
# BRIEFING NOTES

# BN-21-Cyber and space as key enablers-Oct2020

## PRIVACY AND DATA PROTECTION

Authors: Mohammadreza Nematallahy[1], Edward Gharibian[1], and Kash Khorasani [2]

[1] Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

## SUMMARY


- Privacy and data protection represent as major issues in today's online society and life. Companies utilize customers data in variety of means and purposes.
- Privacy has been a long-lasting right of humans in free and democratic societies that should be revised and adapted based on recent changes in technology trends and due to interactions among people and novel products and services.
- AI systems, due to their speed and capabilities in processing large amount of data as well as their complex internal structure, do highly affect privacy of people implying that their roles should be addressed and properly regulated.
- Instead of trying to fit AI technologies into current privacy frameworks that are highly incompatible with these novel technologies, instead reforming and revising laws, policies, and regulations seem to be the more appropriate and formal methodology for this context.
- There are certain rules and laws regarding privacy and data protection, and the Canadian Government offers advisory services.
- It is essential to educate the citizens of their rights and practices for data protection laws and policies. Moreover, the Canadian Government can have a more active role similar to the EU data protection authorities.


## CONTEXT

- It has been for some time where traditional laws of privacy and data protection have lost he ground due to increasing dependence of people to internet and other software connected to the internet.
- AI systems due to mainly their speed and ability in processing and analyzing large data sets and also due to their internal complex structure, have challenged data protection and privacy concerns in recent years.
- Considering the significant amount of personal and business data that are used in modern economy, a strong data protection rules are required for protecting personal data. In past years several companies have been fined in different European countries for violating these rules, the most notable one was Google that was fined 50 million Euro in France.
- Identity theft, leaks of sensitive data, and intrusive surveillance tools represent as some examples of the concerns and issues. Data protection represents as a global issue and many countries have adopted some regulations regarding data protection. Proper implementation and enforcement of data protection policies are vital issues of significant importance.
- There are various rules and regulations regarding personal data privacy in Canada. Moreover, there are some well-known data protection policy and tools to help companies comply with these rules. However, as the rules and regulations are new and are evolving, small and medium sized

companies have difficulty in implementing them. Also effective implementation of data protection regulations require in-depth knowledge and expertise.

- Canada has some federal rules regarding privacy protection and enforcement of these laws that are handled by various government organizations. The data protection rules in Canada are governed by federal laws and three general private-sector laws in three provinces. Canada has also anti-spam legislation. Personal Information Protection and Electronic Documents Act (PIPEDA) is federal law that applies to inter-province and international cases.
- The key rights that individuals in Canada have in relation to processing of their personal data are governed as follows:
    - **Access to data** – On request, an individual must be informed of existence, use, and disclosure of their personal information, and must be given access to that information.
    - **Correction and deletion** – If the personal information that is in an organization are inaccurate or incomplete, the organization must correct the inaccuracies.
    - **Objection to processing** - Individual must be able to withdraw their agreement at any time, "subject to legal or contractual restrictions and reasonable notice".
    - **Objection to marketing** - Individuals must agree before companies use their data for marketing, and must be able to withdraw their agreement to the use of their personal information for marketing purposes.

## CONSIDERATIONS

- The challenges are not limited to only AI system capabilities in de-anonymizing the protected information and mining complementary data from large data sets, but also AI systems very commonly have been used as decision making service providers and due to their highly complex structure, one cannot ensure if sensitive information has been used or not.
- The role of different parties such as designers, data owners, and also people should be clearly defined and traditional top-down methodologies should be revised.
- Identity theft and leaks of sensitive information are major issues for both individuals and companies that do indeed affect the economy, politics and life of citizens.
- Misuse of personal data in social media has become a challenging problem in recent years, and there are no clear rules for limiting the extend that companies can use personal data.

## NEXT STEPS *(If applicable)*

- Since designers currently depend highly on data, data protection laws should put more responsibility on their shoulder, in contrast with traditional laws, in which by consent agreement the contract would have assumed more responsibility on people.
- Instead of considering the data itself, it would be more logical to focus on how the data will be utilized and their possible impacts. This is more relevant to the value of information and is more compatible with new technologies and AI systems.

- The internal complexity of AI systems structure highlights the role of explainability in achieving safer and more privacy aware technology, which minimizes the risks and harms on people and society.
- EU member states have been established data protection authorities (DPA). They are "independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law". They are also working actively to fine the violating companies.
- However, monitoring the entire social media is neither practical nor recommended. Clear rules and policies are lacking in this area and filtering of inappropriate posts and accounts are mostly done based on public pressure and decision of owners of social media. There are significant rooms for working on this area specially for educating younger generation in schools and facilitating actions against offensive and inappropriate contents.