Anatomy of AI projects from the vantage point of export controls

February 26, 2026

Authors

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Anaïs Martini

Lawyer

In a previous Bulletin, the authors broadly outlined the legal framework that applies to export controls, as well as the challenges surrounding large language models in artificial intelligence in an era of knowledge sharing. Given that a number of legal and geopolitical developments covering various aspects of this topic took place in 2025, a brief overview is timely on the potential implications for the development of your AI projects, with a special mention of generative AI (or "**GenAI**"), as the new year begins.

What are export controls?

Export controls establish rules designed to curb the risk of transferring military, strategic and dual-use (civilian and military) goods and technologies to destinations deemed contrary to national security interests. Such technologies can take on various forms, ranging from physical hardware to technical information.

In Canada, export controls are based on a licensing system, under which permits are given based on a series of items listed on the *Export Control List* ("**ECL**") under the *Export and Import Permits Act* ("**EIPA**"). To find out if parts of your AI projects are subject to export controls, you should primarily (but not exclusively) refer to that list and to the guide prepared to better understand the list.

Key events in 2025

Order SOR/2025-89

On March 7, 2025, an Order amending the ECL was published in the *Canada Gazette,* in an effort to include emerging technologies that are increasingly faster and more scalable, the capabilities of

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

which raise concerns about potential adversarial military applications.[1] Of particular interest in this context, subitem 5506(1) of the schedule to the ECL has been replaced by a number of paragraphs and subparagraphs.

But what do these changes mean for AI projects in practice?

The amendments made to subitem 5506(1) do not target AI applications (algorithms, models, data), but rather:

> extreme ultraviolet ("EUV") lithography equipment, namely EUV masks and reticles making it possible to use this technology to manufacture advanced integrated circuits;
> cryogenic cooling equipment and ultra-sensitive amplifiers for quantum computers;
> advanced semiconductor materials;
> development and production softwares related to certain of the foregoing technologies.[2]

In other words, subitem 5506(1) targets the industrial toolbox used to build advanced computers, in particular through its inclusion of EUV lithography, which is used for cutting-edge integrated circuits and quantum computers that are revolutionizing the world of advanced computing. It can therefore be said that these rules affect the AI industry because of a form of hardware dependence, since tight control over these infrastructure manufacturing technologies necessarily affect the ability of a country or company to develop and operate advanced AI.

In sum, these latest amendments are simply the continuation of those made in the previous year's Order, which targeted the fields of quantum computing and advanced semiconductor manufacturing in particular (GAAFETs, representing next-generation integrated circuits).[3]

It has yet to be ascertained how the aforementioned orders will directly affect typical GenAI projects (model development, AI SaaS services, etc.). Those who will experience the more direct repercussions are suppliers of advanced computing equipment and businesses doing R&D on semiconductors, integrated circuits and quantum computing.

Notice to Exporters No. 1159

Apart from the technical components, a certain complexity arises when we understand that the definition of a "technology" subject to export controls within the meaning of the law is meant to be broad, and that it includes technical data, technical assistance and information necessary for the development, production or use of an item appearing on the ECL.

In other words, the scope of the technologies concerned goes beyond simple physical components or equipment. This is especially true given the proliferation of often cross-border cloud-based solutions, which make technical knowledge accessible digitally and circulate it far and wide.

Given this context, it is appropriate to read the *Guidance on the movement to and storage of controlled technology in the Cloud* (Notice to Exporters No. 1159), published in November 2025 by the Government of Canada. The document was prepared to clarify instances when the use of cloud services constitutes a transfer of controlled technology under the EIPA, requiring a permit.[4]

In summary, the guidelines state that:

> it may be considered a **transfer** if a controlled technology is disclosed from a place inside Canada to a place outside Canada;
> a controlled technology is considered **disclosed** if it is sent from Canada and stored in a foreign location in a way that creates a reasonable possibility that a person located outside Canada would be in a position to examine that technology;
> a **reasonable possibility** means more than a mere possibility, but less than the standard of "more likely than not";
> the location of servers hosting controlled technology only matters if it affects the reasonable possibility that the

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

technology could be disclosed outside Canada;
in general, it is considered a transfer when a person located outside Canada holds decryption keys or routine access rights that create more than a remote possibility that the technology may be examined, or when a cloud service provider creates an unencrypted backup copy that contains controlled technology to restore a system after an incident, and that such copy is stored on servers outside Canada where foreign administrators can access it;
when cloud services are used, both the owner of the controlled technology and the cloud service provider have a degree of care and control of the technology.

Thus, not only is there a risk of knowledge sharing where items directly listed on the ECL are involved (whether to manufacture them or otherwise), but the possibility of violating export controls also exists because of the interaction between cloud services and the knowledge that could be transferred (within the meaning set out above), if the cloud contains information about or relates to a controlled technology.

Considerations regarding GenAI

What about GenAI projects?

Despite all of the above, these projects may still suffer indirect repercussions, and not only on highly technical components. You will need to exercise a certain degree of caution regarding the compliance of your GenAI projects because of the amount of information they can accumulate through the various layers of their structure.

Training data

There are the data used during the GenAI's learning phase, before it is rolled out. The amount of this data can be massive, and it can be structured or unstructured. It is used to provide a knowledge base for the model and enable it to produce relevant outputs when it is given inputs. The learning phase is risky if the datasets contain controlled technical information and if the data can be regurgitated or combined when users use the GenAI.

The GenAI's weights, filters, and other operating parameters

These parameters can be compared to physical control buttons—they are adjusted during the GenAI's training and during the configuration of the solution that uses it. They determine how much each input element will influence the response and refine the model (i.e., the structure that allows the GenAI to interpret inputs and generate outputs). In the United States, weights in particular are a hot topic considering the country's export policy, under which they can constitute key parameters for the most advanced AI models.

Inputs

This is the data provided by users to generate relevant outputs (e.g., text, images, structured data) when the GenAI is already rolled out. Such data is used to trigger a response or behaviour from the model. Just like with training data, inputs will be critical depending on the use made of the model and the information disclosed to obtain a response. Conditions consistent with legal requirements must be provided to prevent the model from being contaminated by sensitive data after it is rolled out, especially if it stores all the inputs provided to it for its continued learning.

Outputs

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.

This is what GenAI generates in response to inputs. Outputs can be in the form of text responses or images, codes, or even data-based predictions. Given the above, it will be challenging depending on the datasets conveyed by the GenAI, to ensure that outputs do not violate export controls, as they could make it possible to indirectly obtain information the direct access to which would otherwise be prohibited.

Conclusion

We can imagine that the recent changes to export controls in Canada are just the beginning of an effort to address new concerns arising from this rapidly changing and ever more powerful technology.

Export controls are also not devoid of a diplomatic context. For now, making AI subject to export controls seems to be the preferred mechanism to curb the exponential powers of such technology in Canada. The extent to which this will be done remains to be seen and will be interesting to follow.

---

1. Government of Canada, *Order Amending the Export Control List:* SOR/2025-89 (March 7, 2025): Canada Gazette, Part II, Volume 159, Number 7: *Order Amending the Export Control List:*
2. This is not an exhaustive list, but rather a few relevant examples that apply to advanced computing.
3. Government of Canada, *Order Amending the Export Control List:* SOR/2024-112 (May 31, 2024): Canada Gazette, Part II, Volume 158, Number 13: *Order Amending the Export Control List:*
4. Government of Canada, Notice to Exporters No. 1159 – *Guidance on the movement to and storage of controlled technology in the Cloud* (amended November 10, 2025): Notice to exporters no 1159 – Guidance on the movement to and storage of controlled technology in the Cloud

Copyright (c) Lavery, de Billy, S.E.N.C.R.L. - L.L.P.