Who is responsible when AI causes harm? AI and product liability

AUTHORS

 Grant Worden

 Nicole Mantini

 Alicja Puchta

 Lauren Nickerson

Further reading:

- Does AI have patent and copyright ownership?
- AI in financial services: are consumers better protected, or more at risk?
- The board says we need an AI strategy, how do we start?

AI is increasingly being incorporated into a wide variety of products, including chatbots, medical devices, autonomous vehicles and household appliances[1]. In many cases, AI makes these products more efficient, effective and adaptive; however, integrating AI also comes with risks. This raises an important question: who should be held responsible if something goes wrong and users are harmed?

Attributing fault for harm caused by AI systems

While AI is relatively new, product liability is not. Canada's existing product liability framework is well-equipped to govern claims related to harm caused by AI-enhanced products. This framework commonly engages three types of product liability claims that can be readily extrapolated to the AI context:

1. **Failure to warn** applies where manufacturers and/or sellers fail to provide sufficient warnings or instructions about a product's risks. In the context of AI-assisted products, a failure to warn consumers that AI is involved in the product's function or use could create exposure to the risk of a novel failure to warn claim. Similarly, sellers could be exposed to risk for failing to warn buyers or users about AI-related risks that may not be evident at the time of sale.

2. **Design negligence (or defective design)** applies where product designers or manufacturers fail to make reasonable efforts to ensure that a product is safe for its intended use. Failure to anticipate and mitigate foreseeable outcomes and risks could expose creators of AI or AI-containing products to the risk of design negligence claims.

3. **Manufacturing negligence** applies where manufacturers fail to make reasonable efforts to prevent product defects during manufacturing. Manufacturers and sellers who sell products with outdated algorithms or provide incorrect outputs could be exposed to manufacturing negligence claims.

Due to the unique features that may exist with AI-enhanced devices, additional types of claims in tort that are less commonly seen in the product liability framework, such as negligent misrepresentation, could also conceivably arise in this context. For example, a claim could arise where a consumer relies on an inaccurate representation or statement generated by AI, or uses a product for which the extent of AI integration has not been disclosed, and is harmed as a result.

> “
>
> Because chatbots are not considered separate legal entities, companies can be held responsible for their mistakes.

Ultimately, in Canada, product liability is a matter of negligence and not strict liability, requiring a causal link between the harm suffered by the consumer and the negligence of the designer, manufacturer or seller. The existence and strength of this causal link depends on the circumstances, including whether the harm incurred was foreseeable and, if so, what steps were taken to avoid it.

The evolving nature of AI complicates this analysis. Because AI systems learn and evolve through use, there is potential for something to “go wrong” at various stages of a system’s lifecycle: it could be designed with insufficient model parameters, developed with low-quality training data, or used carelessly or with inadequate instruction. In some cases, all three circumstances could materialize, potentially making it difficult to apportion liability between the designer, manufacturer/developer and user. Moreover, what is considered “foreseeable” may shift as awareness about AI and its risks continues to grow. Below, we discuss three case studies in which these issues play out.

Case studies: chatbots, AI-assisted medical devices and autonomous vehicles

Chatbots

Chatbots are one of the most popular current uses of generative AI. This popularity is attributable to their versatility; they can perform many different tasks in different contexts. However, chatbots have their share of pitfalls. For example, the general-use, large-language models underlying many commonly used chatbots come with a risk of “hallucination”. Often trained on data that is indiscriminately scraped off the internet, some chatbots tend to lack robust fact-checking systems and may be sensitive to minor variations in inputs or prompts. When a chatbot is asked a question, there remains a decent chance that its answer will be wrong or misleading.

This lack of reliability is problematic for companies seeking to incorporate chatbots into products, services and webpages. Because chatbots are not considered separate legal entities, companies can be held responsible for their mistakes. Recently, an airline was required to honour its website chatbot’s misrepresentation of company policies, which a customer relied on in booking a flight[2]. The British Columbia Civil Resolution Tribunal found that companies are required to take reasonable care to ensure that the representations on their website “are accurate and not misleading”—whether they come from static text on a website or a dynamic chatbot.

AI-assisted medical devices

AI is also being used in medical devices with increasing frequency. AI systems can be used to analyze patient data, assist with procedures and diagnostic analyses, monitor various health indicators, and assess and administer medicine dosages to patients, among other uses.

Such medical devices have the potential to attract "failure to warn" allegations, particularly if patients are not fully informed of the role that AI plays in a device or the risks associated with its use. A failure to warn patients that AI is informing medical decision-making or treatment could create a risk of a novel type of failure to warn claim. In this context, given the complex nature of AI algorithms, plaintiffs may view failure to warn allegations as preferable to design and manufacturing claims as it may be more difficult to identify—and therefore to establish—design or manufacturing defects (for more on AI in healthcare, read "Will AI replace my physician? Navigating the legal and regulatory landscape of AI in healthcare").

Autonomous vehicles

The idea of autonomous vehicles (AVs) has long captured futuristic imaginations. Now, they are a reality. In San Francisco and Los Angeles, for example, you can now hail a self-driving "robotaxi"[3]. Although fully autonomous vehicles are not widely available for public use in Canada, federal and provincial governments have granted exemptions to their existing frameworks for AV research and development[4].

While the potential risks of getting into a self-driving car may be more self-evident to consumers than in some other AI applications, thereby making it hard to successfully assert a failure to warn claim, harm caused by the use of AVs may be more likely to raise allegations related to negligent design or manufacturing.

Strategies for mitigating risk

Manufacturers and sellers of products integrating AI can take steps to minimize their litigation risk:

1. **Issue clear warnings:** The internationally recognized principles of AI transparency, explainability (particularly where failure to warn issues arise), and human oversight are especially relevant in the context of product liability. It will be important to (a) clearly identify when, how and for what purpose AI is being used in the product; (b) educate consumers about the foreseeable uses, capabilities, limitations and risks associated with the use of AI; (c) identify inputs that may affect a device's performance; and (d) issue clear warnings about how a product should *not* be used.

2. **Implement continuous monitoring:** Risk assessment may be challenging for products that evolve through consumer use. As AI systems learn and adapt, their risk profile changes. Risks can be mitigated by implementing continuous monitoring measures. These measures can include (a) periodic testing, simulations, and field performance assessments; (b) tracking use and misuse; and (c) documenting design changes.

3. **Consider reasonable alternative designs:** Consider alternative designs that could decrease potential risks associated with the product, including what data should be used to train the algorithms, and employing algorithms that are finely tuned for the task required by the specific product at hand without expanding their operations beyond their intended use absent human oversight or intervention.

FOOTNOTES

1. With special thanks to Gabrielle da Silva and Louis Althaus for their research assistance.

2. *Moffatt v. Air Canada*, 2024 BCCRT 149.

3. See Reuters, "Waymo to expand autonomous ride-hailing service areas in Los Angeles, San Francisco" (August 6, 2024).

4. Section 9(1)(b) of the federal *Motor Vehicle Safety Act*, SC 1993, c 16 allows companies to apply for exceptions to certain standards to promote the development of "new kinds of vehicles, technologies, vehicle systems or components." Provincial initiatives include Ontario's Automated Pilot Vehicle Program and Quebec's pilot project for autonomous buses and minibuses.

This article was published as part of the Q4 2024 Torys Quarterly, "Machine capital: mapping AI risk".

To discuss these issues, please contact the author(s).