



# BRIEFING NOTES

#BN-41-Emerging technology and military  
application-Feb2021

## DATA PRIVACY AND LIABILITY OF EMERGING TECHNOLOGIES AND AI

Authors: Edward Gharibian<sup>1</sup> and Kash Khorasani<sup>2</sup>

<sup>1</sup> Graduate student, Department of Electrical and Computer  
Engineering, Concordia University, Montreal, Canada

<sup>2</sup> Professor, Department of Electrical and Computer  
Engineering, Concordia University, Montreal, Canada

## SUMMARY

- ✚ **Objectives:** Emerging technologies, and specifically AI and machine learning solutions, have created new concerns on privacy of personal data and the associated liability considerations. In particular, the current tort law cannot handle a number of these situations and circumstances. Therefore, it is necessary to study and investigate the associated emerging technologies and develop and propose policies for respecting privacy of consumers. Moreover, we need to make operators of these technologies liable in order to protect both the consumers and developers. In addition, the above considerations are imperative in order to accelerate the investment and to ensure and keep the industrial stakeholders competitive.
- ✚ **Scope:** Our focus is on emerging technologies, and more specifically on AI systems, from the point of view of privacy of personal data and how operators of AI and emerging technologies should be liable for their products.
- ✚ **Target audiences:** Our research attempts to facilitate and empower the policy makers to have a better understanding of (a) the emerging technologies and AI, (b) the possible ways and means that these systems use data and make decision, and (c) how to make recommendations to address their liability and privacy issues.

## CONTEXT

- ✚ Solidifying a cybersecurity strategy is becoming more important than ever since one is witnessing many attacks over the past few years. In view of this fact and the prevailing trends in cyberattacks, prevention, detection and response policies are three essential challenges that we need to be considered with in articulating our cyber security strategy.
- ✚ In today's world, there exist a number of Internet services that are mostly free such as text messages, emails, maps, and free storage, to name a few. However, one actually pays for these services with one's personal and private data. In digital era, user's personal data represents as among the most valuable assets for companies.
- ✚ One recent case is Google's \$2.1 billion bid to acquire Fitbit, an American company in the wearable equipment business. EU regulators are investigating the case, and It seems that the concern is on the use of health data by Google [\[1\]](#).
- ✚ The privacy and data issues have become much more complicated by the increased use of AI by companies that already own huge amount of personal data, such as Google and Amazon. More data implies more dominance on the market.
- ✚ Data is raw material for AI systems, and the bigger the data size, results in higher quality decisions by the AI systems. Companies use these data to improve their products and services, that might be threaten by the customers' privacy.
- ✚ We are surrounded by devices that are known as Internet-Of-Things (IoT) or smart things. Devices such as smart TVs, smart thermostats, smart refrigerators, smart cars,

etc. These devices are practically internet connected sensors that collect our personal data.

- ✚ Use of personal data can significantly improve the targeted advertisements, that many, may not have any problem with, but, the issue is the use of data for rather unexpected purposes. AI systems can analyse our health condition, driving or eating habit, and sell it, for instance, to an insurance company, which is violation of the privacy laws and regulations.
- ✚ UK and Australia are investigating a facial recognition company for a database of 3 billion photos of people, collected from internet, and their concern has to do with protecting their citizens personal information and privacy [3].
- ✚ COVID-19 also has recently triggered a lot of attention towards use of digital technologies in health care systems [4]. Canadian hospitals already have started to use a facial recognition software to track health of patients remotely [2]. Canadian government, also explores the use of AI in governmental programs and services [5].
- ✚ With this amount of attention to data and AI systems, the privacy and liability of these systems have become a real concern. Emerging technologies always create new cases in use of our private data where few can anticipate ahead of time. This also, challenges organizations on how and to what extent they collect data.
- ✚ In legal systems, to be able to obtain a compensation for a physical or financial damage, one should be able to attribute faults to a party, through causation [6]. This is done either by breach of a contract terms or by “breach of a duty of care in tort” [6].
- ✚ The decisions made by AI systems are mostly based on machine learning schemes that are data driven and provided to AI systems. In other words, it is only loosely as a result of programming mistakes, which makes it difficult to trace an error to a human oversight or negligence. This problem is known as “causation challenge” in law [6], [7].
- ✚ European union Expert Group on liability and new technologies [8] in 2019 issued a report entitled “Liability for Artificial Intelligence and other emerging digital technologies” [9]. The report studied EU members law, and concluded that current regulation in many cases provide a basic protection for consumers of emerging technologies such as IoT, however in cases as in AI systems, that need analysis of complex structures and codes of the system, the result can be unfair [9], [10].
- ✚ Among the key findings in that report is that in cases where tort law fails, and when providing evidence can be impossible or very expensive, existing legislation could not provide fair outcomes and new duty of care need to be developed [9]–[11].
- ✚ The office of Information and Privacy Commissioner (OIPC) of Canada, has proposed some enhancements to the PIPEDA (The Personal Information Protection and Electronic Documents Act [12]) to address these challenges [13], [14].
- ✚ The emerging technologies and AI are rapidly evolving, and hence to protect the society and economy, policy makers, politicians and legislators need a continuous flow of

consumable information to make proper proposals and enhancements to the current regulations.

### CONSIDERATIONS

- ✚ Emerging technologies such as IoT, AI, autonomous systems, etc., can create value and opportunities to the economy and society. In order to facilitate economic growth and improve social life, proper legal frameworks are necessary to accelerate the investments in these fields and provide assurances to consumers and industries.
- ✚ Current duty of care tort law may come short in cases where damage is result of using a complex AI system.
- ✚ With prevalent use of personal data by AI systems, specifically in ways that cannot be anticipated, proper liability and privacy laws are required to protect both the consumers of the technology and promote industrial stakeholders to keep the economy competitive.

### RECOMMENDATIONS

- ✚ Further study and analysis on trend of emerging technologies and how they may affect privacy of citizens, and opportunities and threats arising from these technologies for business and society should be conducted.
- ✚ Need to study different cases of AI systems and other digital technologies that may result in liability issues or privacy violations where one needs to offer recommendations to the policy makers.
- ✚ Comparative study on data privacy and liability regime in other countries and how they may affect the Canadian businesses, and citizens, and Canadian Armed Forces should also be investigated.

## REFERENCES

- [1] “Exclusive: Google can ward off EU antitrust probe into Fitbit deal with data pledge,” Reuters, Jul. 09, 2020.
- [2] “Duckface can save lives: Binah.ai raises \$13.5M to monitor health condition through selfies,” GeekTime, Jun. 11, 2020.
- [3] A.Ng, “UK and Australia open joint data-privacy investigation into Clearview AI,” CNET.
- [4] “Digital technology for COVID-19 response.”
- [5] T. B. of C. Secretariat, “Responsible use of artificial intelligence (AI),” aem, Nov. 22, 2018.
- [6] “Artificial Intelligence in Construction? | Law Bulletins | Taft Stettinius & Hollister LLP.”
- [7] “Artificial Intelligence: Privacy and Legal Issues,” CPO Magazine, Feb. 19, 2018.
- [8] “Register of Commission expert groups and other similar entities.” (accessed Jul. 11.
- [9] Expert Group on liability and new technologies, “Liability for AI and other emerging digital technologies.” European Union, 2019.
- [10] “Commission Expert Group Report on Liability for Emerging Digital Technologies,” Inside Privacy, Dec. 01, 2019.
- [11] Liability for Artificial Intelligence and Other Emerging Digital Technologies– H. Snellman
- [12] O. of the P. C. of Canada, “The Personal Information Protection and Electronic Documents Act (PIPEDA),” Sep. 04, 2019.
- [13] “Privacy and Artificial Intelligence – Slaw.”
- [14] O. of the P. C. of Canada, “Consultation on the OPC’s Proposals for ensuring appropriate regulation of artificial intelligence,” Jan. 28, 2020.