national borders there is less support for giving extra security checks to visible minorities. People take more steps to protect their personal data in each country, although they worry much more about what corporations, as compared with governments, might do with them. Fluctuations by age and gender occur here too.

Introduction

It is one thing to note the proliferation of new surveillance technologies and techniques and to track their use and consequences around the world. It is another, and even more complicated thing, to try to understand how and why ordinary people respond to or engage with such surveillance. Yet the ways in which new surveillance affects everyday life simply cannot be gauged without grappling with the interactions between surveillors and surveilled. Students of surveillance use a number of means to investigate such interactions, from fine-tuned ethnographic analysis or personal interviews with selected respondents to statistical analysis of, say, camera use to imaginative engagement with literature or film.¹ Each has its pros and cons.

A further mode of analysis is offered by large-scale public opinion surveys, which is the topic of the present research note. The advantage of the large-scale survey is that, if appropriately framed, researchers can obtain at least a snapshot of views at a given moment, that indicate differences and similarities between population groups on the one hand, and different settings for and types of surveillance, on the other. The picture may be fuzzy, but surveys do yield a sense of shapes and shadows. Of course, many

¹ See for example 'Doing Surveillance Studies', *Surveillance & Society* 3(2/3) 2005, edited by Kirstie Ball and Kevin Haggerty, <http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/380>

considerations have to be borne in mind when attempting to frame a survey of surveillance and privacy experiences, and this approach too has limitations as well as benefits (Zureik et al. 2010: 5-45; Bennett and Raab 2006: 62-75).

However, public opinion surveys become more useful when a time-element can be introduced, allowing one to follow changes over a period of several years. This both shows the ways in which attitudes alter with context, socio-technical change or familiarity, and offers the chance to track trends, at least in a general fashion. The present study is made possible by adding new survey results obtained in 2012 to already-existing data on Canada and the USA from 2006. While some continuities are apparent, there are also some noticeable discontinuities that call out for explanation. The point of the research note, however, is simply to draw attention to these survey results and to invite their further analysis.

In 2006, working with The Surveillance Project at Queen's University,² Elia Zureik led a nine-country international survey on attitudes about surveillance and privacy and experiences with the global flow of personal data.³ The cross-national survey was conducted using primarily telephone and some face-to-face and on-line interviews with 9,606 respondents in Canada, the USA, Brazil, Mexico, China, Japan, France, Hungary and Spain. This research was part of the wider multi-disciplinary and collaborative project called 'The Globalization of Personal Data', which was concerned with the surveillance of ordinary people and how they are affected by information flows in government, corporations, by employers and everyday technologies.⁴

The survey included 50 questions on participants' attitudes about consumer surveillance, racial profiling at airports, terrorism and security, national ID cards, CCTV, media coverage of surveillance issues, workplace privacy, knowledge of privacy regulations, knowledge of various technologies, actions taken to protect information, control over personal data and public trust in government and private companies. The quantitative surveys were preceded by qualitative focus group interviews and background reports in the nine countries. The analyses in the present research note only scratch the surface of the volume of data available, which remain publicly available for further analysis.⁵

In 2012, a follow-up survey contained 10 of the original survey questions from 2006, as well as 14 additional questions about new technologies with a focus on social media in particular as a new development since the original survey.⁶ The surveys were carried out using national online panels in Canada, the US and the UK. In contrast, in 2006, interviews in Canada and the US were administered over the telephone using Computer Assisted Telephone Interview (CATI) technology and took approximately 20-25 minutes to complete. Thus, the sampling techniques for the 2006 and 2012 surveys differ greatly

² Now called the Surveillance Studies Centre, see <http://www.sscqueens.org/>

³ For more information on the Globalization of Personal Data (GPD) international survey, and summary findings, see: http://www.sscqueens.org/research/intl_survey. The project was funded by the Social Sciences and Humanities Research Council of Canada and the survey was fielded primarily by Ipsos-Reid in seven countries, and Millenriver Marketing Research in China and Macromil Inc. in Japan. Fuller discussion of findings is in Zureik et al. (2010).

⁴ More on this project can be found here: <http://www.sscqueens.org/projects/gpd>

⁵ The 2006 GPD survey findings were archived by Jeffrey Moon and Alexandra Cooper at the Maps, Data and Government Information Centre, Queen's University, Stauffer Library in the odesi system. Researchers interested in obtaining access to all of the survey materials and findings should contact Jeffrey Moon at moonj@queensu.ca

⁶ The survey was carried out by Angus Reid public opinion, a Vision Critical practice, under the direction of Andrew Grenville and in consultation with the Surveillance Studies Centre. The additional questions and findings will be analyzed in a separate article. Angus Reid recruited these panels using proactive invitations with a double opt-in screening process. Targeted banner-ad placements were used on a variety of partner non-governmental and charitable organization websites, and national socio-demographic balance was achieved. With the proliferation of cell phone-only households in recent years, combined with an 8 per cent lower response rate over the phone, panels were the preferred and more reliable method of conducting the 2012 surveys. See '20 elections since 2007: Angus Reid's record in the U.S. and Canada', by Angus Reid, Vision Critical, which demonstrates that their on-line polling methods either match or outperform telephone polls in 19 of the 20 elections that have been covered.

and their comparative value is debatable. Despite this, the following is a summary of comparative findings from 2006⁷ and 2012⁸ on the ten overlapping questions in Canada and the US.⁹ It is difficult to determine whether changes in responses are due to disparity in sampling methods, variation in question order, or changes in general attitudes in the past six years. Interesting comparisons can be made nonetheless.

Summary of Comparative Findings

Knowledge about the internet and GPS remains high in both countries, with an increase of about 10 per cent in reported knowledge about the internet (from 82 to 91 per cent in Canada and 80 to 93 per cent in the US) and GPS (from 55 to 64 per cent in Canada and 60 to 70 per cent in the US) from 2006 to 2012. In contrast, there is a decrease in the much lower reported knowledge about RFID, CCTV, biometrics and data mining since 2006 (see Figure 1). The 2006 and 2012 findings show a dwindling in reported knowledge of these technologies in the older age groups, with the exception of CCTV which was slightly higher in the 55+ category in 2012. Significantly more men than women report they are knowledgeable about all of these technologies (i.e. in 2012: GPS- 71 per cent and 55 per cent, RFID- 36 per cent and 14 per cent, CCTV- 58 per cent and 36 per cent, Biometrics- 31 per cent and 17 per cent, Data mining- 36 per cent and 17 per cent), except for the internet, where the numbers are virtually the same.

Figure 1: [VC 1]¹⁰[GPD 1]¹¹
In general, how knowledgeable are you about each of the following?*

*Refers to the summation of 'very knowledgeable' and 'somewhat knowledgeable'

In 2012, a larger proportion of Canadians and Americans thought that they had an increased amount of say in what happens to their personal information, as compared with 2006 (see Figure 2a). In 2006 almost 70 per cent of Canadians and Americans felt they had some or no say with only about one-third believing

⁷ In 2006, the Canadian sample included 1,001 respondents and took place from June 26-July 21 and the US sample included 1,000 respondents and took place from June 27-July 28. Respondents were screened to ensure nationally representative samples based on gender, age and regional distribution.

⁸ In June 2012, with 1,000 respondents in Canada and the US, screened to be representative of the general population.

⁹ These two countries were chosen as they were the only two countries that were both surveyed in the 2006 and 2012 polls. The UK was also polled in 2012, however, this will not be included here, as this was not a country that was surveyed in the original GPD polls and there is no comparative data.

¹⁰ Vision Critical (VC) question 1.

¹¹ Globalization of Personal Data (GPD) question 1.

they had complete or a lot of say, while in 2012 the split became more even for Canadians (45 and 44 per cent). It skewed towards the complete/a lot of say for Americans at 52 per cent, with only 37 per cent claiming they had some or no say (see Figure 2b). Younger people in the both surveys felt they had more say in what happens to their personal information than older people (in 2006; 18-34: 39 per cent, 35-54: 27 per cent, 55+: 25 per cent and in 2012; 18-34: 51 per cent, 35-54: 44 per cent, 55+: 42 per cent), while there were negligible gender differences in response.

Figure 2a: [VC 7] [GPD 2]

To what extent do you have a say in what happens to your personal information?

Figure 2b: Broken down by combining upper and lower responses

In Canada and the US, there has been a decline in the proportion of respondents reporting that they are knowledgeable about laws protecting privacy in government departments, dropping from 47 to 39 per cent (8 per cent) in Canada and from 54 to 42 per cent (12 per cent) in the US (see Figure 3).

Figure 3: [VC 8a] [GPD 3a]

How knowledgeable are you about the laws in [your country] that deal with the protection of personal information in government departments?*

*Refers to the summation of 'very knowledgeable' and 'somewhat knowledgeable'

Similarly, in both countries there was also a drop of about 10 per cent in the number of respondents reporting they were very or somewhat knowledgeable about laws dealing with the protection of personal information in private companies, from 41 to 31 per cent in Canada and from 52 to 43 per cent in the US (See Figure 4). There was little difference based on age and gender in both years. In 2006 slightly more older people than younger people claimed to be knowledgeable about laws protecting information in government departments, while in 2012 slightly more older people than younger people claimed to be knowledgeable about laws protecting information in private companies. Men reported being more knowledgeable than women about laws protecting personal information in government and private companies by 10 per cent in 2012.

Figure 4: [VC 8b] [GPD 3b]

How knowledgeable are you about the laws in [your country] that deal with the protection of personal information in private companies?*

*Refers to the summation of 'very knowledgeable' and 'somewhat knowledgeable'

Correspondingly, the Office of the Privacy Commissioner (OPC) found that when asked about their knowledge of personal privacy rights under the laws protecting their personal information, most Canadians said their knowledge was poor (36 per cent) or neither good nor bad (33 per cent), while 30 per cent said it was either very good (4 per cent) or good (26 per cent) (OPC 2011).¹² However, they found that the level of knowledge has increased since 2006. At the same time, two-thirds (67 per cent) of Canadians were not aware of any federal institutions that help them with privacy and the protection of personal information from inappropriate collection, use and disclosure (Ibid.). Despite this, Canadians felt that they were doing well at protecting their own personal information, with more than half saying they were doing a good job (56 per cent). This has also increased since 2006.

There is an increase in the number of Canadians and Americans who believe the government laws aimed at protecting national security are intrusive upon personal privacy, with a greater increase in Canada from 48 to 60 per cent and a slight increase in the US from 57 to 63 per cent, raising it to the majority of respondents in both countries (see Figure 5). There is little difference based on age or gender in both years, but about 10 per cent more men than women felt that laws are highly or somewhat intrusive in 2012.

Figure 5: [VC 9] [GPD 17]

The government of [your country] has enacted laws aimed at protecting national security. To what extent do you believe laws aimed at protecting national security are intrusive upon personal privacy?*

*Refers to the summation of 'highly intrusive' and 'somewhat intrusive'

In contrast, the OPC found that Canadians have become more confident that the federal government is taking its responsibility to protect citizen personal information more seriously over time. In 2006, 20 percent said that the government was not taking its responsibility seriously and 14 percent saying that the government was taking its responsibility seriously, compared with 2011 where 22 percent say the government is taking its responsibility seriously, rather than not seriously at 11 per cent (OPC 2011). Compared with OPC findings from 2006, Canadians have also become more confident that businesses are

¹² The federal Office of the Privacy Commissioner of Canada commissioned Harris/Decima to undertake a series of surveys from 2005 to 2011 of Canadians understanding and awareness of privacy issues, legislation and institutions. This was a telephone survey with a randomly selected and representative sample of 2,000 Canadian adults, 18 years and older, between February 23 and March 6, 2011.

taking seriously their responsibility to protect consumer personal information, with 14 per cent saying that businesses take their responsibility seriously, 13 per cent disagreeing and 68 per cent believing businesses were taking this task somewhat seriously (ibid.). Thirty per cent of Canadians were also concerned about the personal information they provide at borders or airports being used by other Canadian government agencies, 50 per cent showed some level of concern and 20 per cent were not concerned. However, concern with the sharing of information between the Canadian government and foreign authorities was higher: almost half (47 per cent) showed concern about this, with another 38 per cent being somewhat concerned and only 14 per cent saying they were not concerned (OPC 2011).

In the GPD survey results, there is a marked and surprising increase in the belief in effectiveness for in-store (from 66 to 80 per cent very or somewhat effective) and community CCTV (from 79 to 87 per cent) in Canada, while the US remained the same (71 per cent for community CCTV, and 80 and 81 per cent for in-store CCTV). In both countries the majority of respondents believe both are effective (see Figure 6). In the 2012 results, belief in effectiveness of CCTV was higher with age, for community CCTV 84 per cent of the 55+ category believed in their effectiveness compared with 67 per cent of those 18-34 and 76 per cent of those 35-54. The same was true for in-store CCTV, with 90 per cent of those 55+ believing in their effectiveness, compared with 78 per cent of those 18-34 and 84 per cent of those 35-54. These age findings were not as pronounced in 2006. There is little variation based on gender for both years.

Figure 6: [VC 10] [GPD 20]

Some communities and private companies in [your country] are using surveillance cameras, also known as Closed Circuit Television or CCTVs, to monitor public places in order to deter crime and assist in the prosecution of offenders. Please indicate, in your opinion, how effective you think they are.

Similar low proportions of respondents accept employers monitoring employees electronically with surveillance cameras in 2006 and 2012, with the highest response category being only if the employee gives informed consent, at 37 and 43 per cent in Canada and 29 and 26 per cent in the US, respectively (see Figure 7a). The most notable increase was with US respondents choosing yes, but only for the purpose of evaluating an employee's performance (from 17 to 26 per cent).

Figure 7a: [VC 11] [GPD 21]

To what extent do you think employers should be allowed to monitor their employees electronically with surveillance cameras and to read the e-mails their employees send or receive on the employer's computers?

Electronically monitor with surveillance cameras

With respect to responses to employers reading e-mails their employees send or receive, acceptance of this was also low with fewer respondents in the US feeling it is the right of the employer to monitor emails (from 27 to 18 per cent) and more strongly against employers reading emails (from 22 to 35 per cent) in 2012 (see Figure 7b). There were no noticeable differences based on age for responses to these questions in both years, and only slightly more men than women agreeing that it is the employer's right under any circumstances, only for the purpose of evaluating employee performance or if the employee gives consent to be monitored with surveillance cameras or to read their emails.¹³

Figure 7b: Read emails

¹³A 2006 Pew Internet & American Life Project poll found that 54 per cent of respondents found it 'very' and 'somewhat' important not be monitored at work (Pew 2006).

There was an increase in the proportion of respondents claiming that employers should under no circumstances share information about employees with government, a rise of 18 per cent in Canada (from 18 to 36 per cent) and 15 per cent in the US (from 21 to 36 per cent). In the same way, there was a drop in support for an employer's sharing information about employees if they were suspected of wrongdoing, a 14 per cent decrease in Canada and an 18 per cent decrease in the US (see Figure 8a). There are few significant findings based on age or gender in both years; however in 2012 the older categories (35-55 and 55+) were more likely to say no to employers sharing information with government under any circumstances at 38 per cent, compared with the youngest age category (18-34) at 26 per cent.

Figure 8a: [VC 12a] [GPD 22a]

To what extent do you think it is appropriate for an employer to share their employees' personal information with third parties, such as the government or private sector?
Government

Responses remained relatively the same for employers sharing employee information with the private sector from 2006 to 2012, with most respondents feeling that employers should not share information about employees under any circumstances with the private sector, ranging from 40 to 49 per cent. Likewise, in 2012 the older age categories were more likely to say no to employers sharing information with the private sector under any circumstances, with age 35-54 at 50 per cent, those 55+ at 49 per cent and those 18-34 at 35 per cent.

Figure 8b: Private Sector

Another domain of surveillance covered in the survey concerns travel. Responses are comparable for both years, with a slight increase in those feeling it is not really acceptable for airport officials to give extra security checks to visible minorities, and a slight decrease in the proportion claiming it is not acceptable at all in both countries (see Figure 9). In the 2012 findings older people were more likely to say it is very acceptable to give extra security checks to visible minorities (25 per cent), double that in the 18-34 age category. Men were also more likely than women to say it is very acceptable (23 per cent versus 15 per cent). Further work is needed to say why these generational and gender differences appear with respect to racial profiling but it should be noted that in this case only travel through airports is in view. Thus, given the post-9/11 association of airports and terrorist threats it is likely these, rather than profiling for other criminal behaviour, say, when travelling through urban areas, that give rise to the findings. Anti-terrorism profiling is often seen as more acceptable than for crime prevention (Johnson et al. 2011).

Figure 9: [VC 12b] [GPD 26]

How acceptable do you feel it would be for airport officials to give extra security checks to visible minorities?

Individuals are increasingly encouraged to take precautions with their personal information. There are many similarities in responses about the steps taken, comparing 2006 to 2012 findings, with respondents remaining reticent about sharing information with companies and less so with government. Responses

remained nearly the same with about three quarters refusing to give information to a business because they thought it was not needed (Canada 77 per cent to 79 per cent, but this declined in the US 77 per cent to 65 per cent) compared with only about one-third refusing to give information to a government agency because they thought it was not needed (Canada 33 per cent to 31 per cent, US 34 per cent to 32 per cent). Asking a company to remove them from any lists they used for marketing purposes also remained high (Canada 71 per cent to 76 per cent, US 77 per cent to 75 per cent), while asking a company not to sell their name and address to another company declined (a slight drop in Canada 66 per cent to 62 per cent, and a greater drop in the US 73 per cent to 59 per cent).

There was a small decline in respondents asking businesses they were thinking of dealing with about policies on the collection of consumer information (from 28 to 24 per cent in Canada and 37 to 28 per cent in the US), as well as asking companies to see what personal information besides billing information they had about them in their consumer records (18 to 14 per cent in Canada, and 24 to 20 per cent in the US). The most notable increase occurred with respondents purposefully giving incorrect information about themselves to marketers (from 20 to 43 per cent in Canada and from 22 to 35 per cent in the US), suggesting a greater awareness of the need to protect this type of information which is demanded at every consumer transaction. In addition to this, there was an increase in respondents reporting they had read the on-line privacy policies at websites when making a purchase from a private company (49 to 60 per cent in Canada and 56 to 60 per cent in the US). In terms of sharing information with government, small increases were also shown in those reading on-line privacy policies at government websites when sending them information electronically (40 to 46 per cent in Canada and 38 to 44 per cent in the US) whereas purposely giving incorrect information about themselves to a government agency remained very low (5 per cent in both years for Canada and 9 and 8 per cent in the US).

Figure 10: [VC 19] [GPD 7]

Have you ever done the following for the purpose of protecting your personal information?

In 2012 the older the age category the more likely respondents were to refuse to give information to a business because they thought it was not needed, asking a company to be removed from any lists they use for marketing, and asking a company not to sell one's name and address to another company, by about a 10 percent increase in each instance. However, younger people were more likely to purposely give incorrect information to a marketer (46 per cent of 18-34 year olds, 39 per cent of 35-54 year olds and 30 per cent of those 55+) or when using a website (55 per cent of 18-34 year olds, 43 per cent of 35-54 year olds and 27 per cent of those 55+). Differences in terms of gender were minimal, with the most prominent one being more men (31 per cent) than women (24 per cent) refusing to give information to a government agency because they thought it was not needed, and more men (44 per cent) than women (38 per cent) purposely giving incorrect information when using a website.

In contrast, the OPC found that only 20 per cent had taken actions to protect their personal information, such as contacting an organization, visiting a web site or reviewing a publication, while 80 percent had never done this; the result is consistent since 2009 (OPC 2011). Canadians voiced concerns with managing their on-line privacy, but only 20 per cent said they always (7 per cent), often (14 per cent) or sometimes (28 per cent) read the privacy policies for internet sites they visit. Those who read these policies found them to be vague (35 per cent) or very vague (18 per cent).

Importantly, the OPC found that 65 per cent agreed that protecting the personal information of Canadians will be one of the most important issues facing the country in the next ten years, and 60 per cent felt they had less protection of their personal information in their daily lives than they did 10 years ago (OPC 2011).

Towards a Conclusion

The finding of these two linked surveys indicates that changes over time are significant in some respects and, apparently, not in others. As noted above, various reasons may be suggested for the variations over time, not to mention between the two countries. Overall, the similarities in surveillance experiences between Canada and the USA appear to be greater than the differences, which also hints at the possibility of some emerging common trends. Variations in age and gender are significant but not decisively so, although it is possible that these differences could become greater, for instance as the proportion of so-called digital natives increases in each country.

The generational differences may thus be a key area to watch in order to understand trends in experiencing surveillance and negotiating visibility. Yet while a divide might be apparent on some indices it is also important to note that differences may also be discerned within the broad categories. Younger teens, for example, use social media differently from older ones, including college age students (Livingstone 2008). And young people from higher socio-economic backgrounds are likely to use the internet in more informed and more varied ways than those with less privileged homes (Hargittai 2010). Gender differences in use of technology as well as experiencing surveillance, combined with age, are also an area needing further exploration.¹⁴¹⁵ This is a volatile area but at present several generational and gender differences seem significant.

In general, the findings of these surveys are not reassuring for those concerned with the proper protection of personal data, whether by the 'data subjects' themselves, or by public and private agencies that collect

¹⁴ As Ball et al. point out in their editorial 'Surveillance Studies Needs Gender and Sexuality', "the critique of surveillance through these lenses is still in its infancy" (Ball et al. 2009).

¹⁵ For an example of current research on gender, privacy and equality in online social networking see Bailey et al. 'The eGirls project': <http://egirlsproject.ca/>

and process them. People claim they are more knowledgeable about the technologies and that they have a say over their data-travels but fewer actually know about laws governing personal data and, for those who use them, their preferred modes of self-protection vary considerably. They are also far more confident about the effectiveness of camera surveillance than are researchers on the topic, and in Canada strikingly so. Although it is a matter of ongoing debate, much serious research agrees that surveillance cameras in public places are ineffective at fulfilling either the claims made for them by their promoters or the confidence placed in them by the public (See Doyle et al. 2011; *Surveillance & Society* 6[1] 2009).

Two areas are particularly worthy of further investigation, perhaps using these data alongside others. One is the reasons for variation in opinion between surveillance domains. Why, for example, is personal data in the workplace seen differently from those at national security checkpoints such as airports and land crossings? One certainly could not reliably predict attitudes in one domain from those in another. And what lies behind the variations of views of what information one might withhold from government compared with what would not be divulged to a corporation? This, too, is a complex question, but at a time when, increasingly, personal data are sought and exchanged across a range of organizations, both public and private, both policy and public opinion could benefit from better understanding. Clearly, contexts are crucial, as Helen Nissenbaum (2009) and others have argued, but how can these data on changing attitudes be considered contextually?

The other area calling for further consideration is the question of trust, its perceived basis, and how it is developed and maintained. Corporate handling of personal data is growing faster than that of government departments,¹⁶ the respondents to these surveys reflect a greater concern and suspicion for information in corporate hands than in government departments. These two domains, the public and the private, are increasingly inter-linked and, despite technical and legal limits, personal data flow more freely between the two, leading to even greater complexity in these trust relationships. For instance, in both Canada and the US legislation is sought to permit police and intelligence agencies to obtain personal information from telephone companies and Internet Service Providers (Parsons 2011; see also Ball and Snider forthcoming). Lack of transparency about information collection and sharing points to a great need for promoting public awareness about what is happening with personal information. Most importantly, subjectivity and how individuals experience surveillance in all aspects of their lives needs to be sought through various methods in order to uncover the more complex picture of how individuals accept, negotiate, comply with, reject, ignore, are unaware of, engage with or simply participate in the surveillance that permeates their lives.

As this research limits itself to reporting some findings of interest to others working in the field of surveillance and privacy it does not consider explanations to the extent that would be necessary to form strong conclusions. It is hoped, however, that these and other data will be used by others for further analysis as one way of getting to grips with the rapidly changing world of personal information and surveillance in a digital era.

Acknowledgements

The authors wish to thank Elia Zureik and Charles Raab for their helpful comments on this research note and Andrew Grenville of Vision Critical for his work with us on the 2012 survey itself.

References

- Angus Reid. 2007. 20 elections since 2007: Angus Reid's record in the U.S. and Canada. Vision Critical.
 Bailey, J., Steeves, V., Burkel, J., Regan, P., Saginur, M. and Tallin, J. 'The eGirls Project', funded by the Social Sciences and Humanities Research Council (SSHRC), under its *Partnership Development Programme*. Available at: <http://egirlsproject.ca/>

¹⁶ See for example Pridmore, J. and Zwick, D. (eds) 2011. 'Marketing and the Rise of Commercial Consumer Surveillance', *Surveillance & Society* 8(3): 269-277. Available at: <http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Consumption>

- Ball, K. and Snider, L. (eds) 2013. *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. London and New York: Routledge.
- Ball, K., Phillips, D.J., Green, N. and Koskela, K. (eds) 2009. Surveillance Studies Needs Gender and Sexuality. *Surveillance & Society* 6(4): 352-355. Available at: <http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Gender>
- Ball, K. and Haggerty, K. (eds) 2005. Doing Surveillance Studies. *Surveillance & Society* 3(2/3): 129-138. Available at: <http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/380>
- Bennett, C. and Raab, C. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge MA: The MIT Press.
- Doyle, A., Lippert, R., and Lyon, D. (eds) 2011. *Eyes Everywhere: The Global Growth of Camera Surveillance*. Routledge. Available at: <http://www.routledge.com/books/details/9780415696555/>
- Hargittai, E. 2010. Digital Na(t)ives: Variations in internet skills and uses among members of the 'Net Generation'. *Sociological Inquiry* 80(1): 92-113
- Johnson, D., Brazier, D., Forrest, K., Ketelhut, C., Mason, D. and Mitchell, M. 2011. Attitudes toward the use of racial/ethnic profiling to prevent crime and terrorism. *Criminal Justice Policy Review* 22(4): 422-447.
- Livingstone, S. 2008. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society* 10(3): 393-411.
- Murakami Wood, D. (ed) 2009. Revisiting Video Surveillance. *Surveillance & Society* 6(1). Available at: <http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Relaunch/showToc>
- Nissenbaum, H. 2009. *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford CA: Stanford University Press.
- Parsons, C. 2011. Lawful Access, its potentials and its lack of necessity. *Technology, Thoughts and Trinkets* (blog). Available at: <http://www.christopher-parsons.com/blog/technology/lawful-access-its-potentials-and-its-lack-of-necessity/>
- Office of the Privacy Commissioner of Canada (OPC). 2011. '2011 Canadians and Privacy Survey Final Report', Presented to The Office of the Privacy Commissioner of Canada by Harris/Decima, March 31, 2011. Available at: http://www.priv.gc.ca/information/por-rop/2011/por_2011_01_e.asp
- Pew Internet & American Life Project (Pew). 2006. November. Available at: <http://pewinternet.org/iPoll%20results.aspx>
- Pridmore, J. and Zwick, D. (eds) 2011. Marketing and the Rise of Commercial Consumer Surveillance. *Surveillance & Society* 8(3): 269-277. Available at: <http://library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Consumption>
- Zureik, E., Harling Stalker, L., Smith, E., Lyon, D. and Chan, Y. 2010. *Surveillance, Privacy and the Globalization of Personal Information: International Comparisons*. Montreal and Kingston: McGill-Queen's University Press.