Emerging technologies series: Regulating artificial intelligence in Canada, the U.S. and Europe

May 16, 2023

This is part one of a three-part series.

With software such as ChatGPT, artificial intelligence (AI) has become an increasingly hot topic, not only in tech but across all industries – including legal – on a global scale.

On May 4, 2023, BLG Partner François Joli-Coeur was joined by Marc Etienne Ouimette, Global Lead, AI Policy (AWS) at Amazon and Michael Bahar, Partner at Eversheds Sutherland to discuss different approaches for regulating AI in Canada, the U.S. and Europe, preparing compliance programs, and the latest in AI litigation and enforcement.

The below is a summary of the upcoming AI legal framework. To get full details on strengths and weaknesses of legislative approaches, opportunities for interoperability and what businesses can do to prepare, check out the full 30-minute webinar recording or skim the transcript*.

AI legal framework across jurisdictions

As part of Bill C-27, the Canadian government introduced new legislation, *the Artificial Intelligence and Data Act* (AIDA), to set the foundation for the responsible design, development and deployment of AI systems. AIDA's focus is on high impact systems, which are outlined in the AIDA companion document.

In the U.S., government regulators are ensuring they are mitigating risk from AI tools before capitalizing on the opportunities. Existing laws and regulations are going to be applied vigorously by regulators like the Federal Trade Commission, Consumer Financial Protection Board, the U.S. Department of Justice, and others.

With the EU's *Artificial Intelligence Act*, the EU seems to want to establish the gold standard in which all other nations orient their own legislation. Two significant points about the law, which is set to come into force by the end 2023:

1. It will have extraterritorial reach and like the General Data Protection Regulation (GDPR), it's reach could radiate outwards to other places, such as Canada and the U.S.
2. The fines are sizable with the idea that companies internalize costs.

Approaches to legislation differ based on jurisdiction. The two approaches taken are horizontal approach and vertical approach:

Horizontal approach	Vertical approach
Aims to cover all AI solutions and classify them as either high risk, no risk or prohibited, and establish a set of obligations associated with high-risk deployments. Along with a few other countries, **Canada** is trying to take this approach with Bill C-27.	Rather than a top-down approach regulating all of AI, this approach aims to go industry by industry or department by department. This is the approach being taken by the **U.S.** and **U.K.**

To better assist companies on their digital transformation journey, BLG's 3-part webinar series covers artificial intelligence, the metaverse and the Internet of Things. If you have any questions about the legal framework around AI, or the topics covered in this series, please reach out to any of the authors or key contacts listed below.

**Recording and transcript are available in English only.*

Read the full transcript here

François Joli-Coeur

Hi everyone, my name is François Joli-Coeur and I'm a partner in the Privacy and Data Protection Group at BLG. I'm practicing out of the Montréal and Toronto offices. Welcome to the first session of our Emerging Technology series. So we're kicking off the series with a very topical subject – Artificial Intelligence. So since the release of ChatGPT at the end of last year, AI has really been a hot topic in the tech community but also in the legal community and I'm very happy to have two great panelists join us today to talk about this topic from an international standpoint. So we have Marc Étienne Ouimette and Michael Bahar. Marc Étienne Ouimette is Amazon Web Services Global Lead for AI policy. He's advised on organizations and governments on RND scale of support and technology governance policy both domestically and internationally. He sits on the AI Advisory Board of Turtoise Media, is Board Chairman of MTL Centre of Expertise Global Partnership on AI. He's given numerous talks on AI and data policy and before A.W.S., he served as the head of Public Policy at LMDI, a global AI product company headquartered in Montréal.

Our second panelist is Michael Bahar. Michael is a litigation partner in Evershed Southern, Washington DC office and the co-lead of the firm's global cybersecurity and

data privacy practice. Prior Evershed Southern's, Michael served as Deputy Legal Advisor to the National Security Counsel at the White House, as Minority Staff Director and General Counsel for the U.S. House Intelligence Committee and as an active and duty Navy Judge Advocate General.

So in terms of the agenda today, we'll start with a quick overview of the upcoming legal framework on AI and then we'll open the discussion for a few specific topics. We might have time for a few questions at the end, so please feel free to enter them in the Q & A. Please use the three dot button at the bottom right of the screen so not the Chat. So if we don't have time to answer your questions, please feel free to email me directly and I'll be happy to respond. So, let's get into the framework.

So currently there is no comprehensive AI legislation in Canada and even globally as far as I know but that doesn't mean AI is unregulated. Most countries have privacy legislation, for instance, that will apply whenever personal information is used to create an AI model or an AI system is used to make decisions about individuals. There's also a lot of copyright questions for AI. We've heard about that AI generated Drake and Weeknd songs. Human Right laws are also important when an AI system violates Human Rights, for instance, Human Rights laws could apply. In terms of product liability, there is a lot of questions, for instance, who is liable if an autonomous vehicle injures someone. And we're also seeing a lot of initiatives to specifically regulate AI, including in Canada, with Bill C-27, which will introduce the *Artificial Intelligence and Data Act* or "AIDA" and Bill C-27 passed the second reading last week at the House of Commons and it should go to Committee at some point this summer. So I'll start with a quick summary of AIDA to set the stage for the rest of the conversation. In terms of scope, AIDA would apply to AI systems, it's a pretty broad term and it would regulate essentially two types of activities; the first category lists the data that is used for design development and use of an AI system, so this would capture, for instance, an organization that makes the data available to another organization for the purposes of developing an AI model. The second category essentially covers any person involved throughout the lifecycle of the AI system, from the design development, making the system available for use, so for instance, commercializing it, with the organization that uses the system.

What's the goal of the proposed legislation? Well the stated purpose of AIDA is to prohibit certain conduct in relation to AI systems that may result in serious harm to individuals or harm to their interests and AIDA's focus is really on high impact systems and that term is not defined in the legislation, it's left to be defined by regulations, but the Minister of Industry, ISED has released a companion document to AIDA in which it gives a few examples of systems that would likely be considered high impact systems, for instance, screening systems that will impact access to services or employment, biometric systems used for identification and inference systems that can influence human behaviour at scales, such as AI-powered content recommendation systems or AI applications that integrate health and safety functions, such as automated driving systems and systems making triage decisions in the Health sector, which could cause direct physical harm to individuals. There's also an enforcement mechanism with fines that could go up to $25,000,000.00. In terms of key obligations, they will depend on the categories of regulated activities that a person carries out. So there are essentially a few buckets of obligations that apply, depending on the person's role in relation to the system and there are overlaps between the buckets. So the first one is the person who makes available for use anonymized data in the course of regulated activity. Um, this

could be, like I said earlier, person that makes its anonymized data available for another person to use it to train it, to train an AI model. So that person would need to take measures regarding the ways in which the data is anonymized and the use in management of the anonymized data, but the specifics of these obligations would be left to the regulations. The second bucket applies to any person responsible for an AI system. This includes designers, developers, those that make it available for use, for instance, that sell it or those that manage the system's operations. They have obligations to assess whether their system is high-impact and depending on that determination, then other obligations will flow. So, any person that's responsible for a high-impact system will be subject to the most obligations. They will have to take measures to identify, assess and mitigate risk of harm or bias output. They'll need to monitor compliance with these measures, they will need to record these measures and they have notification obligations to the Ministry of Industry if the use of the AI system could result or is likely to result in material harm. And on top of that, there are additional transparency obligations. For those that make available or manage the operation of high-impact system, they must publish plain language description of the system and how it is used. So that was a quick summary of what's may be coming in Canada in terms of AI regulation. So enough of me talking. I'll pass it over to Michael, he can provide a quick overview in the U.S. on that front.

Michael Bahar

Yeah, it's a great question because if you asked me that yesterday, it would be a slightly different answer than if you asked me that just now. This is an unbelievably fast-moving space, not only technologically but from the prospective of regulation and legislation. And I think, you know, one way to sort of think about it, you know, the New York Times, Tom Freedman, the noted columnist, when ChatGPT first really became a splash, he wrote a column and he called it the "Prometheus Moment" invoking the moment in Greek mythology when Prometheus defies the gods and allows humans to have fire. That is often been associated with knowledge and scientific discovery and it's got endless possibilities. Yesterday, however, he wrote another column and this time he used a different, although importantly related myth and he calls it "Pandora's Box" and interestingly if you see the statement by President Biden only about six hours ago, or the Chair of the Federal Trade Commission, Lena Khan, they're starting to be less, this a Prometheus Moment and more, we are now opening a Pandora's Box and we need to really be careful. So for example, President Biden said "Yes, AI is one of the most powerful technologies of our time, but in order to seize the opportunity to present, we must first mitigate its risks." First mitigated risk, right? It's not going to be, you know, from the U.S. perspective like what happened from Web 2.0, right, where the idea was "move fast, create stuff, disrupt, and then figure it out later". Here, whether it's Lena Khan, the Chair of the FTC who came out with the, an opt-ed yesterday or President Biden, or other regulators, they're taking a different approach. You know, first do no harm then try to capitalize on the opportunity. It's a subtle but important shift when you're thinking about AI regulation. In the United States, you know, it's always very difficult for us to pass a law especially when we are now very close to a US election. That's not to say a law's not going to be percolated, but really what we're seeing and we can talk more about this later in the United States is that something that you said earlier, François, is that existing laws and existing regulations are going to be applied rather vigorously it seems by regulators such as the FTC or the CFPB, the Consumer Financial Protection Board, or the US Department of Justice and a bevy of other regulators as well. Again, we'll talk more about that later, I don't see U.S. really having a

federal legislation yet. We obviously can't get privacy legislation yet either, that's not to say places like New York City and Colorado haven't weighed into that and we can talk more about that later. But also, right, we can look to the EU, and they've got their EU AI Act that is pretty advanced, pretty far along and like the GDPR, Europe's Privacy Law, I think Europe is looking at its AI Act to similarly be the model, the gold standard and if not the gold standard, at least the lone star which all other nations ought to orient themselves in their own legislation. Interestingly we were expecting parliamentary approval for that at the end of March, we're now in May, because again, everything, the technology is moving so fast, that they're looking at how can we, do we need to expand this even further. They remain confident we're going to see a law by the end of the year, but it may take a little bit of time to implement it. But a couple, two quick points about that law that are significant; (a) like the GDPR, it has extra-territorial reach, so like the GDPR, it's going to radiate outwards and have an out-sized effect and as Europe goes eventually so too will others including the United States. Number 2, the fines are to use a technical word, ginormous. Uh, right, they can go to something like $30,000,000 euros or 6% of global annual turnover, with the idea being similar to what Biden is saying "We must make sure that companies internalize the costs, not just seize the opportunities." So we can talk in more detail but that's the general overview, again, both from the EU perspective and the psychologic principles based, like focusing on the data input, focusing on no discrimination, discord impact, even trying to root out bias, and being able to be accountable right, and being able to demonstrate that you know what your algorithm does and you can, and the algorithm doesn't discriminate, isn't unfair and its responsible. And I'm going fast, we've got a lot to cover. François?

François Joli-Coeur

Thanks, Michael. I think that's a good segway to a question Marc Étienne. So in terms of different approaches to regulating AI, I believe there are horizontal or vertical approaches. Can you speak a bit on the strength and weaknesses of the different approaches and the respective challenges that they would create for businesses?

Marc Étienne Ouimette

Sure, uh, thanks for having me. Look, um, horizontal approaches are a little bit or exactly like what Michael described that the EU AI Act is trying to do. So it's an over-arching belt that is going to attempt to cover all artificial intelligence solutions, classify them as either high risk or no risk or prohibited and then establish a set of obligations associated with high risk deployments. Essentially like a product certification scheme, provider to be able to sell on the common market of a…. That's the approach by Canada is also trying to take with Bill C-27's Part 3, of the *Artificial Intelligence and Data Act*, and a few other countries are seemingly following a similar path. As Michael pointed out, this somewhat, akin kind of what happened with GDPR, where those Brussels effect where we knew that that the EU approach to regulation and the power of its market but ended up having a bit of contagion effect elsewhere because, you know, companies would want to comply with the EU approach to be able to sell AI, which then begets kind of similar regulations elsewhere. In this case, I think the jury's still out to see whether there will be a Brussels effect. I know there's not, I wouldn't call it Brussels effect, but a Brussels campaign to make it happen in the sense that uh, the Commission and the Presidency are proactively working in many jurisdictions to try to get them to adopt a similar approach and multi-lateral bodies like the Trade and Technology

Counsel or venues where they are very aggressively pushing for alignment with regards to horizontal regulation.

The vertical approach is more the one taken by the U.S. by the U.K., in particular, where instead of trying to have a talk-down approach by you regulate all of AI, you go by department by department, existing laws in the U.S. case and see. So if you have specific regulations necessary for self-driving cars, that essentially is regulated by the Department of Transport or the Ministry of Transport in the UK. Strengths and weaknesses of both, generally speaking, this is just my personal point of view, I think vertical approaches make more sense, in the sense that they are closer to the use spaces they are trying to regulate. It is very difficult to come up with a “one size fits all” set of controls and solutions for AI in the same way that it would be for electricity. Imagine trying to draft like the Electricity Bill, where you’re covering obligations for high powered lines coming down from Northern Canada and your electrical socket for your kitchen or bathroom and your, you know, electrical clients. They have very, kind of different sets of risk analysis that you need to control. So I think a use-case specific approach is a little bit better, and then another issue you face with horizontal approaches and this one is certainly core to issues we’re seeing with C-27 in Canada, is kind of a lack of understanding of the AI value chain. So you talked about person responsible, right, that’s the definition of who’s on the hook under C-27. Well, the way it’s defined essentially everybody from researchers to developers to companies who are deploying to ultimately users are similarly responsible. If you think, and this is an analogy and analogies are necessarily imperfect, but of the eco-system we’ve put in place for ensuring a safe and driving eco-system and safe cars there are distinct obligations based on where you are in that eco-system. So you would not hold a brake pad manufacturer responsible for a driver turning left on a red light, right? So it’s extremely important that you get the people responsible, or the organizations or companies responsible for the right portion of where they are at in the AI value chain. So back to my analogy, the brake pad manufacturer has obligations of transparency on what they get from internal views, they need to meet a certain standard of thickness, they need to be able to explain which cars this can be deployed on and so on. Its not to say there’s no obligation on the brake pad manufacturer but they’re very distinct in what we expect of drivers and what we expect of engine manufacturers and the like. So I’ll stop there for now, but plenty more to talk about.

François Joli-Coeur

Yeah, thanks. Michael, it’s you know, our businesses are already trying to deploy in their businesses there is no, there’s no necessarily specific regulation with respect to AI. How can they think about building a compliance program or is there something they can leverage to build that?

Michael Bahar

Absolutely. And it’s in a sense maybe the good part of the, the aspect that existing laws apply, say the regulators that are going to regulate that. Well they look to those existing laws and leverage your compliance programs with those existing laws and you’ll largely be in good shape for AI. So one of the most specific ones of course is privacy because private information in our personal data is really at the core of a lot of AI. Obviously there’s a lot other things that could be used to fuel the underlying, but if you leverage as an organization, your personal information, your personal data, protection and privacy

programs, you're gonna be in great shape because part of it is getting a handle on knowing what data you have that's going into this model. So if you do DPIA, Data Privacy Impact Assessment, or you have your record of processing activity, that's a great place to start. Um, I think a lot times companies that going in head first into the AI are leveraging their privacy compliance programs. Similarly, if you're in the financial services sector, you're already highly regulated, especially in the United States and you're already not allowed to discriminate or have a disport impact. So now you just have to make sure that the data that's fuelling the AI engines are not somewhat corrupting it. Uh, you have to check the results of it to make sure that the model is not producing unfair outcomes. You have to make sure you've got a monitoring program in place to watch for model drift, etc. So if I could say probably the most important thing that you can do when you're trying to figure out, figure how to use AI which still seemingly there is lack of specificity in the regulation, is intent matters, right? A lot of times the regulators are not going to be able to readily look at your algorithm and figure out things. They're gonna eventually get there and of course if they really try they can. But what they're going to be looking at is your record. Like, hey, does the Board meet on AI? Is it saying, hey, whatever we do, do not, you know, make sure there's no disport impact, no discrimination. Because the flip side and we've already started to see this the Courts, where they will look at public statements made by certain Tech companies and then actually, the whole point of this, like marketing campaign using AI, was in fact, so you have targeted advertising by gender, by age, that's not allowed. So intent really matters as well as the ability if ever challenged, to show your math, or show your workings, like to be able to explain what goes on inside that black box, show you tested it, show you monitor it, very similar to controls in other regimes. François?

François Joli-Coeur

Great, so you're talking about privacy and it makes a good link to the next issue. We see, we advise global companies on complying with privacy laws around the world and those are different in the U.S. for instance, it seems that you're gonna have 50 different state privacy laws, so good luck, Michael.

Michael Bahar

[Laughs]

François Joli-Coeur

Um, you're gonna be a busy person and maybe we're gonna see something similar for AI where organizations will have to comply with different regimes all around the world, so, we're still at the early stages of AI regulations, so Marc do you see kind of effort from governments to build inter-portable frameworks and if not, are there standards that businesses can look at to help themselves comply with, like to prepare to the upcoming regulation?

Marc Étienne Ouimette

Yeah, so I mean it's very early on relatively speaking. Regs are coming, you know, quick and fast and numerous um, as are Bills but their enforcement days are coming into four states, uh, or roughly in general, about two years away. And the framework of the EU AI Act uh, and ultimately the Canadian Bill as well, is essentially to refer

substantive obligations when I talked about the product compliance kind of approach that they were taking. So what you need to comply against to standards bodies, right, so standards and define what you know, transparency entails in given circumstance or what minimizing bias entails in a certain circumstance. And so, those standards are currently in development, you know, at my company, at ADA U.S., you know, we have an AI now standards team that reports into my team that's you know, very proactively working in those standards to be able to get them across the line as quickly as possible. So those standards aren't international, they're mostly happening is ISO, the International Standards Organization, and ultimately, what we hope, is that you'll get to a position where the EU, through it's own standard body, adopts international standards to define what good behaviour is for the ADU. And so if Canada has its own regulation, if C-27 passes, if it refers for transparency back to ISO or for risk management systems to ISO 42001, then ultimately your compliance of 42001 in Canada would, you know be able to be carried like a passport into the EU or Brazil or wherever else, right. Where you're not gonna get alignment likely is in risk classification, so different countries are gonna have different risk appetites or thresholds, if you will, culture has a lot to do with that as well, so what they're willing to lean into or not and so there might be certain applications that are considered high risk in Canada that are not considered in Japan or in South Korea or in the U.S. but if you are considered high risk in one and you certify yourself against the underlying sense of standards, then nominally speaking the objective would be that that carries across different jurisdicions. There's certainly a lot of efforts to drive that way, as Michael was talking about before, there was a press release this morning from the White House and there was another press release an hour after that of, their emerging technology standards strategy and how they like really want to ensure inter-operability between like-minded countries saying kind of declaration of G7 and G20 at the Global Partnership on AI where I am Board Chair and lots of work on that as well, that try to align on what the substantive uh, standards entail.

François Joli-Coeur

Perfect. Um, and what do you, Michael, for those of us in Canada it's always interesting to look at what's going on in the U.S. in terms of litigation and enforcement because you're always a few steps ahead if we think about class actions for instance and the privacies there. Um, are you aware of any interesting enforcement action or litigation on the AI front in the, in the U.S.?

Michael Bahar

Yeah, and I alluded to it earlier, it's, you know, the U.S., a big social media and tech company in a sense, for designing a system that allowed advertisers to discriminate. That's also really interesting. Um, and it goes to something Marc Étienne was talking about is who do you hold responsible. Right. So, the U.S. is, if we look at the statement by the White House, they are very focused on both holding the upstream, you know, those that are actually designing the algorithms and producing these web3 technologies, like AI, responsible as well as those that implement it. Right? And, sometimes when they may start at the top first, as a way to, to trickle down to, to the bottom. But interestingly about that case right there, they went after the upstream for designing a system that facilitates them. Not to say that they're not going to go after the advertisers but they went after that first. Um, and again, what to do about this, right, because you're right, the U.S. can get very litigious, very quickly, where we are very slow in legislation, we're very fast in litigation. Um, and that's why its going to be really

important to have that, sort of, a proactive risk-based comprehensive data strategy which it specifically includes AI. Again, show that you care and a lot of good things will happen. Make sure its all of company, right? Legal, compliance, security, marketing, HR, gov affairs, if you have that, and IT. Bring everybody together like we do already with privacy and cyber security by consider board engagement and allocate risk via contract. Right? That's what we're getting to. This is, you know, to move away from Greek Mythology, if you go to those early days in torts. Right? When a train is going by, an early locomotive and it throws off a flaming squid and they're trying to figure out who has to pay for the burning yard. That's where we are in AI as well, but you can allocate that risk via contract. Hey, if you put it on the designer of the brakes, you know, when they sell those brakes, they'll make sure to flow some of that back up. Right? A lot of those things, if you look at those, it will be a great place to start, and of course again, intent matters. That's all.

François Joli-Coeur

Thanks Michael. So, we're actually almost on time. So thanks again, Marc and Michael for your participation. It was great to have you. Very insightful thoughts for the audience, if you have not already done so, you can register to Part 2 and 3 of series, so, back to the session on the metaverse on May 18 and Part 3 is on Internet of Things on June 8. You will receive the slide decks within a few days with CPD information and that's all. Thank you very much. Have a nice day. Feel free to email me if you have any questions. Bye-bye.

Michael Bahar

Thank you.

François Joli-Coeur

Thank you.

Expertise

Artificial Intelligence (AI)

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.