Data privacy of vulnerable populations like teenagers or elderly in Canada

Date: 14 April 2024

Course: COMP261

Sec: 002

Professor: Mehrdad Tirandazian

Group 4:

Manpreet Kaur (301239154)

Rincy Kuriakose (301217536)

Maharsh Patel (301301102)

Arun Gopakumar (301175785)

Dishank Trivedi (301171796)

Introduction

Data security and privacy have emerged as major global concerns in the digital era, and Canada has responded by passing laws and regulations to safeguard the personal data of its inhabitants. However, because of their limited technological literacy and potential for exploitation by dishonest parties, vulnerable populations—such as teens and the elderly—are especially vulnerable. This paper seeks to examine Canadian ethical issues related to data security and privacy, with an emphasis on safeguarding these marginalized populations.

In Canada, several legislative frameworks, such as the Personal Information Protection and Electronic Documents Act (PIPEDA) and provincial privacy legislation, incorporate ethical considerations pertaining to data protection and privacy. These laws set forth rules for the gathering, using, and sharing of personal data with the intention of striking a compromise between people's right to privacy and justifiable commercial and societal objectives. Even with these precautions, it can still be difficult to adequately protect vulnerable groups, especially the elderly and teenagers.

Why Teenagers and elderly populations are vulnerable?

Teens may lack the information and experience necessary to fully comprehend the ramifications of their behaviour on the internet due to their inexperience with technology. Seniors and the elderly, however, have a distinct set of problems. Older adults may find it difficult to keep up with the rapidly evolving technological landscape, and their physical and mental health may make it difficult for them to engage with it.

Let’s discuss both age groups in detail.

Teenagers:

Teens utilise digital technology extensively; they frequently use social media, play online games, and use other platforms where it is possible for personal information to be gathered and misused. Clear privacy policies, age-appropriate permission procedures, and increased parental participation in supervising and controlling their adolescent children's online behaviour are all ethical considerations. Additionally, educators and legislators are essential in advancing digital literacy and giving teens the power to decide how they want to present themselves online.

According to a 2014 McAfee Canada survey, there is a big digital divide in the online behaviour of Canadian kids (ages 10 to 23) and their parents. According to research, 76% of young people confess to disguising their online habits from their parents. These behaviours include browsing history clearing and watching violent and sexually suggestive content. Many young people still discover ways to hide their internet activity, even if some parents try to keep an eye on their children's conduct through parental restrictions and communication. In order to close the digital divide and encourage young people to behave responsibly online, McAfee highlights the significance of parental involvement, computer literacy, and online safety education.

Online privacy education is essential because kids and teens live in a world where social media and smartphones rule and they are constantly exposed to information about their personal lives online. It is critical to regulate the collection, usage, and sharing of personal information because even seemingly unimportant elements might be combined to identify specific individuals. Online data collection involves the use of a variety of overt and covert techniques, which raises concerns about identity theft and reputational damage. To enable youth to make responsible decisions, conversations on online privacy should begin early and continue throughout their lives. Setting family rules, utilising privacy settings, sharing personal information with caution, and abstaining from risky activities like accessing public Wi-Fi and

taking online quizzes are all practical measures that can be taken to protect privacy. Parents and teenagers can find resources from organisations such as the Office of the Privacy Commissioner of Canada, which emphasise the importance of taking preventative measures to protect personal data and ensure safe online activities.

Global regulators are stepping up their enforcement of privacy laws to protect minors online, focusing on several digital service providers with fines and injunctions. There are several different approaches to youth privacy legislation because of legislators closely examining internet characteristics that encourage negative behaviours. While some jurisdictions, like the U.K. and California, emphasise the need for companies to protect children' privacy and safety by proactive measures like age-appropriate design requirements, others place more emphasis on parental gatekeeping. In order to reduce legal risks and protect minors' privacy and well-being, businesses that provide online services to them must carry out youth impact assessments, put in place age estimation mechanisms, prioritise high privacy settings, make sure that legal language is clear, practise data minimization, use algorithms responsibly, offer parental controls, and put in place robust security measures.

Elderly:

The elderly may have difficulties using digital platforms because of things like low technological literacy or cognitive deterioration. Creating user-friendly interfaces, making privacy settings available, and providing support channels that are specifically catered to the needs of senior citizens are all examples of ethical practices. Elderly people's digital data should be secure and private, and family members and carers should be made aware of this to respect the autonomy of the elderly and ensure their well-being.

According to data from the Canadian Internet Use Survey conducted in 2022, eight out of ten seniors 65 and over now access the Internet, a 6.3 percentage point rise from 2020. With 75%

of seniors sending and receiving emails, email is still the most popular online activity among them, followed by social networking and instant messaging. Seniors are also using video streaming services, online banking, and appointment scheduling at significantly higher rates. Remarkably, a tiny fraction of seniors uses dating apps or websites, illustrating an increasing trend of digital connectedness among Canada's senior population.

In the digital age, strong laws are necessary to protect vulnerable populations' data privacy and security, but so is social commitment to ethical technology usage and education. A more inclusive digital environment may be created by getting communities involved in discussions regarding the moral implications of digital technology. Ultimately, in an increasingly interconnected world, innovation in privacy-enhancing technology provides a proactive means of safeguarding people's digital rights and freedoms, particularly those of the young and old.

Let's analyse the topic using various ethical frameworks.

Ethical Frameworks

Utilitarianism:

Utilitarianism prioritises maximising utility, or total happiness, and bases decisions on their effects. A utilitarian approach to data privacy and security for seniors and teenagers in Canada would entail putting strict privacy laws and security mechanisms in place to safeguard their personal data. If a social media platform gathers copious amounts of user data for the purpose of targeted advertising, for instance, a utilitarian viewpoint would assess the possible harm resulting from invasive data gathering techniques against the advantages of tailored adverts. Therefore, to maximise the general happiness and well-being of teenagers and the elderly, politicians may prioritise passing legislation that restrict data collecting and guarantee informed permission.

Deontology:

Deontological ethics emphasises upholding moral obligations or laws regardless of the repercussions. A deontological approach would emphasise preserving the privacy and autonomy of minors and the elderly as a basic moral obligation in the context of data privacy and security. Consider the following scenario: a healthcare organisation wants to gather patient data for research but cannot get consent. A deontologist would contend that, whatever the possible advantages of medical research, honouring patients' autonomy and right to privacy is unavoidable. As a result, the organisation would have an ethical duty to put gaining individuals' informed consent ahead of gathering their data.

Virtue Ethics:

Cultivating moral character and virtues like honesty, integrity, and empathy is emphasised by virtue ethics. A virtue-based approach to data privacy and security would concentrate on developing an ethical conduct culture in society and organisations. A virtue ethicist would stress the significance of honesty and integrity when handling sensitive financial information, for instance, if a technology business created an app for financial management aimed at senior citizens. As a result, the business would place a high priority on openness, security, and user empowerment while encouraging moral behaviour and dependability in both its staff and users.

Rights-Based Ethics:

Respecting and defending people's fundamental rights—such as their right to privacy and autonomy—is at the centre of rights-based ethics. A rights-based approach would give priority to protecting the privacy and autonomy of minors and the elderly when it comes to data privacy and security. Consider the scenario when a marketing firm wants to gather teens' personal information for the purpose of targeted advertising without getting their permission. Teenagers should be given the authority to decide how to use their personal information and have a

fundamental right to regulate it, according to rights-based ethicists. As a result, the marketing firm would have an ethical duty to get youngsters' express approval before gathering and utilising their data.

Conclusion

Adopting a multifaceted strategy that considers the various requirements and vulnerabilities of various demographic groups is necessary to ensure ethical practices in data privacy and security. Stakeholders can manage the difficulties of data governance while respecting core values of justice, openness, and respect for individuals' rights by employing ethical frameworks such as utilitarianism, deontological ethics, and virtue ethics. To protect vulnerable populations' privacy and security in the digital age, Canada must continue to enhance regulatory frameworks, advance digital literacy, and cultivate a culture of ethical responsibility.

References

Determann, E. D. T. D. D. T. D. D. T. (2023, August 29). Kids' and teens' online privacy and safety: 8 compliance considerations. *International Association of Privacy Professionals*. https://iapp.org/news/a/kids-and-teens-online-privacy-and-safety-8-compliance-considerations/

Government of Canada, Statistics Canada. (2023, August 14). *Canadian seniors more connected than ever*. Statistics Canada. https://www.statcan.gc.ca/o1/en/plus/4288-canadian-seniors-more-connected-ever

McAfee, Inc. (2018, December 25). 76 Per Cent of Canadian Youth Admit to Hiding Online Behaviour from Parents. *www.newswire.ca*. https://www.newswire.ca/news-releases/76-per-cent-of-canadian-youth-admit-to-hiding-online-behaviour-from-parents-513761701.html

Mydoh. (2023, May 16). *What kids and teens need to know about online privacy*. Mydoh. https://www.mydoh.ca/learn/blog/education/what-kids-and-teens-need-to-know-about-online-privacy/#:~:text=The%20best%20way%20to%20control,asked%20to%20share%20certain%20information.