RELEVANT
FOCUSED
READY

Cyber Surveillance & Privacy in Canada

Megan McGibbon

Introduction

The purpose of this study is informed by the statement "balancing the emergency against the intrusion" (Geist, 2015). The context of this statement describes the need for cyber surveillance in order to best ensure national safety, against an overstepping into citizens' personal information. The intention of this study was to provide an informative and current report in the field of public safety and law enforcement, focusing on cyber surveillance and privacy. This research study sought to answer the question: Does cyber surveillance help or hinder the safety of Canadian citizens?

Background

In a recent study conducted by McAfee and the Center for Strategic & International Studies, they have estimated that two-thirds of the people online, more than two billion individuals, have had their personal information stolen or compromised (Lewis, 2018). It is also estimated that cybercrime may now cost the world almost $600 billion, or 0.8% of global GDP (Lewis, 2018). It is clear that this is an inherent problem not just for Canada, but worldwide. It is because of statistics like these that surveillance through government and law enforcement agencies is deemed necessary. Advocates of a surveillance society see this as an important and useful resource for law enforcement to prevent crime like never before, and an opportunity to provide irrefutable evidence if a crime is committed and surveillance is available. These supporters follow the old adage, if you aren't doing anything wrong, there is no reason to fear. However the trade-off for this kind of protection could mean justice for all, and privacy for none (Bilton, 2013). Inquiries into whether the government and their agencies are collecting beyond the reasonable needs of their operations is where the beginning of the concern lies.

Methods

The methodology used for this study was a mixed methods approach, using both qualitative and quantitative data. Only secondary sources of information were used to ensure timeliness and compliance with outlined ethics standards. Information was gathered primarily using the Justice Institute of British Columbia online library, Camosun library database, and Google Scholar. This literature was then compared with results from the Public Opinion Survey of Canadians on Privacy years 2014 and 2016, prepared for the Office of the Privacy Commissioner of Canada. The data was analyzed for trends and patterns to illuminate the current status of both the academic literature against Canadian public opinion.

Results/Findings

The 2016 Public Opinion states that "nearly three in four Canadians feel that they have less protection of their personal information in their daily life than they did ten years ago" (OPCC, 2016). This statement echoes the ones made in the 2014 Public Opinion Survey that Canadian's felt that their ability to protect their personal privacy online was becoming obsolete (OPCC, 2014). Canadians who rated themselves more knowledgeable about privacy rights were more likely to express extreme concern for protection of personal privacy.

A finding of interest is that in 2016 "half of Canadians [surveyed] agreed that intelligence gathering and law enforcement agencies do not have enough power to collect private information from citizens in support of national security and public safety" (OPCC, 2016). This statement appears to contradict the literature, which often stated that the expansion, intensification, and integration of surveillance measures by government and law enforcement may have too much power already (Haggerty & Ericson, 2000).

In addition, there is seemingly no option to opt-out of hierarchical cyber surveillance should a person feel that it is unwanted. Such surveillance can be seemingly undetectable, and an individual may not even be aware their privacy has been breached. It is recommended that provisions are implemented into government policy to provide accountability and oversight when such powerful tools are being used, often beyond the scope of public knowledge. While national security is of the utmost importance, the upholding of civil liberties needs to be included in the conversation as well.

Discussion

This research is important as it highlights a current and pressing issue in law enforcement and public safety. The digital landscape changes rapidly, and the public must be educated and legislation adjusted in appropriate time. Giving governments the authority to conduct warrantless data collection should be informed by research, not by fear. There appears to be no consensus in regards to a formal definition of privacy, and this problem needs first to be addressed to target the center of the issue.

What a society doesn't want is this fear driving policy. The seemingly never ending fight against terrorism can serve as a major proponent that lends itself to a never ending excuse to spy on civilians personal lives (Bilton, 2013). Giving government the social authority to conduct this sort of cyber espionage has critics quick to reference these activities as being a step along the path to an Orwellian society. It is a high stakes enterprise in which society is a major stakeholder, and should treat the responsibility as such.

Conclusion

The significance of this research study is that it shines a light on Canadian attitudes regarding cyber surveillance and the protection of their personal privacy. These attitudes were examined against the findings from academic and scholarly literature, to illuminate an apparent disconnect between citizens levels of knowledge and concern about some of the problems that academics are predicting. Technology and the Internet are such powerful tools, often for positive purposes, but they can be weaponized for negative purposes as well. This body of work encompasses a brief snapshot of a much larger issue, and is intended to supply a level of basic knowledge about the subject. Further research should be conducted into programs to educate and inform the public about their privacy rights online.

References

Bilton, N. (2013, July 16). The pros and cons of a surveillance society. Retrieved from https://bits.blogs.nytimes.com/2013/07/16/the-pros-and-cons-of-a-surveillance-society/.

Geist, M. (2015). *Law, privacy and surveillance in Canada in the post-Snowden era*. [N.p.]: University of Ottawa Press.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage / L'assemblage surveillant. *The British Journal Of Sociology*, (4), 605

Lewis, J. (2018). *Economic impact of cybercrime: No slowing down*. Retrieved from https://www.mcafee.com/us/resources/reports/restricted/economic-impact-cybercrime.pdf .

Phoenix Strategic Perspectives Inc. (2016). *2016 Survey of Canadians on Privacy: Final report*. Privacy Commissioner of Canada.