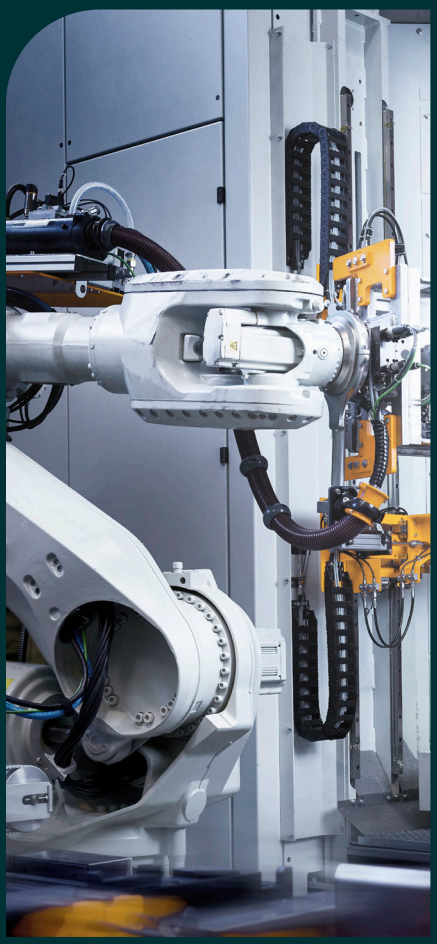
unisys

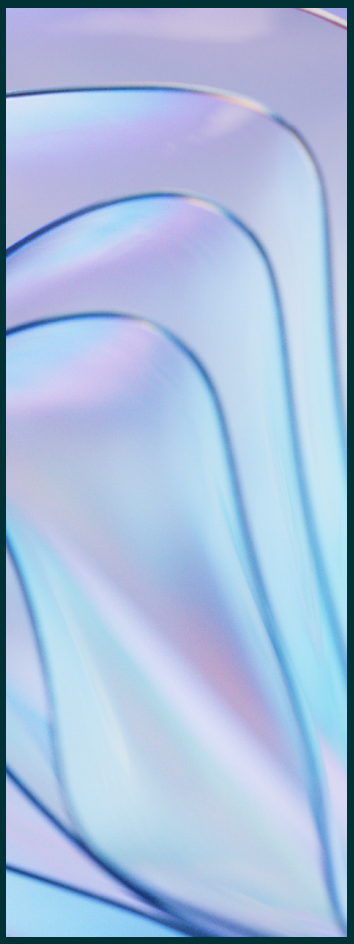
Complying with evolving regulations for AI and machine learning and implications for the cloud

Expert insights from a Unisys webinar: Standing at the crossroads: the increasingly complex regulatory landscape.

Featuring:

- Suzanne Taylor, Ph. D., vice president, innovation and emerging technologies, Unisys
- Michael Egan, partner, Cooley LLP





Complying with evolving regulations for AI and machine learning and implications for the cloud

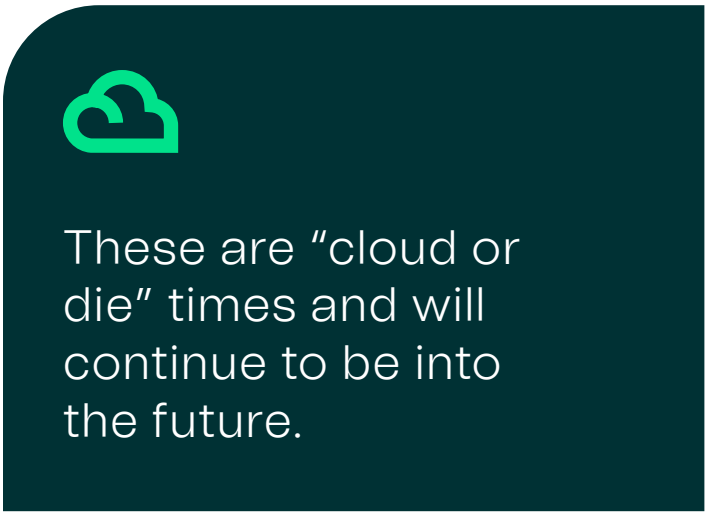
The cloud is taking AI and machine learning mainstream

If there's one thing the COVID-19 pandemic has tested, it's the agility of businesses to respond to unprecedented disruption. Some companies seemed to transition to remote working effortlessly. Even their finance departments successfully closed their books each month – no paper required. These businesses had already digitally transformed core operations by moving to flexible, secure, cloud-based solutions. In contrast, businesses that had put off digital transformation felt the pain acutely, stumbling their way through lockdowns, unable to swiftly make the switch to remote working, selling and customer service.

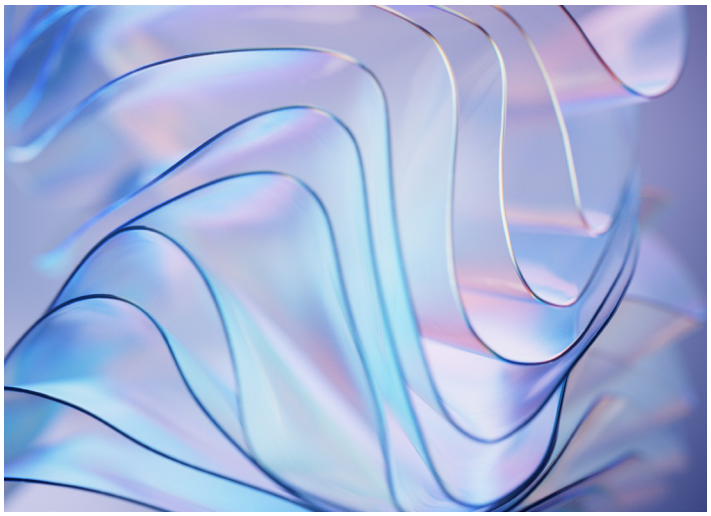
No wonder Microsoft CEO Satya Nadella stated that just a few months into the pandemic, his company "had seen two years of digital transformation in two months as its customers started adopting cloud solutions."1 These are "cloud or die" times – and will continue to be into the future. The cloud also gives businesses fast, affordable access to artificial intelligence (AI) and machine learning (ML) technologies previously only available to the largest and wealthiest tech firms. These early adopters – such as Amazon, Google and Microsoft – have built cloudbased AI and ML solutions and services that make these technologies available to any business – no up-front expense or technology expertise required.

However, as explored in a webinar hosted by Unisys, "Standing at the Crossroads: The Increasingly Complex Regulatory Landscape," deploying these technologies in a way that meets increasing security and compliance demands is no small task. In this webinar, thought leaders from Unisys, including Suzanne Taylor, Ph. D., Vice President, Innovation and Emerging Technologies, and guest Michael Egan, Partner, Cooley LLP, discuss wide-ranging legal, ethical and yet-to-be-defined regulatory topics with which highly regulated businesses must contend. As businesses move forward with cloud-based solutions, these topics warrant additional consideration.

Most industries still lack clear regulatory guidance on AI and ML technologies. In the case of emerging technologies, there can be a serious disconnect where the regulation can't keep pace with the technology, resulting in laws that are several years behind the technology it seeks to regulate. While we see emerging regulation in the EU and cloud-related rules embedded in other legislation, specific cloud infrastructure regulation is largely absent or in development.



These are "cloud or die" times and will continue to be into the future.



Given how quickly technology is moving, this is no surprise. "Just a few years ago, cloud computing was a challenge, and people were trying to figure out how to make it work," explains Egan. "Now it's everywhere. As businesses push forward with using new technologies to solve problems and innovate, there's a real need for new data privacy laws and technology laws that provide frameworks and protections for individuals and nation-states – but in a way that doesn't hinder innovation and growth."

At the same time, there are many unanswered legal and ethical questions around technology use, especially in highly regulated industries that demand, for example, decision transparency and protection of personal data. Businesses must look at these issues in the context of "What regulations do we think will likely apply to new technology? How can we keep innovating and make it work from a regulatory perspective, knowing that it's not going to be perfect?" What follows are highlights of this discussion.

Innovating while regulations evolve

For businesses in highly regulated industries that want to harness the latest AI and ML technologies, one thing is clear: Being agile is essential to success. As noted by Egan, "Everyone is trying to deploy these new technologies in the current regulatory environment, which is always going to be a bit behind where the technology is. This gap creates a 'square peg in a round hole' syndrome for innovators that is further complicated because the regulatory environment is continually evolving. So, what might work now may not work in six months, a year or two years from a legal and regulatory perspective."

Public and advocacy concerns will drive change

Regulatory changes rarely happen in a vacuum, of course. Public perception, which is shaped by the media, advocacy organizations and peers, can influence regulatory priorities and outcomes. "We've seen this in the personal data space where privacy advocates have brought about huge shifts in the regulatory environment, from the elimination of cookies to data transfer rules and more," adds Egan. "And we already see this happening with AI."

In the case of emerging technologies, there can be a serious disconnect where the regulation can't keep pace with the technology, resulting in laws that are several years behind the technology it seeks to regulate.

For example, when something goes wrong with an AI solution – such as a driver using an autopiloted electric car in a hands-free mode that gets into a severe crash – it's quickly shared through news stories that influence how people understand AI. These stories lead to exposure bias and even fear that people are not in control with AI. It's a fundamental, very primal fear of control being taken away. We see this happen in the biometric space as well, where people hear stories about people being put on no-fly lists because their facial recognition data matches up with someone on a terrorist watch list, and they can't unwind it. It incites fear not just of man against bureaucracy, but of man against machine.

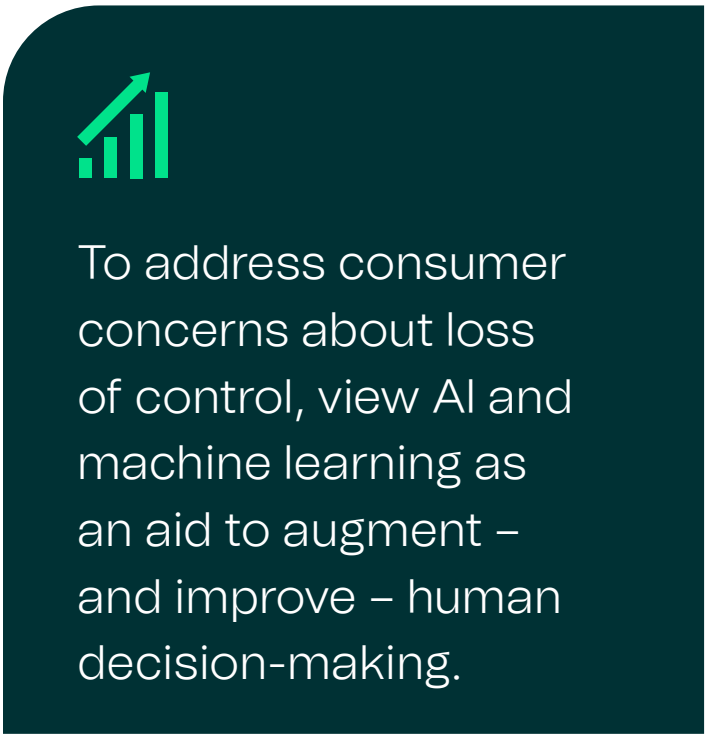
Should businesses postpone AI and ML initiatives until regulations are more defined?

"Absolutely not", says Taylor. "You don't want [caution] to hinder progress. The key is understanding the relevant issues around emerging technologies and figuring out if you should design for the most stringent potential regulations – or just most of them."

The takeaway? Be thoughtful about how you develop your technology while remaining true to core principles like data privacy by design. Build flexibility into your solutions and pricing models so you can be responsive to regulatory change.

So, what kinds of concerns and issues are rising to the top and influencing future AI and ML regulations? And what strategies can be used as "checks and balances" for them?

Let's take a closer look at the perspectives the thought leaders shared in their wide-ranging discussion.



To address consumer concerns about loss of control, view AI and machine learning as an aid to augment – and improve – human decision-making.

Key considerations for innovators

1. The explainability expectation

Explainability in AI and ML – the ability to trace the input all the way to the output, much like a decision tree – is gaining momentum as a regulatory requirement. "In some highly regulated industries such as banking, finance and even healthcare, you need to have perfect traceability of every step back to the decision," states Taylor. "So, the question is, how do you deploy AI, or deep learning and neural networks, if they are 'black-box' approaches that can't be fully traced?"

You can't, in most cases. As Egan notes, "The whole purpose of AI neural networks, that black-box approach, is that it can get to a deeper level of understanding than a human can actually just 'trace' through. The problem is, if you can't explain the output, you can't explain that it was right – and you can't explain where it might've gone wrong in some cases. As a regulatory standard, it's a tough one to keep up with."

In other words, you may not be able to use certain AI and ML techniques, even though they may provide close to the same decisions – or even higher levels of accuracy – than traditional analytics.

Recommendations

One way of working around the explainability issue is to focus on related goals of transparency and the ability to reproduce results. "Scientists have always been very good at the rigor and discipline around this," explains Taylor. "But now, businesses must be able to reproduce how they created their AI models and demonstrate that these models behave consistently when fed the same data." This ability will require building testing into model development so companies can prove consistency rather than explainability.

2. Consumer protection requirements

As noted previously, many people are fearful of fully automated AI and ML technologies because they associate them with losing control – and for good reason. Having out-of-control bureaucracies and autonomous machines turned against people is the stuff of nightmares. Without proper regulations and controls to protect them, people have reason to fear, notes Egan, and regulators are equally concerned. "There's this idea of a human right to not be subject to automated decision-making. We're seeing privacy regulations emerge stating that there must be a human check to ensure that everything's okay."

Then there's the concern about model bias. This occurs when AI and ML models "learn" to be biased because the data fed to them is already biased. Regulators know bias can distort the decisions made by AI and ML models and lead to unfair and inequitable outcomes for consumers. "That's where you get into the ethical issues," explains Egan. "And those are brought into the regulatory environment in different ways around the world. For example, in the U.S., the FTC and several attorneys general have been looking at this and how to determine if companies are using AI and ML to engage in discriminatory behavior."

Recommendations

The speakers agreed that organizations deploying AI and ML in the cloud must align with existing consumer protection laws to overcome these issues. The challenge, of course, is that these laws can vary widely by country and region. For example, the draft anti-discrimination laws in Europe specify certain things that AI should never be used for, including surveillance, real-time biometrics and social scoring of individuals. Yet these are the most common use cases for AI deployments by the Chinese government. This highlights the need to address and incorporate ethical considerations into not only the language but also the implementation of relevant legislation.

To address consumer concerns about loss of control, Taylor advises viewing AI and machine learning as an aid to augment – and improve – human decision-making. For example, a major university invented a little robot – an AI coach – to help an ER department optimize beds by recommending where everybody should be placed. The nurse still made the final decisions, however.

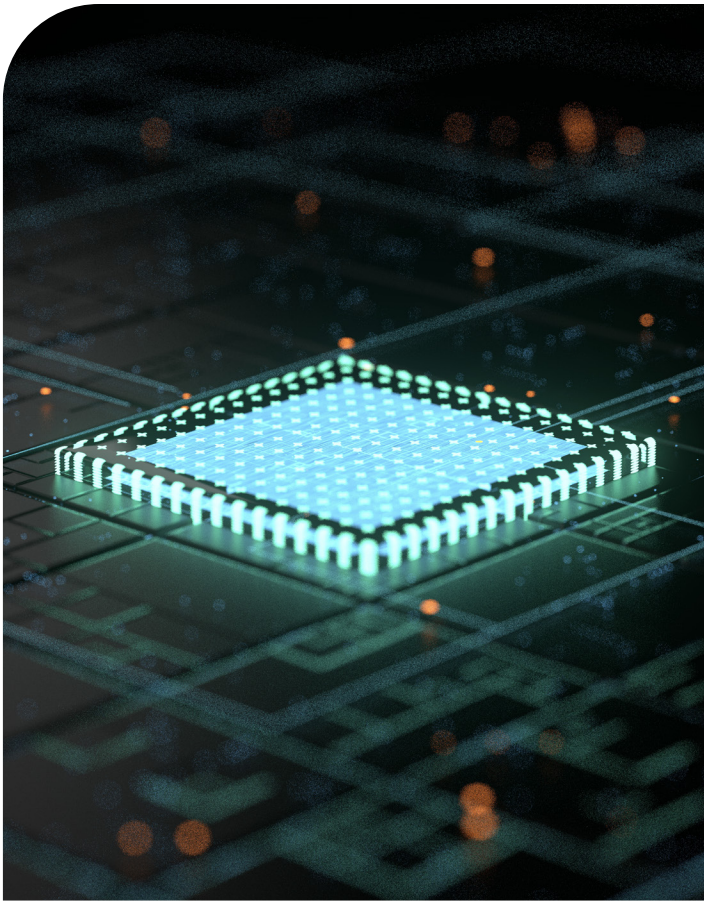
This same concept can be applied to other decisions within hospitals to improve operations and accelerate processes. Adds Egan, "Imagine in a hospital setting knowing that a nurse or the doctor is there to say, 'Yeah, I agree,' or 'I actually don't think that's right … we're going to do something else.' Because a human is in the decision loop, companies can use this strategy to address concerns about traceability and explainability as well as address fear and trust issues amongst consumers. In fact, we're already seeing this idea reflected in some of the new industry regulations."

Some companies are taking things a step further by hiring chief ethics officers who can, for instance, advise on how a proposed use of AI or ML aligns with their organization's principles and ethics. "This investment is about going beyond compliance," explains Egan. It can demonstrate a business's commitment to doing what's right – which can be consciously choosing not to employ technology in a way that would serve the business but could harm its customers or society at large.

3. Demands for personal data privacy and protection

Almost everything businesses use in the cloud is powered by data. The regulations around data are particularly tricky to navigate. "This is an incredibly complex ecosystem," notes Egan. "There could be multiple laws, even in a single jurisdiction such as the EU, that are governing data, especially if personal data is involved."

Some countries have little or no regulation on these issues, while others are already highly regulated or moving quickly in that direction. Governments also bring vastly different philosophies and priorities to data protection regulation. Europe is leading the charge with its general data protection (GDP) regulation, which assumes data privacy rights and controls are a fundamental human right and empowers individuals to control the data that organizations collect on them and how it can be used. In contrast, the U.S. views data privacy as a consumer protection issue. And China, which just came out with its Personal Information Protection Law, lays out a comprehensive set of rules for how business operators can collect, use, process, share and transfer personal information.2



Recommendations

Navigating vastly different data protection philosophies and emerging regulations will be difficult, notes Egan. "The challenge for companies creating cloud solutions is how to make them work around the world, rather than be jurisdiction specific." He advises looking beyond the debates and regulations to understand their intent. "We can say, 'Okay, here's what the law says,' but what are they really trying to protect? And how do we address that as we innovate with cloud and AI and machine learning solutions?" By anticipating where regulations will likely focus – and the philosophical underpinnings of those regulations, businesses can move ahead with cloud-based AI and ML and minimize adaptation when regulations are released.

4. Emerging issues around data, AI inventions and intellectual property

Beyond AI and ML technologies, organizations must grapple with regulations that impact intellectual property (IP). As Egan explains, "There's the input data that goes into the AI (the AI algorithm) and what the AI generates as output. And each has a potential IP issue associated with it."

For example, in recent U.S. cases, it was questioned whether or not an AI algorithm or tool can be listed on a patent as an "inventor." The answer was no, but elsewhere, like Australia, the answer is yes. That raises a lot of questions about who owns the patent – the organization or the AI tool? And if AI is only as good as the data that's going into it, can you say you own the data set that feeds the algorithm? These are all philosophical questions for many at present – but in time will likely become more common.

Recommendations

Taylor anticipates that because there are so many issues around data, a whole new technology area around synthetic data will emerge. "Businesses have two problems – getting access to data because of privacy and other regulations and getting enough of it to draw unbiased conclusions. With synthetic data, data is readily available and already safe to use, making it the ideal workaround for some of the issues we've discussed."

> Businesses have two problems – getting access to data because of privacy and other regulations and getting enough of it to draw unbiased conclusions. With synthetic data, data is readily available and already safe to use, making it the ideal workaround for some of the issues we've discussed.
>
> - Suzanne Taylor, Vice President, Innovation and Emerging Technologies, Unisys

> There's this idea of a human right to not be subject to automated decision-making. We're seeing privacy regulations emerge stating that there must be a human check to ensure that everything's okay.
>
> - Michael Egan, Partner, Cooley LLP

In the absence of clear regulations, commit to self-regulation

Without clear regulations for AI and ML, industries must self-regulate by anticipating and inventing around likely regulations – and be agile enough to adapt as things change. This is no less true for cloud infrastructure. There can be industry agreement on self-regulation that may be more effective and more informed than anything the regulators might come up with. For example, Unisys has published a statement to document our commitment to developing and leveraging emerging technologies, including AI and ML, in a responsible, transparent and ethical manner. Others have published whole treatises on this subject.

And as noted by Taylor, businesses can step up as well by creating ethical statements, principles that their engineers must agree to adhere to, and having the right testing in place for AI and ML algorithms. "This allows companies to monitor what is actually operational and watch for things that may be perceived as unlawful or outside ethical guidelines – intentional or unintentional. This must be built into the whole development process and made the responsibility of developers, in my opinion," she adds.

Egan also notes that a proposed regulation by the EU provides a model for self-regulation elsewhere: "The regulation would require that companies continuously analyze and assess AI and ML systems – especially for high-risk AI systems – to ensure they continue to operate in a transparent and trustworthy way."

This could mean establishing regular testing of models to detect drift, and even malicious interference, so issues are detected early and models are retrained and rescored before being redeployed.

According to Egan, when regulators see that an industry is effectively self-regulating and innovating and testing with their priorities in mind, it can take a lighter regulatory touch, which is very beneficial. Industry regulations are usually more controlled and done to facilitate the commercia success of what organizations are trying to achieve.

Be thoughtful about how you develop your technology while remaining true to core principles like data privacy by design. Build flexibility into your solutions and pricing models so you can be responsive to regulatory change.

Learn more

Despite the challenges, highly regulated businesses have reasons to be optimistic about how to harness AI and ML as part of their cloud-based digital transformation strategies. As you develop solutions or implement technologies, you can put the proper testing and check and balances against those priorities. Then you can be more fluid as regulations change.

Unisys is partnering with companies to help them navigate the uncertainties of cloud-based AI and ML adoption so they can keep moving forward to achieve the compelling business outcomes made possible by digital transformation. Our solutions help organizations adhere to the highest security and compliance standards and mitigate risk at each stage of the cloud-adoption lifecycle – even for organizations with the most demanding and complex cloud systems.

To learn more, visit us online or contact us today.

Michael Egan
partner, Cooley LLP

Michael Egan advises clients across various industries on matters relating to global privacy, data protection and data security, cyber security issues, as well as blockchain, artificial intelligence, and other information technology issues.

Suzanne Taylor, Ph. D.
vice president, innovation and emerging technologies, Unisys

Suzanne Taylor, Ph. D., is a technology business leader who balances technical, analytical and business competencies to transform products and solutions. She leads the global innovation practice at Unisys and applies emerging technologies to solve business problems.

unisys

unisys.com

02/23 23-0176