06 septembre 2023

Lois canadiennes, américaines, britanniques et européennes entourant l'Internet des objets

Cet article présente les faits saillants du webinaire sur l'IdO s'inscrivant dans la série de BLG sur les technologies émergentes.

Les appareils connectés gagnent en popularité, entre autres dans les secteurs des soins de santé, des sciences de la vie, du transport, des infrastructures, de la fabrication, des finances et de l'agriculture.

Dans le cadre de la série sur les technologies émergentes de BLG, notre associée Edona Vila s'est entretenue avec deux avocates spécialisées dans la responsabilité du fait du produit et la sécurité des produits, Rachel Raphael, associée chez Crowell & Moring, et Katie Chandler, associée chez Taylor Wessing. Ensemble, elles ont discuté de l'état actuel de la législation entourant l'Internet des objets (IdO) dans divers territoires, comme les États-Unis, le Royaume-Uni, l'Union européenne et le Canada, particulièrement en ce qui concerne les questions de conformité et les défis connexes de même que les pratiques optimales pour les entreprises qui déploient des solutions IdO au-delà les frontières.

Le sommaire qui suit expose la manière dont les lois existantes dans divers territoires peuvent s'appliquer aux questions liées à l'Internet des objets au Canada, aux États-Unis et en Europe. Pour tout savoir sur les enjeux de conformité, vous pouvez visionner l'enregistrement du webinaire, d'une durée de 30 minutes, ou prendre connaissance de sa transcription*.

Lois actuelles concernant l'Internet des objets : ce qui se fait ici et ailleurs

À mesure que les appareils de l'IdO se démocratisent dans plusieurs secteurs, les gouvernements doivent examiner la législation en vigueur et déterminer si de nouvelles lois s'imposent.

États-Unis

Que ce soit au palier fédéral ou à l'échelle des États, nos voisins du Sud ne se sont pas dotés de beaucoup de politiques qui ciblent la réglementation des appareils de l'IdO de façon globale; toutefois, certains États, dont la Californie, ont adopté des lois qui les visent spécifiquement. Entrée en vigueur au début de 2020, la loi de la Californie sur l'IdO impose aux fabricants d'appareils connectés l'obligation d'équiper leurs appareils de certaines caractéristiques de sécurité qui cadrent avec leur nature et leur fonction et avec les renseignements qu'ils recueillent.

Plusieurs normes sectorielles américaines offrent également certaines lignes directrices, comme celles de l'ASTM (organisme anciennement connu sous le nom d'American Society for Testing and Materials), guide par excellence pour ce qui est d'assurer la sécurité de produits de consommation connectés; elles abordent notamment la question des mises à jour à distance, des logiciels et des micrologiciels, du risque de configuration et de certains contrôles de cybersécurité. De plus, Underwriters' Laboratories propose une cote de sécurité de l'IdO, qu'elle fournit au terme d'un processus d'évaluation de diverses méthodes d'attaques visant certains produits intelligents.

Malgré le manque relatif de réglementation, certains acteurs de l'industrie et États donnent le ton pour ce qui touche la norme de diligence.

Royaume-Uni et Union européenne

Bien que la réglementation et la législation entourant l'IdO continuent d'émaner en grande partie de ce qui se fait dans l'Union européenne, certains changements survenus après le Brexit distinguent le régime britannique de celui de l'UE. Bon nombre des activités de traitement sécurisées liées à l'IdO seront visées par le Règlement général sur la protection des données (RGPD), loi européenne régissant la protection des données. Comme les appareils de l'IdO peuvent traiter des données personnelles, les fournisseurs concernés devront s'assurer de se conformer à ce règlement.

La cybersécurité est un autre aspect essentiel. En plus de la Loi sur la cybersécurité de l'UE, une multitude de lois sont en cours d'élaboration dans l'UE et au Royaume-Uni afin de réglementer les risques de cybersécurité liés aux produits de l'IdO, dont la directive NIS2, qui énonce des normes et des obligations précises en matière de cybersécurité portant notamment sur la communication d'information instantanée et d'autres obligations visant les fournisseurs de services numériques, et la Loi sur la cyberrésilience, qui point à l'horizon et a pour vocation de réglementer le matériel informatique et les logiciels, en particulier ceux qui comportent des éléments numériques.

En ce qui concerne la sécurité des produits, la création très récente de la directive relative à la sécurité des produits, loi européenne approuvée dernièrement, figure parmi les nouveaux développements. Il s'agit en fait d'une version remaniée des actuelles General Product Safety Regulations visant à les mettre à jour compte tenu des avancées technologiques et numériques et à englober les produits physiques comportant des éléments logiciels et connectés.

Canada

À l'heure actuelle, le Canada ne dispose d'aucune législation visant précisément l'IdO; son approche de la réglementation de ces solutions est généralement fragmentaire. On s'attend à ce que le cadre réglementaire entourant l'IA au Canada influe sur les solutions IdO propulsées par cette technologie ou présentant des fonctionnalités qui s'appuient sur celle-ci.

Le Canada planche sur une législation adaptée à l'IA qui, lorsqu'elle entrera en vigueur, devrait entraîner des modifications à son cadre législatif ciblant les produits de consommation. Reste à voir comment les choses évolueront au pays, mais le cadre visant l'IA aura certainement une incidence sur les solutions susmentionnées.

** L'enregistrement et la transcription sont offerts en anglais seulement.*

Transcription

Emerging Technologies Series: The Internet of Things (IoT)

Edona Vila	Welcome everyone and thank you for joining us in our emerging webinar series with today's discussion focussed on the developing IoT law across jurisdictions. For today's discussion we're joined by two product liability and product safety lawyers, Rachel Raphael of Crowell & Moring to provide the U.S. perspective and Katie Chandler of Taylor Wessing to provide the U.K. and EU perspectives. I'd like to introduce both panelists formally but I see, or you see, also, on your screen, you'll have their contact information as well. My name is Edona Vila, and I'm a partner in the Toronto office at BLG, focussing on product liability and product safety generally, although most of the time I'm a litigator in relation to product disputes. But in terms of our panelists today, I did want to say a few words, so you get to know them a little better. Rachel is a Partner at Crowell & Moring where she's a member of the firm's Mass Tort Product and Consumer Litigation and Product Risk Management groups. Rachel advises clients on a range of consumer products' issues with focus on product safety and regulatory compliance. Rachel's practice focuses on a broad spectrum of complex commercial, consumer and retail litigation, including defending class actions and multi-district litigation. Now I'd like to introduce you, Katie. Katie is a Partner, as I said, at Taylor Wessing. She's based out in London, U.K. She leads the Product Liability and Product Safety team in the U.K. at Taylor Wessing. She's a litigator with broad experience in the technology, life sciences, automotive, consumer and retail, and food and drink sectors. Katie regularly works with clients in the technology sector with a focus on emerging technology such as automated vehicles. That's one connected asset that we have in common, Katie; 3D printing and Internet of Things, that's very apropos for today's discussion. So just to provide a bit a roadmap of our discussion today, we'll canvass two segments. In the first segment, we'll discuss a little bit the current state of IoT law across jurisdictions in the U.S., U.K., EU and Canada and for the second segment, we'll focus on compliance issues, compliance challenges and best practices for businesses deploying IoT solutions across borders. So without further ado, we'll start off with our first segment on the current state of IoT law. We'll engage in a level setting, if you will. So perhaps Rachel, we'll start off with you, our neighbours to the south, who are the recipient of much of the Canadian smoke issues right now with the wildfires *(laughing)*. Switching gears in terms of the current state of IoT laws, what's brewing in your jurisdiction?
Rachel Raphael	Sure. So, in the US there are not many policies at the Federal or State level that are focussing on regulation of IoT devices more generally. There are some states that have adopted IoT specific security laws. One of the first adopters of those, frankly not surprising, is California. California's IoT law was enacted at the beginning of 2020 and imposed a security requirement for manufacturers' of connected devices. Requires those devices to be equipped with certain security features, all tailored to the nature and function of the device and the information it collects. And there are also several industry standards out there that provide guidance. You have ASTM, the standard guide for ensuring the safety of connected consumer products which provides guidelines for different things like remote updates or software and firmware, configuration risk and certain cybersecurity controls. You also have an organization called Underwriters' Laboratories here in the US that have an IoT security rating. So it's an evaluation process that rates certain smart products on common attack methodology with various levels of security ratings. So, you know, despite the kind of relative lack of regulation, there are some industry actors as well as some states that kind of set the floor when it comes to the standard of care here.
Edona Vila	Very helpful. Moving across the Atlantic, we'll go to Katie with sort of the state of play in the U.K. and EU in respect of IoT law generally and specific regulation or legislation around IoT.
Katie Chandler	Sure, so, I mean at the moment, it does still derive from EU law predominantly and post Brexit, you know, there have been some changes and there are some new laws coming which will separate the sort of U.K. regime from the EU regime. But, for the purposes of this, I'll sort of broadly talk about them as, you know, a marriage, still a marriage. This really, it's a hodgepodge of laws and regulations that come from the sort of general umbrella legislation for data protection. So many of the safe processing activities involved in IoT will fall within the space of the general data protection regulation and you know, IoT devices can process personal data, so you know, IoT providers have to ensure that they are complying with those requirements under the GDPR. Cybersecurity is obviously another key feature and there's a whole raft of legislation and EU legislation and that which then is commenced in the U.K. to, you know, try and regulate the cybersecurity risks in relation to IoT products outside the Security Act. Ummm we've got the NIS2 Directive which sets out particular cybersecurity standards and obligations on instant reporting and other particular obligations on digital service providers and then we've got some proposals coming down the pipe for the *Cyber Resilience Act* which is on the horizon and it's aiming to focus security on hardware and software and particularly the software with digital elements. So we are talking about smart home devices as well. Not entirely clear at the moment when that will come into force but, you know, we're probably looking at the next couple of years. And then on the sort of product safety side, there has been a very recent development which is the introduction of the new proposed General Product Safety Directive. Now, this is European legislation. Post Brexit it won't be directly applicable in the U.K., but basically it's a re-work of the General Product Safety Regulations which are currently in force to bring it up to date with the digital age and advancements in technology and to expressly refer to and cover those products where a physical product meets a software and connected element to it. The text of the new General Product Safety Directive was approved only a couple of weeks ago and it is now admitted into EU law and will be applicable by the end of next year. And just sort of at a very high level and I know we've got lots to discuss today, it covers those products that are not caught by sector specific products. And so you've got medical devices that fall under the European Legislation of the Medical Devices Regulation, you've got toys that fall under the Toy Safety Regulation, cosmetics, other products. The General Product Safety Regulations and now the new General Product Safety Directive is a sort of over-arching protection in respect of the general consumer product. But why it's interesting, is it has now, you know, sort of grapple with some sort of framework around the safety of IoT products. The Medical Devices Regulation has done that as well and the updates to that in 2021 were to make it clear that any conformity assessment and marketing authorization for a sort of digital health product that was incorporating IoT, was going to fall within that regime and, but as I say, some of the other legislation hasn't quite caught up. But just really briefly, what the General Product Safety Directive is now expressly providing for is, you know, interconnected products. So where there is a product that is interconnected to other items and then, you know, it falls under this regime and it also seeks to expand aspects of how you assess the general safety of that product. So you would look at the warnings, the labels, the instructions for use. But now this new legislation is specifically including the effects on other products where it's reasonably foreseeable that it will be used in other products. So again this is going to the interconnection point, the effect that other products might have on that product where it's you know, being used or, you know, including sort of, the effect of non-embedded items, what's the effect of cybersecurity features and potential malicious third party risks, what's required to protect the product and it's safety, if there are evolving learning and predictive functionalities, so this is of relevance, to it's AI system. And really importantly, what's the state of the art and technology that is sort of applicable for the opinion in terms of understanding the safety of that product. So a real shift and move towards getting it up to date. And I'll just say very briefly, it's not going to apply in the U.K. because of Brexit. But our product safety, our product of safety standards is conducting its own assessment and review of the current regime because the general understanding and view is that these existing laws are very old and that this particular legislation is 20 years old. We've got product liability legislation that is 35 years old. Doesn't necessarily cover IoTs.

Edona Vila	That's very interesting and a perfect segway into my next question and just briefly for those tuning in and certainly from a Canadian perspective, we don't have IoT specific legislation yet. Very much of us are of a piece meal approach of regulating IoT solutions across Canada, but we do have an interesting development when it comes to AI specific legislation that dissipated to also cause some amendments to our consumer product legislative framework when it does it come into force. It's not anticipated to come into force any time soon. Any time soon being this year, it's just making its way through our federal system right now. I think its just passed second reading and so it will be interesting to see in terms how we move in our jurisdiction, but certainly our AI regulatory framework is anticipated to impact those IoT solutions that are AI empowered, and have those AI features through them. In terms of positioning it seems like we are positioned at least for the proposed AI regulatory scheme, somewhere in between where the EU is and where some U.S. States are. very much how Canada moves in this space, so perhaps not completely surprising. So just tagging along in terms of the next piece, Katie you touched on this, so maybe I'll switch gears with U.S. perspective with Rachel, but is there a gap, Rachel, in the current regulatory framework in the U.S. in regulating IoT and if so, how is it being addressed?
Rachel Raphael	Sure and I'll say, you know that I'm obviously speaking given my background from the interconnective products' product safety lense, when I talk about this and that kind of informed my prior answer which you know, was the point that like Canada I think it's really been left up to the States thus far and it's a bit of a patch work. So given the lack of some kind of uniform regulation there are some gaps to fill. I do think that IoT products and the risk associated with those products are certainly on the radar of many U.S. regulatory agencies and that includes the Consumer Product Safety Commission and the Federal Trade Commission, the National Highway Traffic Safety Administration and the FTC in the U.S. remains, kind of the nation's lead data security and private enforcer at the federal level, and its view of those issues has significant ramifications for the companies that make, distribute and sell internet connective products but companies are kind of largely left to cobble together much of the guidance by looking at what States have done and looking at you know, past enforcement actions for example. I think we are slowly working towards something that is considered universally acceptable and that's where kind of filling in the gap fits in. Very recently in April, guidance was published by the Cybersecurity and Infrastructure Security Agency along with FBI, NSA and other cybersecurity authorities around the world that are a step in that direction. This guidance is called shifting the balance of cybersecurity risk and it's the first of its kind. It outlines several core principles to guide software manufacturers when they are building software security into their design processes prior to developing, configuring and shipping their products. I think historically it's often been kind of thought on as an add on or an after thought and the idea of this guidance is to make integral, kind of an each stage of the development process. And there are a couple of core principles that I will just mention briefly. The first is kind of taking ownership of the security outcome. So you know, security should be the baseline, is the idea, and products should automatically enable the most important security controls that are needed to protect, you know the product, the information that they collect, etc. from kind of malicious cyber actors. Another principle has to do with embracing transparency and accountability and also building the right organizational structure even from the executive level on down, that prioritizes software security as a critical element of product development. And then as mentioned kind of the theme of the guide codes that this new guidance sets out is integrating security as early as possible into that design process for IoT connected products.
Edona Vila	Thanks Rachel, and Katie I know you touched briefly on this but what are you seeing in terms of gaps in your jurisdictions. I appreciate you covering the EU perspective as well, and whether it is ... are you seeing sort of a more siloed approached to regulating different types of connected assets in terms of what's, what's currently circling?
Katie Chandler	So EU is pretty, well it's moving pretty fast, I would say and the U.K. is slower. In terms of the gap, there is, I'm just leaving data protection aside and potentially cybersecurity there's quite a lot coming down the pipe on that. But like the liability framework is where there has been real gap and the uncertainty that comes with whether or not they can see the safety laws as they currently stood applies to IoTs and you know what sort of liability regime would they fall within, because of course, the question of liability are complex. You know there's the risk of third-party involvement, who can hack and access the IoT and cause a problem which might lead to harm. There's the design defects and design security flaws that Rachel was just discussing and there's also potentially what the customer and user might do that might lead to any sorts of damage and or any sort of failure and of course you know the updates that the software developers provide of course. So all of these sort of questions of liability really haven't been dealt with and whilst the general product safety directive that I mentioned goes some way to addressing the sort of safety regime, the liability regime is still very much unclear and the product liability directive which is the EU legislation and is implemented in or locally among the member states and in the U.K. is implemented under the Consumer Protection Act and does not necessarily, as it currently stands and it's five years old, cover IoTs because the IoTs are, they are not mutable tangible goods, so you've got IoTs that are ecosystems, that you know have got a lot of range of elements and you know some embedded into hardware, some not. So the big question around software and what the software falls within the existing product liability regime, has been one that has been debated heavily. But just very briefly, being conscious time, what has happened in the EU is that they are taking this very centralized approach to the liability framework for IoTs, for AI integrated systems and looking ahead for whatever the future may hold in relation to advanced technologies. They have currently going through the European parliament is the AI Act and I won't talk about that in detail today because we are focusing on IoTs, but there's the AI Act, there's the AI liability and directive which is being proposed which is the first of its kind and then there is a entirely new draft of the Product Liability Directive. That will not apply to the U.K. post-Brexit but it's very important for any company who is placing products in the EU market, its currently going through the European parliament for debate, and there might be some changes, but the general mood is that it will probably stay as proposed in the draft, by and large ... there might be some amendments, but that could come into place as soon as sort of the next 18 months to 2 years, but getting the crux of why that's important is that that's a strict liability regime so a consumer who suffers harm from a product, doesn't have to establish faults or negligence on the parts of the manufacturer or, now in the new case, in the new draft, the software developer or other third party that has been involved in the design of the product, and they just need to establish that it was defective and some key changes that the new PLD by way of update, are bringing in, will put IoTs and tech and companies firmly into the scope of that strict liability regime. Digital products are going to be, you know now in scope by way of widened definition of product, so software will be caught and it's defined and includes embedded or standalone, it includes AI systems, digital manufacturing, like 3D printing, digital services such as navigation services in autonomous vehicles for example. So that's going to be proposed because the definition of products is going to be widened to some real extent. The expanding definition of what damage is covered is really relevant as well because at the moment, you're liable if your defective product causes death or personal injury. The proposed amendments are suggesting that that should be widened to include losses that arise after the loss or corruption of data. Personal injury could also include some sort of psychological health, some sort of impact that it might have had on your mental health, and that sort of brings into debate some interesting questions around children's products, for example, where you've got a connected toy device of some sort or something where there is some element of loss of data that also causes some sort of physical health impact. And there's a massive question mark as to whether or not that's going to cross over with the GDPR and what really is this regime going to look like, which route is this regime is going to take. And then finally there's a new definition of "defectiveness" which is going to firmly bring in an assessment of whether complex systems like IoT devices were safe as a consumer was entitled to expect. It's an objective sort of safety test at the moment but it's really challenging in the context of IoT's because the consumers do not know much about the software behind the IoT's. It's really difficult to decide whether there are devices functioning properly and these can sometimes act autonomously, make it really hard to describe what sort of level of safety is that should be expected. And then because of all these difficulties with trying to establish for the consumer to bring their claim, because we're talking about complex products, they are suggesting a radical change, and this is quite significant for European clients and European companies because they don't have the regime of disclosure and discovery like we do in the U.K. and the U.S. There's going to be an obligation on manufacturers to give disclosure of some documents around the solutions and potentially trade secrets, confidential information that they will have to be protected for in some way, but the legislation is currently drafted. It's not at all clear on that, but this is, in a way it's a really important questions about the party data, other sort of potential data that's embedded in the IoT, so that is a real change and that's really sort of caused a lot of debate from stakeholders, so it's a bit of watch this space on that, but the liability framework which is being developed by the EU and the European Commission is really sort of moving at some pace so everybody who have products that they market in the EU market should be well aware of those.
Edona Vila	That's fascinating in terms of comparing different jurisdictions because for our next segment, we'd really like to focus on really these compliance challenges for certainly companies that have products that pass borders and in this particular regulatory framework and developing liability frameworks, what's your... we'll go to Rachel first. Rachel, what are the top sort of, maybe I wonder if you can combine both sort of the challenges but also the best practices in terms of how to best solve for those challenges for companies that operate across various borders?
	Of course, of course. So I guess being consistent with what I've spoken about today. You know, the biggest challenge for companies really is where to look. Right? We have some developing standards out there related to IoT products, its the one I've just described but there are, really the lack of anything that's considered universally acceptable, is I think the biggest challenge and it leaves companies guessing a little bit as to the best path forward and it presents a unique risk, particularly, in my mind, as a litigator, for product liability base claims

Rachel Raphael	that are probably next on the list. For those that are premised on some violation of a duty or the inability to satisfy some standard of care, not knowing what that standard of care is, presents some really unique problems for companies. And we're seeing some real indications coming out of some of our sources of guidance like the recent FTC enforcement, that agencies are serious about putting the onus on the actor who's in the best possible position to ensure the safety of these devices. And kind of in the same spirit as the recent guidance that I mentioned earlier, these themes of transparency and accountability and structuring your organization around prioritizing security in your products. You have the FTC holding executives of companies, kind of individually and personally responsible for failure to implement certain security practices. Requiring them to comply with certain obligations whether they stay at that company where there was that data breach or not. One helpful example, is not in a IoT specific context, but in October, FTC took action against an online alcohol marketplace called *Drizly* and its CEO for violations of the FTC Act that prohibits unfair deceptive practices because the allegation was that the company was making false statements about certain practices when it actually had inadequate security that has led to prior data breaches. And what was really unique about this recent enforcement action was that Mr. Rellas, the CEO, is being named personally, and it alleged that he was responsible because he was the one who could have implemented or delegated the responsibility to implement security practices and he failed to do so. He didn't hire anyone at a senior level to kind of implement these steps. And so the FTC proposed in its order, the order would require not just the company to implement and maintain security programs but actually for Mr. Rellas personally to do that, and these obligations would travel with him even if he left *Drizly* which I thought was really interesting. So it's clear that this is a priority and the idea being of who's best situated, that's who should bear the brunt of the liability and the obligation to kind of bring products into this next generation and secure them. Again, the vulnerability that we now face in this evolving environment, and I'll just say really briefly because I know we're really short on time, but in terms of best practices to solve these challenges, I think there are a number of ways that companies can try and stay one step ahead in what really is kind of a constantly evolving environment, both in terms of the technologies and the products that are being developed, and in terms of the regulatory landscape. But it has to do with, first it's your compliance and litigation readiness effort, it's enhancing compliance programs to account for kind of evolving product liability. There really is a potential for more product liability lawsuits. We haven't seen a lot of that in the US, and everyone from the in house legal team to the folks who design the products need to know from a design perspective what the potential failure modes are to products and be able to show that the company went through those issues prior to launching. And the legal department also needs to stay in the loop about product design and maintenance decisions because it's working together that the company, kind of more holistically can try and ensure that safety and liability issues are understood and then if possible, dealt with. I think adapting written information security policies that incorporate IoT products are incredibly important. Taking advantage of the technology, everyone from the legal team to your engineer should understand exactly how these products collect and disseminate data. Be prepared. Have an internet response plan that spells out exactly what folks should do and train your employees as to how to carry that out. Keep learning. So companies should be playing devil's advocate, putting themselves in the bad actor's shoes. Who would be interested in that? What would they be looking for? And just better understand the risks that you face. And also learn from experience of others, your peers. Maybe take a little pleasure at others' misery but try and keep up, right, with other breaches that are publicized and learn from what went wrong there, even if you haven't ... if you've been lucky so far. It's frankly only a matter of time in some circumstances.
Edona Vila	Thanks Rachel, because that summarizes what I would say from a Canadian perspective. Katie, any parting thoughts in 30 seconds or less?
Katie Chandler	Yeah, I would really agree with all of that and it's also highly relevant to EU and U.K. as well. Yes, its just I think simply ... I mean warnings and IFU's and just thinking about your labelling and all of that, it's just the difficulty is obviously in making sure that it's consistent to meet regulations and standards across the different jurisdictions if you are a global product, fine and your product is being placed in different jurisdictions. There are different levels and as you've seen the EU has got some quite stringent regulation now that may affect some of your IFU's and instructions and warnings.
Edona Vila	Thank you both of you. I really enjoyed our discussion today. I think we could go longer. Thank you to everyone joining us today and the BLG crew for facilitating this third webinar series. For those of you that have missed the AI and the Metaverse webinars, let us know, we'll make sure you get the recordings. And sorry we didn't have time to address questions but if you have any, feel free to reach out. Thank you all, have a great day.
Katie Chandler	Bye.
Edona Vila	Bye-bye.

Par : Edona C. Vila

Services : Technologies

Principaux contact

Edona C. Vila
Associée

Toronto

EVila@blg.com

416.367.6554

Martin Abadi
Associé

Toronto

MAbadi@blg.com

416.367.6158

Eric Boehm
Associé

Toronto

EBoehm@blg.com

416.367.6041