Ideas shaping privacy, published by OneTrust DataGuidance®

V6, ISSUE 3
May 2024

Data Protection Leader

THE EXISTENTIAL ROLE OF GLOBAL DATA FLOWS FOR AI

AI GOVERNANCE PRACTICES

Reflecting on best practices for creating effective AI governance structures

CALIFORNIA'S NEW FRONTIER

Exploring California's approach to regulating automated decision-making

BUILDING TRUST IN AI

Q&A on fostering trust and transparency in AI technologies

onetrust
DataGuidance

Contributors to this issue

Eduardo Ustaran
Partner, Hogan Lovells

Eduardo Ustaran is Global co-head of the Hogan Lovells Privacy and Cybersecurity practice and is widely recognized as one of the world's leading privacy and data protection lawyers and thought leaders. With over two decades of experience, Eduardo advises multinationals and governments around the world on the adoption of privacy and cybersecurity strategies and policies. Based in London, Eduardo leads a highly dedicated team advising on all aspects of data protection law - from strategic issues related to the latest technological developments such as AI and connected devices to the implementation of global privacy compliance programs and mechanisms to legitimize international data flows.

Philip James
Partner, Eversheds Sutherland

Philip James is a Partner and member of the Eversheds Sutherland's AI Task Force and Global Data, Privacy, and Cybersecurity Group. Philip counsels clients on commercial data strategy, privacy, cybersecurity, and responsible Gen/AI-driven innovation, together with rights in data and their use in emerging technology, data centers, infrastructure, and associated cloud services.

Monika Tomczak-Gorlikowska
Global Head of Privacy,
Prosus Group

Monika Tomczak-Gorlikowska is the Global Head of Privacy at the Prosus Group, one of the world's largest technology investors. Based in Amsterdam, she has over 25 years of legal experience, including roles at Shell International Limited in London and Miller, Canfield in Poland. Monika holds a Master of European Law degree (LLM cum laude) from the College of Europe in Brugge, Belgium. She has served as Co-Chair of the Forum on International Privacy Law and is a member of the IAPP European Advisory Board. Monika is fluent in six languages: English, French, Spanish, Italian, Polish, and Portuguese.

Shravan Subramanyam
Privacy and AI Governance
Manager, Prosus Group

Shravan Subramanyam is the privacy and AI governance manager at Prosus. Currently based in Amsterdam, he was previously a research assistant at the Tilburg Institute of Law and Technology (TILT). He holds a Master's in Law (Law and Technology) and a Master's in Science (Data Science) from Tilburg University, the Netherlands.

Alex Altman
Senior Associate, Arnold & Porter

Alex Altman's practice focuses on the rapidly changing area of global data protection, privacy, and cybersecurity law. With more than 10 years of experience, Alex has counseled clients from a wide array of industries - including media, technology, finance, retail, and life sciences - on developing privacy and cybersecurity compliance programs, conducting due diligence in the M&A context, negotiating data protection agreements, managing data breach responses, and responding to litigation and government investigations.

Arun Babu
Partner, Kochhar & Co

Arun Babu is a Partner in the Bangalore office of Kochhar & Co. He specialises in Indian data privacy, cybersecurity, and telecom laws.

Paul Connelly

Paul Connelly built the first cybersecurity programs at two of the world's highest-risk organizations - the White House and HCA Healthcare, and led those programs for a combined 28 years in CISO roles. He also spent six years building a cybersecurity consulting practice as a partner at PricewaterhouseCoopers. Throughout, Paul has been a developer of people, with 36 team members selected for CISO positions. Paul retired from HCA Healthcare in 2023 and is currently an independent director on the board of Dismas, a Technical Advisor to the boards of the U.S. Organ Procurement & Transplantation Network and UNOS, on the faculty of the Institute of Applied Network Security, developing cybersecurity programs at Belmont University, and a Senior Advisor to Brighton Park Capital.

Bart W. Huffman
Partner, Holland & Knight LLP

Bart W. Huffman is a data strategy, security and privacy attorney in Holland & Knight's Houston office. With a systems engineering and intellectual property (IP) background, Bart has decades of experience in privacy and cybersecurity/incident response matters and sophisticated technology transactions. He serves as an adjunct professor at the University of Texas School of Law, where he teaches U.S. and EU privacy law. Bart is a Certified Information Privacy Professional - U.S. and Europe (CIPP/US and CIPP/E), and a cybersecurity fellow at the Robert Strauss Center for International Security and Law.

Data Protection Leader is published bi-monthly by OneTrust Technology Limited, Dixon House, 1 Lloyd's Avenue, London EC3N 3DS

Website www.dataguidance.com

Email DPL@onetrust.com

ISSN 2398-9955

Table of contents

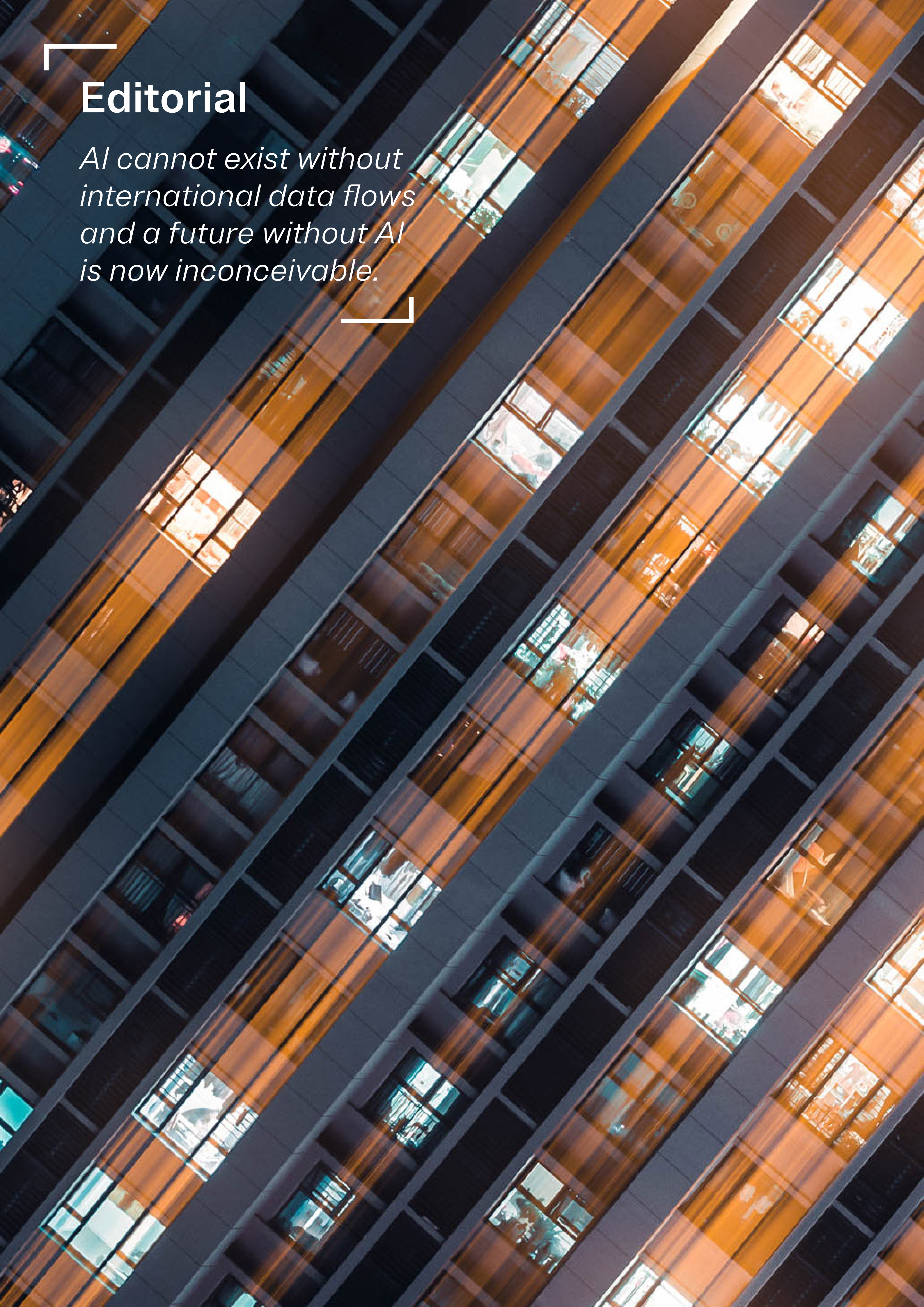
Editor: Eduardo Ustaran | eduardo.ustaran@hoganlovells.com

Managing Editor: Alexis Kateifides | akateifides@onetrust.com

Editorial Lead: Victoria Prescott | vprescott@onetrust.com

Editorial

AI cannot exist without international data flows and a future without AI is now inconceivable.



Editorial: The existential role of global data flows for AI

Eduardo Ustaran
Partner
eduardo.ustaran@
hoganlovells.com
Hogan Lovells, London

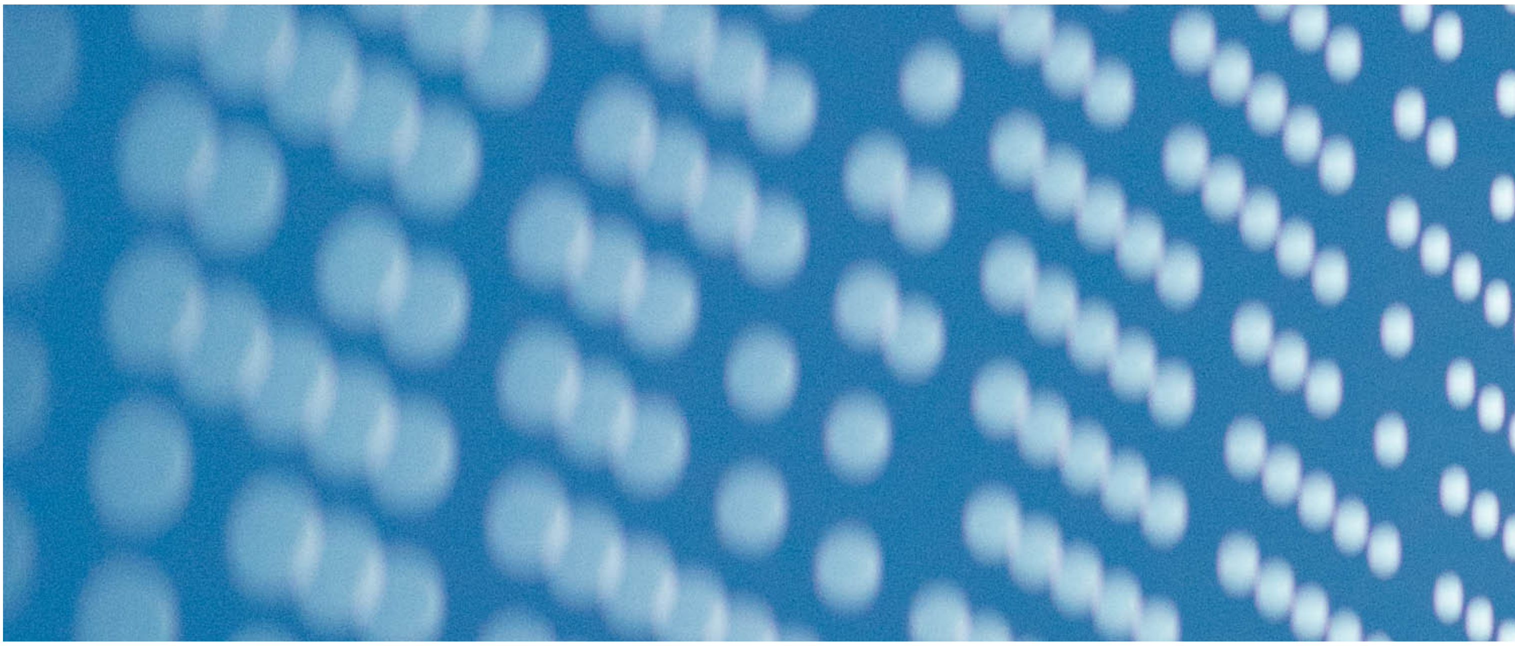
AI development is a computing power challenge. It is also a human talent challenge. But above all, AI development is a data challenge. The availability of computing power, talent, and data is testing like nothing else the ability of AI to meet its sky-high expectations. Before the internet existed, the type of AI applications that surround our daily lives today - from predictive text to voice assistants and from streaming content recommendations to live traffic routes - were simply science fiction. The global network of computers that make up the internet, together with the brains behind them, now provides the ground for AI to exist, but it is the global data used to train, test, and fine-tune AI models that makes the magic happen. Like social media and cloud computing before it, AI development and use is the next technological iteration of a universal need for data to flow around the world. Therefore, it is crucial to address the legal restrictions on international data transfers in a rational, realistic, and responsible way.

Data localization is often presented as the solution to the risks of letting personal data flow beyond jurisdictional borders. Geographically ring-fencing data to make it inaccessible from other parts of the world is seen as a viable way of preserving a valuable asset for the benefit of the local community. The trouble with this line of thinking is that it misses the fact that isolating data is neither a mechanism of protection nor a beneficial practice. This is even more evident in the context of data uses for AI development and deployment. AI cannot be reliably built on the back of isolated, incomplete datasets. One of the greatest concerns about AI is its potential for biased, discriminatory, and unfair outcomes. Insufficient or skewed data has led to undesirable effects - such as a lack of gender or racial diversity in employment practices, demographically biased policing, or inaccurate medical diagnoses in underrepresented populations - that show the limitations of AI technology. Truly beneficial AI that reflects the diversity of the world can only be developed if the data that feeds that development is global and unconstrained by arbitrary limitations.

The issue that has contributed to a zero-risk regulatory approach to international data transfers in recent years is the prospect of unwarranted government access to data. Some European regulators' positions on this point have been particularly strict and dogmatic. The mere hypothetical risk of personal data being exposed to foreign government agencies has triggered an uncompromising stance that leaves no room for a more pragmatic risk-based approach. In the context of globally sourced data to train AI models, this stance requires some rethinking. What is the nature of this data and how widely available is it already? What is the likelihood of such data being massively accessed by governments and for what purpose? The AI world is already subject to an unhelpful level of doomsday hype that does not need further hyperbole about imaginary abuses of data. What it needs is a realistic approach to risk that is able to distinguish between innocuous situations and real threats to privacy and human rights.

This is where responsibility fits in. As with all aspects of personal data processing, AI development and use should be accompanied by a degree of accountability that is also applicable to international data flows. What are the real implications of collecting data from one part of the world and using it to train AI models in another? What impact could the output of AI use in one place have on the rights of individuals in another location? In our digitally interconnected world, it is only right and proper that we consider these issues with care and pragmatism. The role of international data transfer impact assessments is also relevant to AI-related data flows and should be regarded as a key component of responsible AI development.

AI cannot exist without international data flows and a future without AI is now inconceivable. So it is essential to accept this reality and focus on how to ensure that personal data is universally protected. Having an accurate understanding of what personal data is being used for what purposes is a fundamental starting point that requires privacy professionals and engineers to work together. Being able to identify and articulate any genuine - not theoretical - privacy and cybersecurity risks will also be critical, and adopting an agile and creative approach to minimizing those risks and putting people in control of their data globally will be the best way forward.



The EU AI Act: Part two - Cybersecurity, data provenance, and watermarking

Philip James
Partner, Global
Privacy & Cyber Security Group
philipjames@eversheds-sutherland.com
Eversheds Sutherland

Anna Allen
Senior Associate, Global
Privacy & Cyber Security Group
annaallen@eversheds-sutherland.com
Eversheds Sutherland

Robbert Santifort
Principal Associate
robbertsantifort@
evershedssutherland.
com
Eversheds Sutherland, Netherlands

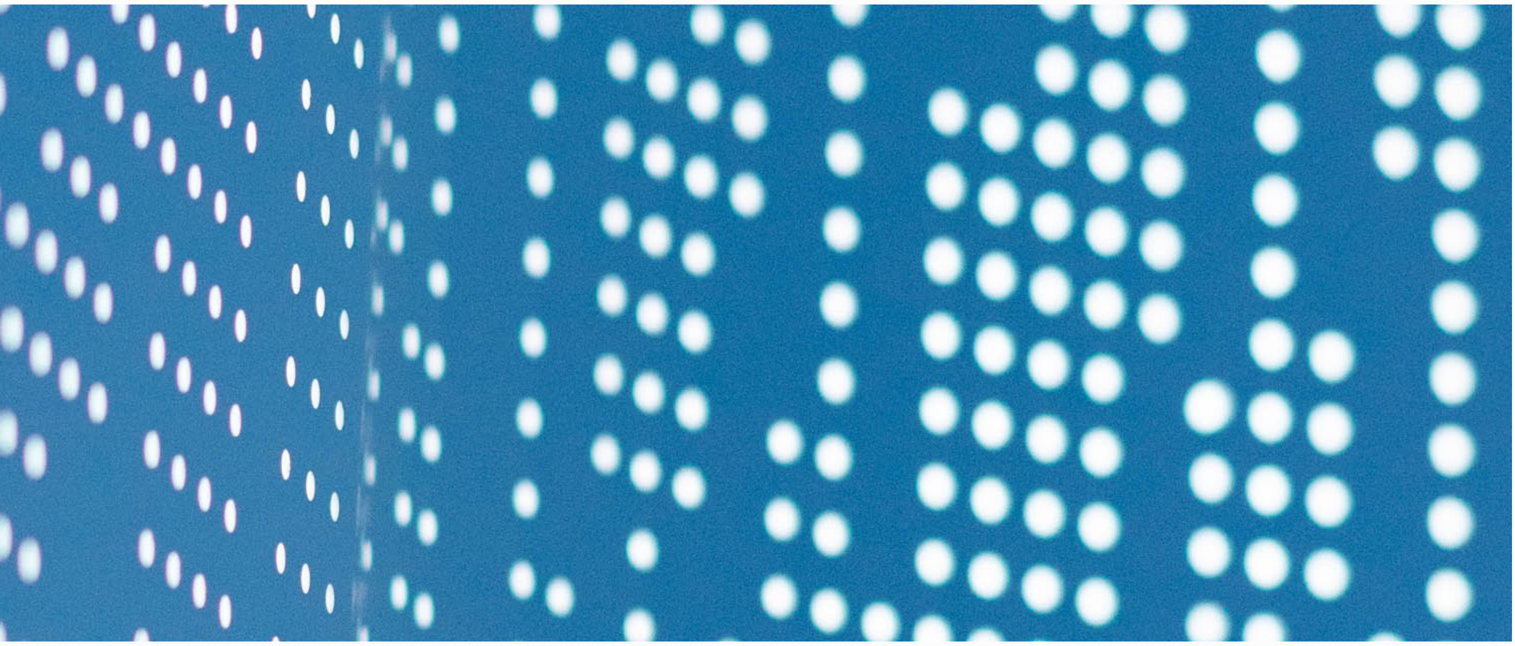
This is the second in a series of two articles by Philip James, Anna Allen, and Robbert Santifort of Eversheds Sutherland, which addresses three themes in the EU AI Act (the AI Act) and the use of AI systems. Part 1 focused on its data protection provisions and a comparable analysis to the existing EU General Data Protection Regulation (GDPR). Part 2 focuses on cybersecurity, data provenance, watermarking, and deepfakes.

Bolstering cybersecurity

The AI Act reinforces the importance of having robust cybersecurity measures for high-risk AI systems. The need for effective cybersecurity in any implementation of new, emerging technology cannot be understated - in that, new methods create new vulnerabilities, as well as compliance process gaps. Providers of high-risk AI systems will have to fulfil the cybersecurity requirements of the AI Act set out at **Article 15.**

Consistent performance

A key obligation for organizations is that high-risk AI systems should perform consistently throughout the AI systems lifecycle, meeting an appropriate level of accuracy, robustness, and cybersecurity, in the light of their intended purpose (Article 15(1), Recital 74). Cybersecurity measures are to be considered and tested at the start of the development phase, following



which it will be a continuous iterative process throughout the AI systems lifecycle. Security by Design, if you like, mirroring the 'Privacy by Design and by Default' under the GDPR.

A similar concept can be seen in the national security agencies' *Guidelines for Secure AI System Development*[1], which references a 'secure by design' approach and the European Union Agency for Cybersecurity's (ENISA) Multilayer Framework for Good Cybersecurity Practices for AI, which stresses the need for dynamic threat assessment and risk management covering the entire lifecycle of AI systems[2]. This approach emphasizes the need for significant resources at all stages of a system's lifecycle. In doing so, security should be a priority, not a consideration.

Under Article 9, it is necessary to implement and regularly review and update risk management systems in relation to high-risk AI systems. This involves identifying and analyzing the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose, adopting appropriate risk management measures to address those risks, and testing the AI system throughout the development process.

In order to comply with this requirement from a cybersecurity perspective, it will be necessary to undertake a cybersecurity risk assessment of the AI system and its components (including the limitations and vulnerabilities of their interactions with other components of the system and threats such as loss of transparency, interoperability, managing bias, and accountability)[3].

These requirements should also take into account AI systems that will continuously learn after being put into service. The AI Act references '*feedback loops*' (i.e., the AI system should continue to send feedback once put into the market) in Article 15, which should be addressed with appropriate mitigation measures. The data flows and network architecture of such systems will be essential for effective assessments (and will inform steps to mitigate security risks).

The AI Act does not provide definitions for 'accuracy' or 'robustness.' However, we see these terms are often referenced in AI-related guidance, as can be seen in National Institute of Standards and Technology (NIST) document on Artificial Intelligence Risk Management Framework[4] which notes that 'accuracy and robustness contribute to the validity and trustworthiness of AI systems' and also provides definitions of each, where accuracy is defined as 'closeness of results of observations, computations, or estimates to the true values or the values accepted as being true' and robustness is defined as 'the ability of a system to maintain its level of performance under a variety of circumstances.'

Resilience

Under Article 15(5), high-risk AI systems must be resilient against unauthorized third-party attempts to exploit their vulnerabilities to alter their use, outputs, or performance. The focus of this provision is on protecting AI systems from changes by malicious actors including 'data poisoning' (manipulating the training data sets), '*model poisoning*' (manipulating pre-trained components used in training), 'model evasion' (causing the AI model to make a mistake), confidentiality attacks, and model flaws.

The technical solutions to be adopted to comply with this requirement must be appropriate to the relevant circumstances and risks and must include measures enabling the prevention, detection, responding to, resolving, and controlling of cybersecurity attacks.

As an additional protective measure, Article 14 of the AI Act includes the need for appropriate human oversight in order to minimize risks to health, safety, or rights, with certain high-risk AI systems being separately verified by two people with the necessary skills, except in specified cases i.e., the purpose of law enforcement.

The Cyber Resilience Act (CRA) includes specific provisions related to high-risk AI systems, as outlined in Article 8. These provisions exclusively apply to AI systems classified as high-risk according to the AI Act. Furthermore, connected devices falling under the purview of the CRA and meeting the Security by Design essential requirements will be deemed compliant with the AI Act. They will be considered to possess the necessary level of protection as indicated by their declaration of conformity. For most of these products, the conformity assessment procedure specified in the AI Act will be applicable, with regulatory bodies overseeing compliance and notification processes[5].

Documentation

As well as undertaking continuous risk management processes, following the implementation of the AI Act, organizations must document their compliance by drawing up and keeping up to date a technical documentation before a high-risk AI system is placed on the market or put into service, which must include cybersecurity measures put in place (Article 11). They must also ensure that the AI system has the technical capability to record, over the lifetime of the AI system, logs of events relevant for identifying situations which may result in the high-risk AI system presenting a risk to health and safety or to fundamental rights of natural persons (Article 12). The idea being that there will be additional levels of traceability of the functioning of a high-risk AI system.

Information about the cybersecurity measures put in place must also be included in the instructions for use of the high-risk AI system that must be provided to deployers (Article 13).

Reporting serious incidents

The AI Act introduces requirements in respect of reporting serious incidents. A serious incident means an incident or malfunctioning of an AI system directly or indirectly leading to death or serious damage to health, serious and irreversible disruption of the management and operation of critical infrastructure, infringements of obligations intended to protect fundamental rights or serious damage to property or the environment (Article 3(49)).

Under Article 26(5), a deployer of a high-risk AI system must notify a serious incident immediately after discovery to the provider, and then the importer or distributor and the relevant market surveillance authorities. Article 60 obliges providers of high-risk AI systems placed on the EU market or tested in real-world conditions to report any serious incident to the market surveillance authorities of the Member State where that incident occurred. The notification must be made immediately and not later than within 15 days after becoming aware of the serious incident (Articles 60(7) and 73). Notification timescales under the GDPR for personal data breaches are significantly shorter (whilst other regulators may also need to be notified).

In addition, where the development or use of a general-purpose AI model with systemic risk causes a serious incident, the general-purpose AI model provider should, without undue delay, keep track of the incident and report any relevant information and possible corrective measures to the AI Office and national competent authorities (Article 55(1)(c)). 'Systemic risk' refers to a risk specific to the high-impact capabilities of Generative AI models having a significant impact on the EU market due to their reach or negative effects (Article 3(65)).

]

Data provenance (and watermarking)

Synthetic media (or deepfakes) and synthetic text created by AI are rapidly becoming more pervasive. With continued developments to the technology came its widespread use and the improved accuracy and sophistication of artificially generated content. As a result, the general public is encountering increasingly more synthetic, often deceptively convincing, content which is difficult for people and detection technology to distinguish from content created by humans. This has raised widespread concerns about the risks of misinformation and manipulation at scale, fraud, impersonation, and consumer deception significantly adversely impacting the integrity and trust in the information ecosystem (as acknowledged in Recital 133).

The risks

Currently, the technology is most commonly used to generate non-consensual deepfake pornographic content with traumatic effects on the victims and the potential to be used for harassment, blackmail, and extortion. Reportedly, such deepfakes usually feature celebrities, with Taylor Swift as one recent victim. There are also numerous examples of deepfakes and generative AI being used to disseminate misinformation, such as the deepfake calls impersonating President Joe Biden discouraging people from voting in the primary presidential elections earlier this year. The proliferation of disinformation in the media is a serious threat to democracy and public discourse, and erodes public trust in media, public institutions, and wider society (evidenced even in the furor surrounding the recently photoshopped images of The Duchess of Cambridge). There are also reports of deepfake technology being increasingly used by fraudsters for identity theft (e.g., to trick identity verification systems in banking) and posing threats to cybersecurity and law enforcement[6]. In addition, a recent study shows that deepfakes and fake information can distort our memories and beliefs which may affect our shared understanding of history and culture. Non-consensual deepfakes also impact the right to privacy of victims, misuse of their personal data and image, and performers' rights. In response, there have been growing calls for banning the technology and criminalizing its use.

The benefits and potential

However, technology is also being utilized for a variety of legitimate reasons, especially in creative arts such as films, TV programs, and gaming. For example, deepfakes are being used to recast actors posthumously (such as Carrie Fisher in the Rise of Skywalker) or introduce their younger versions in films (such as Harrison Ford in Indiana Jones and the Dial of Destiny), translate audio to other languages, or put a lead character's face on a body of a stunt actor. Deepfakes can also be used for immersive gaming (e.g., inserting virtual deepfakes of ourselves or actors into games) and other arts (e.g., recreating virtual versions of deceased artists, such as the deepfake of Salvador Dali interacting with visitors of the Dali Museum in Florida). Other examples of beneficial uses of the technology include creating or recreating unique deepfake voices for people who communicate through synthetic speech; protecting the identity of LGBT+ activists speaking out about persecution; or enhancing global social campaigns (e.g., David Beckham using deepfake voice to 'speak' in nine languages in his campaign against malaria). There is also potential for the beneficial use the deepfake technology in other sectors, such as e-commerce, education, or advertising.

The AI Act's response

Therefore, a total ban or criminalization of the use of the technology is not the right response. Instead, we need appropriate safeguards allowing its responsible development and beneficial use with consent, and regulation protecting intellectual rights and prohibiting and tackling harmful use (such as nonconsensual sexually explicit deepfakes, the use of deepfakes for fraudulent purposes, disinformation, and other uses of the technology with malicious intent). The AI Act attempts to strike such balance between protecting the public from harmful misuse of the technology while fostering technological innovation and its responsible use. In the UK, complementary legislation in the form of the Online Safety Act is also intended to address such issues and how platforms manage online risks of this kind.

Ban on AI systems deploying subliminal techniques

The AI Act introduces a number of safeguards designed to mitigate the risks. These include the prohibition on the placing on the market, putting into service, or use of AI systems that deploy subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of, materially distorting the behavior of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing a person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm (Article 5(1)(a)).

Recent research has identified that experience of metaverse and virtual worlds can be infiltrated by threat actors to create a fake digital VR environment (similar to the original) undetectable by the user - whose biometrics are then collected unwittingly - and who may be deceived into disclosing confidential, personal information, as well as being influenced to making decisions which they may not have done otherwise. This is a particularly potent, virtual cocktail.

Watermarking synthetic content

In addition, the transparency obligations in Article 50 require organizations to inform natural persons that they are exposed to interactions with, operation of, or outputs of certain AI systems (whether or not classed as high-risk). Article 50(4), in particular, covers the watermarking of AI-generated or manipulated content. It obliges deployers of AI systems generating or manipulating: (i) image, audio, or video content constituting a deepfake; and (ii) text which is published with the purpose of informing the public of matters of public interest, to disclose that the content has been artificially generated or manipulated.

A deepfake is defined in Article 3(60) as AI-generated or manipulated image, audio, or video content that resembles existing persons, objects, places, or other entities or events and would falsely appear to a person to be authentic or truthful.

The watermarking obligations in Article 50(4) do not apply to: (i) the authorized use of deepfakes and synthetic text to detect, investigate, or prosecute criminal offenses (not dissimilar to comparable derogations under the GDPR which are designed to allow fraud prevention or the detection of crime); or (ii) to AI-generated content that has been reviewed or edited by humans and where a legal or natural person is responsible for its publication. The latter will be of particular relevance to news agencies, publishers, broadcasters, and PR/comms agencies. So even though you may have reviewed and edited AI-generated content (and therefore a deployer no longer remains responsible for watermarking such text content), reputation and intellectual property infringement (and advertising clearance) must still be considered before release.

The labeling information must be provided to the concerned natural persons in a clear and distinguishable manner and no later than at the time of first exposure (Article 50(5)). Where deepfake content forms part of an evidently artistic, creative, satirical, fictional analogous work, or program, this information can be provided in a manner that does not hamper the display or enjoyment of the work (Article 50(4)).

Underpinning these watermarking requirements will be a requirement for Gen AI model developers to publish a publicly available summary of what training data went into training the AI model. This may be hard, if the original data ingested and records were not meticulously recorded; effective data governance in and around data ingestion and recording sources will therefore become an increasing focal area - as will techniques to hardwire in copyright notices and author paternity right credits for authors, whether in text or audiovisual content.

As part of this, certain technology companies are starting to embrace C2PA, a technical standard (otherwise known as a form of nutrition label) to non-text content - this is an open-source protocol that draws on cryptography to hardwire in metadata around the origin and provenance of a piece of content. In October last year, for example, Leica introduced a new camera, the M11-P, with integrated 'Content Credentials', for this very reason. See here for further details.

The labelling requirements in other EU legislation

The AI Act is not the first piece of EU legislation requiring the labeling of AI-generated/manipulated content. As mentioned in Recital 136, the transparency obligations in the AI Act are relevant to the facilitation of the effective implementation of the Digital Services Act which obliges providers of very large online platforms and search engines to identify and mitigate systemic risks stemming from the design or functioning of their service including that deepfakes are distinguishable through prominent markings when presented on their online interfaces[7].

Summary

The novelty and seductive charm of efficiencies gained by AI (and Gen AI) should not cause cybersecurity and reputational risk to be underestimated. In procuring, implementing, and updating existing applications, routine and due processes should be amended and enhanced to address new risks and vulnerabilities presented by emerging technology (and the inevitable change in the course of data flows - as new tributaries and back currents form). Documenting suitable security risk assessments and, in some cases, leveraging managed service providers (who may help assume a certain level of responsibility for security risk management, especially where smaller businesses are concerned) will be essential. And above all, as part of any risk assessment, the reputational risk should be considered and marketing and communications teams' views should be sought, at the same time as, not solely in addition to, technical, legal, and operations teams. Trust remains the keystone in deploying any emerging technology. Those teams who manage to innovate and maintain (or even enhance) trust will gain significant competitive advantage.

[1] The UK National Cyber Security Centre (NCSC), the US Cybersecurity and infrastructure Security Agency (CISA) in cooperation with 21 other agencies and ministries from across the world guidelines for secure AI system development, 23 November 2023 https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf

[2] European Union Agency for Cybersecurity (ENISA), Multilayer Framework for Good Cybersecurity Practices for AI, June 2023: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence

[3] European Union Agency for Cybersecurity (ENISA), Multilayer Framework for Good Cybersecurity Practices for AI, June 2023: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence; Junklewitz, H., Hamon, R., André, A., Evas, T., Soler

[4] Garrido, J., Sanchez Martin, J., Cybersecurity of Artificial Intelligence in the AI Act, Guiding principles to address the cybersecurity requirement for high-risk AI systems; 11 September 2023, : https://publications.jrc.ec.europa.eu/repository/handle/JRC134461

[5] https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products#:~:text=The%20legislation%20was%20approved%20with,order%20to%20come%20into%20law.&text=New%20technologies%20come%20with%20new,increased%20dramatically%20in%20recent%20years.

[6] Europol, Facing reality? Law enforcement and the challenge of deepfakes, as updated in January 2024: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf

[7] The term 'deepfakes' is not used in the Digital Services Act (Regulation (EU) 2022/2065), but the description of the relevant content used in Article 35(5)(k) is in line with the definition of a deepfake in the AI Act: "an item of information, whether it constitutes a generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful."

Meet a CISO: Paul Connelly

Paul Connelly
PaulConnellyCISO.com

Tell us about yourself and your role.

How would you describe your role?

I've been in Information Security since starting at the U.S. National Security Agency out of college in 1984. Twenty-eight of those forty years have been working in CISO roles at The White House and HCA Healthcare, the largest healthcare provider in the U.S. I retired in 2023 after 20 years as HCA's CISO/CSO and now focus on board service, consulting, and developing future CISOs.

Do you work as part of/ lead a broader team?

I had a 300 person team at HCA, which also included Privacy, Data Governance, and Physical Security.

What does a "typical" day look like?

As a CSO, I was leaving for work at 5:00 AM and getting home at 6:30 PM, and then working more after dinner…
I now have consulting calls through the day, work on thought leadership, engage in board activities, and mentor 7-8 current or aspiring CISOs.

How has the role of a CISO changed since you first took the role? How do you see it changing over the next five years?

The change has been nothing short of incredible. When I started there was no Internet, no mobile devices, and we worried most about the Soviet Union. The CISO role was a manager buried in IT. Today the CISO has become a key part of business strategy discussions, in front of the board, and at the senior leadership table. Over the next five years I expect to see the CISO role at many organizations to morph into a Chief Risk or Trust Officer role and start commonly serving on boards.

What drew you to working in cybersecurity?

The challenge of being part of something new and important, that served an important purpose - protecting people - got me started.

The dynamic change and growth in importance of the role got me to stay. I was the first CISO at two high risk organizations (The White House and HCA), where I had a chance to build the program from the ground up, which was an incredible opportunity. There is never a dull day, and no two days are alike for a CISO.

The field was especially rewarding in healthcare - because we knew we were protecting patients in hospital beds.

What are the key compliance areas that are top of mind for you right now for your program?

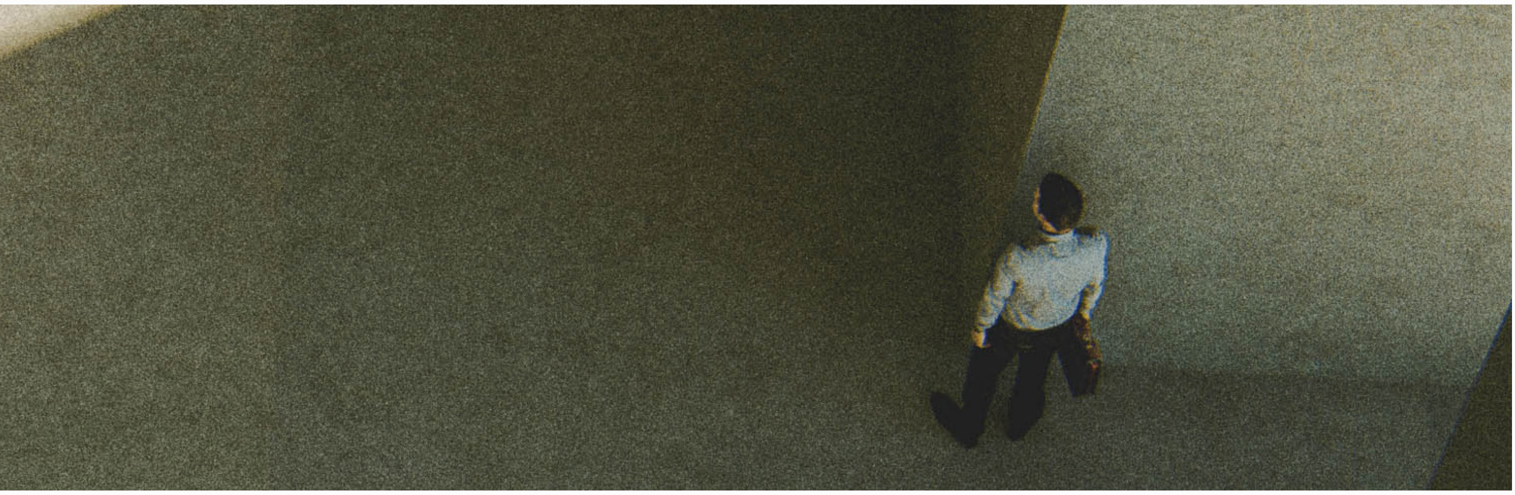
The changes in guidelines from the U.S. Securities & Exchange Commission are driving needed changes and we are still figuring them out.

What are the key elements of your cybersecurity program? Is it based on particular laws / standards / frameworks? How has it evolved over time?

The basic cycle of Identify, Protect, Detect, Respond, Recover, and Govern spelled out in the NIST Cybersecurity Framework have been the common approach from the beginning, but what goes into each of those components changes almost daily with new risks and tools. One constant in my programs has been a focus on people - communication, education, and developing a security-aware culture. The biggest changes I've seen in recent years have been the integration with business strategy, being elevated to the senior leadership team, and focus on Third Party risks.

Which other business functions do you regularly interact with, and why?

IT, Internal Audit, the CFO, and Legal have been our key partners from the start, but now we must work much more closely with business leaders and integrate with their strategies, operations, and partnerships.



What are your thoughts on the rapid pace of change within cybersecurity? Are there any recent developments that have been of either personal or business interest?

The rate of change is incredible, but is necessary to match the speed of threat and technology changes. The growing focus on Data Governance, as well as Third Party Risk, have become mandatory. They should be shared responsibilities with business leaders and provide CISOs opportunities to further integrate with business operations.

What advice would you give to others looking to maintain and evolve their cybersecurity programs?

1. Become business focused. Cybersecurity will always be tied to technology, but successful cybersecurity programs today and tomorrow require deep understanding of business strategy and initiatives, and partnership with senior leaders.
2. Push for the right organizational model. The CISO should be at the senior leadership table, and in my opinion, a peer to the CIO/ CTO, not reporting to them. The role and team must be positioned with visibility into business initiatives, immediate access to senior leadership, and the ability to be completely transparent in their reporting of risks.

What do you think the biggest challenge facing the industry at the moment is? Will this change over the next 5 years?

Keeping pace. Threats, technology, and business models are changing at a rapid pace and cybersecurity leaders must adjust to stay up. That is why the right organizational model and business focus is necessary. Gen AI is the current challenge, but next will be Quantum computing, and something else will follow. Cybersecurity leaders must have the drive and grit to continually push forward and evolve. There is no standing still.

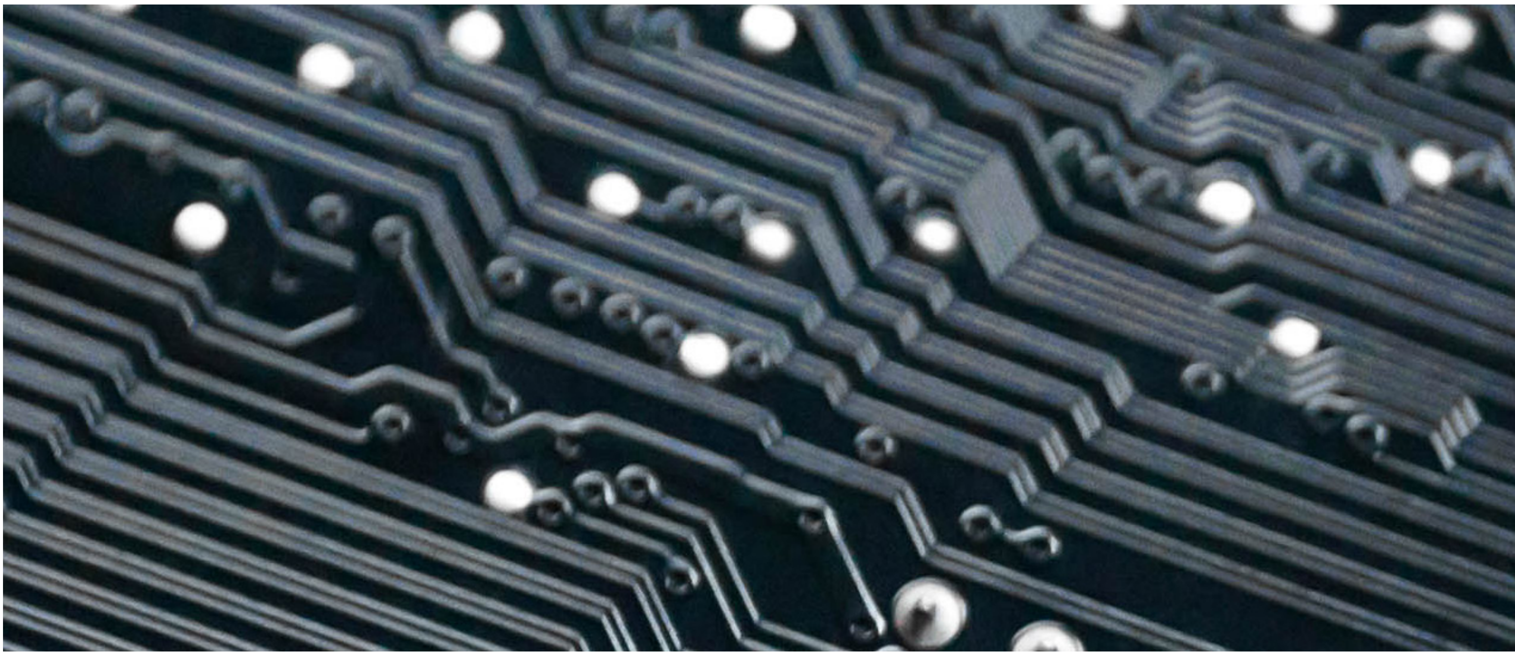
In your last role, you were also responsible for Privacy, Data Governance, and Physical Security - do you think more companies should bring those programs together?

My experience definitely makes me a proponent for cybersecurity, privacy, and data governance to be in the same organization. They work hand-in-glove and have a lot of synergy and efficiency together. I believe Data Governance needs joint ownership with business leaders, but the Cyber/Privacy team can act as the sponsor/facilitator.

Physical Security is a different animal, and while it made a lot of sense at a healthcare provider, that one depends more on the situation. There are definitely synergies, efficiencies, and areas of integration with cyber; and cyber can help physical security evolve to be more technology aided. I believe the fusion between cyber and physical will grow over time.

You now serve on boards - do you see it becoming a trend for boards to have directors with CISO experience?

It must. Technology risk and opportunity is a major factor in most business strategies, yet most boards don't have a single director with the background and expertise of a CISO or a CIO. How does a board meet its fiduciary responsibility to oversee management in a critical area where they have no real expertise? Answer: Not very well. If you look at the boards of the US companies that have had the largest breaches over the past two years, you will find none included a CISO. A savvy CISO brings the experience of being engaged in business strategy and operations, understanding of technology, leadership and people development, building partnerships, and seeing through a risk lens. That would add a valuable and diverse new element to most boards. This is what my experience with the three boards I support (two as technical advisor, one as Independent Director) has been - technology and cyber issues are among the top topics at every meeting, and I raise questions and discussions that would not have come up if I were not there. Part of the issue is that CISOs have not been board ready. That is changing rapidly with the evolution of the CISO role. Boards need to evolve, too. I believe that if they don't change soon on their own, regulators and the courts will force them.



Practical reflections on best practices in building AI governance structures

Monika Tomczak-Gorlikowska
Global Head of Privacy
Monika.Tomczak@prosus.com
Prosus Group

Shravan Subramanyam
Privacy and AI
Governance Manager
shravan.subramanyam@
prosus.com
Prosus Group

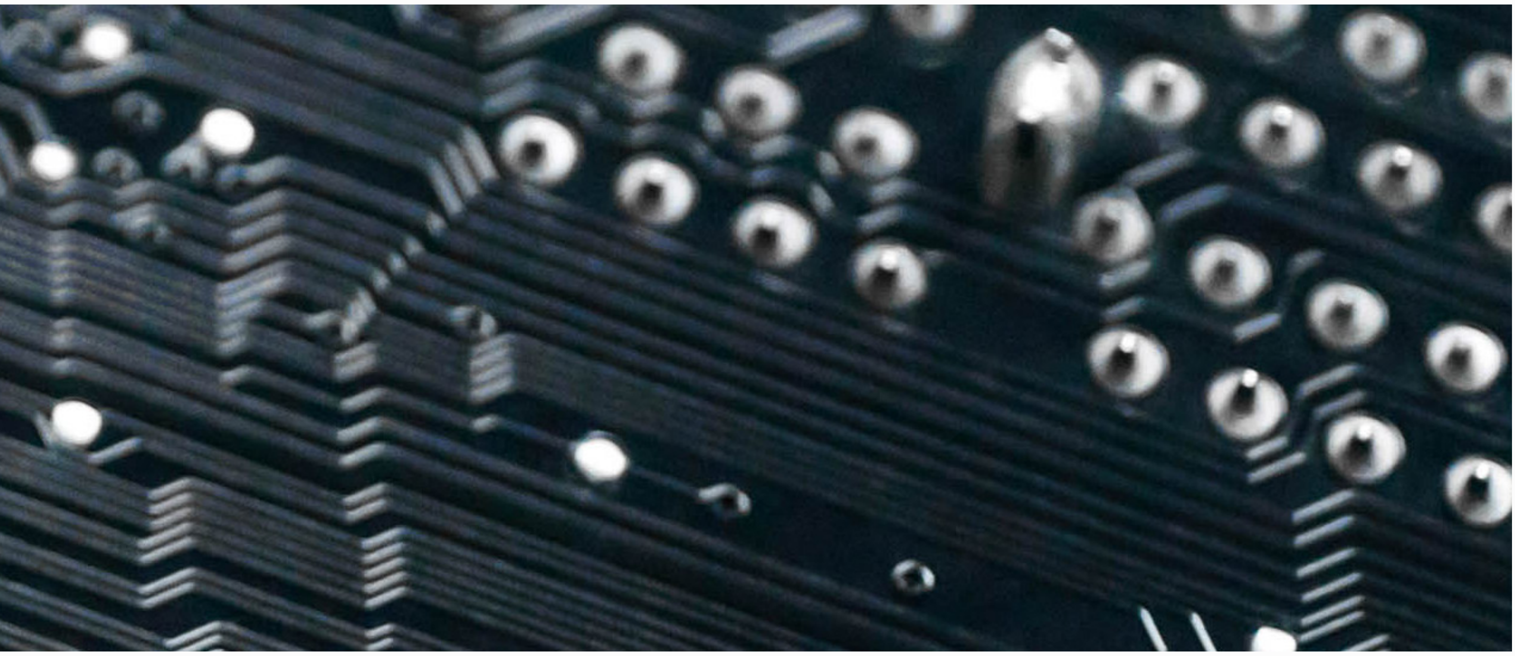
Introduction

With the rapid proliferation of artificial intelligence (AI)-driven products and services and the consequential development of AI regulation, there has never been a more pressing need for organizations worldwide to create or expand robust AI governance programs. Despite a fast-growing body of frameworks, guidance, and documents discussing AI governance, challenges still remain as the majority of such frameworks seem to be oriented towards larger organizations and focus on outlining high-level principles.

Keeping this in mind, this article seeks to outline emerging best practices for organizations of varying sizes and maturity in risk management, taking into consideration elements such as limited resources and more limited exposure to AI systems.

First, it is important to note that there are already numerous definitions of the term 'AI governance.' While there is a significant amount of variance in these definitions, it is important to note that ultimately, the target of an AI governance program is to accompany the entire lifecycle of an AI product/service. To successfully address the risks resulting from the deployment of AI and harness its benefits, organizations cannot limit themselves to adopting high-level compliance policies and applying one-off risk assessment methodologies.

In this article, we have selected a non-exhaustive list of domains in the process of building an AI governance framework and discuss specific challenges and considerations for each of these domains. However, depending on the size, structure, and culture of each organization, the choice of the domains and the prioritization of efforts should be individualized. It may look very different for a mid-size tech company involved in deploying education technology with children and a larger fintech company that is subject to financial supervision and operates mainly in a



business-to-business (B2B) context.

Our selected AI governance domains can be traced back to the specific elements of existing frameworks and guidance pieces as well as emerging regulatory requirements, like the EU's Artificial Intelligence Act (EU AI Act), but we have deliberately wanted to remain framework-neutral.

Executive buy-in, accountability, and corporate governance

Many organizations are currently on the journey of establishing their internal AI governance structures and are in the process of determining a suitable model that allows them to leverage existing processes and frameworks. The following practical aspects can be identified in this domain:

- Executive sponsorship and tone-from-the-top - Organizations should determine which role within the C-suite or Board members is best suited to become the executive sponsor for advancing AI governance and potentially be involved in the monitoring and oversight of those efforts. The designation of such executive or executives is a critical element for the success of efforts in various areas, irrespective of the size and AI maturity of the company involved. Although not every company requires the designation of a specific AI oversight officer at a Board level, executive buy-in and clear accountability remain critical.
- Establishment of a multidisciplinary, high-level AI and ethics body or board - With the increased recognition that AI requires cross-functional collaboration and that AI governance cannot be achieved by one existing function on its own, most organizations could benefit from establishing a multidisciplinary board, body, working group, or equivalent. Such a multidisciplinary group would be better placed to leverage the executive buy-in and drive the high-level oversight of ethical deployment of AI, assessing the impact of regulatory developments and creating a forum for setting the strategic direction of more specific efforts. While there is no fixed structure regarding the composition of this group, ensuring the participation of the AI, risk, strategy, privacy, legal, and sustainability functions are beneficial to ensure effective communication and collaboration.
- Adoption or expansion of the organization's AI ethical principles - Again, a growing number of companies have decided to adopt and sometimes make publicly available their guiding principles for responsible and ethical deployment of AI. This trend aligns with the growing number of international initiatives aimed at creating a globally accepted set of standards for responsible AI development, like the OECD AI Principles. Although the guiding principles should be benchmarked against the external frameworks and industry efforts, each organization should determine which aspects of responsible and ethical AI deployment are the most pertinent for its activities.
- Corporate governance - In view of the expanding nature of the fiduciary duties of the Board and C-suite executives, AI governance has become a boardroom topic. Most organizations regularly keep their Boards up to date in terms of the risks related to the deployment of AI, the progress in building AI governance, and the fast-paced digital regulatory requirements around the world. These updates can be added to existing governance structures such as specific reports/risk committees, but can also be provided on an ad hoc basis to keep the Board abreast of the developments and regulatory risks.

Stakeholder coordination and management

To complement the establishment and mandate of the AI and ethics board or working group, AI governance requires continuous involvement of a diverse group of stakeholders and working collaboration on a day-to-day basis. From our experience, the following groups of stakeholders are involved in various aspects of the AI operational side of AI governance:

- AI developers (machine learning engineers);
- legal and policy teams;
- privacy teams;
- intellectual property teams;
- cybersecurity and IT management;
- communications; and
- business representatives for specific AI deployment areas.

The forums for the above stakeholder coordination and engagement vary depending on the nature, scale, and risk profile of the AI solutions at stake. For instance, organizations deploying AI at scale in consumer-facing solutions may define stakeholder collaboration differently and also involve other stakeholders, such as end users or UX specialists. Therefore, the nature of the AI solution should drive the stakeholder selection process.

From our practical experience, such 'working collaboration' is most successful if stakeholders have at least some understanding of the AI technology and the respective requirements/risks that apply. In order to speak to AI teams successfully, one needs to understand some underlying technology aspects, and, vice versa, AI teams benefit from the awareness of some implications of their work, like IP risks, data privacy considerations, and ethical aspects. We will further elaborate on this aspect in the training domain discussed below.

Data governance, AI mapping, and risk assessments

Complementing the above domains, but no less important is the domain of operationalizing data governance, AI mapping, and AI risk assessments, adjusted to the dynamic nature of the AI lifecycle. At its core, AI is all about the collection and use of data, but traditional data governance controls may not always work seamlessly in this space. For this domain, we would like to highlight the following practical considerations:

- Mapping AI systems and use cases - Most organizations start with leveraging existing data mapping processes and tools, for instance, those used in the context of a data privacy program, and potentially tailoring those to the specific needs of AI deployment. Some decide to create dedicated AI repositories, including specific information on sources of data and the manner in which such data is collected, processed, and stored. Depending on the nature of the data used for training, for example personal data, the controls may need to be adjusted. Furthermore, a distinction needs to be made between data used for the purpose of training the model and data that is required to be fed into the solution by the end user following its deployment. To summarize, data should be tracked across the various stages of the AI lifecycle. Further complexity in this space can depend on the technical aspects of pre- and post-processing of data. This usually involves cleaning and scrubbing data, in addition to potentially extracting certain elements of the data for use by the AI solution.
- AI risk assessments - Risks related to the deployment of AI should be assessed for specific use cases, particularly in relation to the deployment of so-called 'general purpose AI systems.' Although tying up the risk assessment process to existing risk assessments, such as the Data Protection Impact Assessment (DPIA), makes sense, additional assessments may need to be built on top based on some triage criteria, taking into consideration societal risks or risks for the organization itself.
- Models oversight - It is important to recognize the role of AI models in powering AI solutions. While the headlines are mostly dominated by mentions of large language models (LLM), it must be noted that there are a wide variety of AI models already in production today. These models perform various complex tasks across the fields of computer vision, image upscaling, audio transcription, and so on. Furthermore, the landscape of AI models is fairly complex. For example, the leading players in the market, such as OpenAI, Google, and Mistral provide their services in a manner similar to that of software as a service (SaaS) products/services. However, one of the defining features of the AI boom in the last few years has been the massive development of the open-source landscape, which has led to the rise of companies such as HuggingFace. Additionally, the recent release of Meta's Llama 3 has created opportunities for start-ups or smaller companies to incorporate this model into their own product to provide a service capable of beating the incumbents in this space. This fast-paced landscape creates challenges for mapping and overseeing the various emerging models in terms of IP liability, privacy, and security concerns as well as the open-source licensing restrictions. Emerging best practices in this regard include a bespoke model of due diligence and oversight that is focused on these features.
- Monitoring output data and bias detection and monitoring - As mentioned above, the AI lifecycle requires continuous oversight and monitoring following the deployment of AI systems into production, particularly in the context of the risks related to bias, copyright infringements, misuse of the AI systems by users, data architecture, and retention for output data, among others. These elements

should be addressed in the AI risk assessment with potential technical guardrails and agreed ways to monitor the model, for example, for the detection of bias.
- Security aspects - Last but not least, a comprehensive risk assessment of deploying AI requires the identification, assessment, and potential remediation of security risks. In this context, involvement and collaboration with the cybersecurity teams in the organization is crucial. Such collaboration from the earliest possible stage is even more important if the organization aims to obtain standard security certifications such as SOC or ISO.

Policies, procedures, and training

The rapid expansion of generative AI tools and employees' appetite to use AI for work-related tasks has forced many organizations to accelerate their efforts in terms of increasing AI literacy amongst employees as well as introducing policies and guardrails for the responsible use of AI.

From a practical perspective, one can differentiate between the following efforts:

- Guidelines/policies for the broader public in the organization - The purpose of such policies is to set forth and communicate guardrails for the responsible use of AI in the context of the performance of various tasks in the workplace. In particular, such simple and practical guidelines should accompany the launch of broadly available generative AI tools that can be used for a variety of tasks. Organizations would need to decide where to draw the line in terms of the nature of the data that should not be used as input for such models and the limitations of access to the output.
- Guidelines/policies for the AI/ product team - These guidelines/ policies should be much more technical in nature and address the risks related to the AI lifecycle that we have discussed above. From practical experience, such guidelines/policies work best if originated/embraced by the AI teams and somehow embedded into the actual tools or workflows used by the AI teams. These guidelines should generally have a dynamic nature and be adjusted to the nature of the AI use case, the development of best practices in tools related to bias mitigation, privacy-enhancing technologies (PETs), etc. They can also be linked to the AI risk assessment process.
- AI upskilling and AI governance certification initiatives - In response to the expansion of the use of AI tools in the workplace, organizations should consider expanding AI literacy and responsible use of AI through training for the broader audience in the workplace. Many formats can be combined to roll out such training, such as by leveraging the expertise of in-house AI teams, bringing external experts, making content available in learning platforms, and organizing awareness sessions and events. Additionally, organizations may consider rolling out external certification programs, for instance the new AI Governance Professional (AIGP) certification offered by the International Association of Privacy Professionals (IAPP) in order to create a network of employees in various roles with an enhanced understanding of AI governance and the regulatory framework.
- Specialized training for AI teams for ethical and regulatory issues - Technical AI and product teams would also benefit from specialized training to address ethical considerations in developing AI, the emerging technologies for bias detection and mitigation, and the broader regulatory issues impacting the development of AI within the organization. These trainings should be tailored to the nature of the AI use cases in the organization and not necessarily focus on the biggest AI risks that make it to the front page if these are not pertinent for the type of models the AI and product teams are working on. Specialized training of this nature provides a great opportunity to bridge the gap between the broader principles and AI governance structure and the actual data mapping, risk assessment, and mitigation in concrete AI systems.

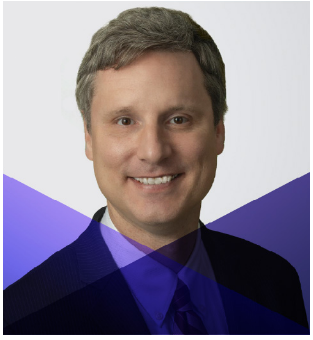
Conclusion

From practical experience, building an appropriate AI governance structure within the organization is a continuous journey and requires a multidisciplinary and holistic approach. Although organizations have a growing number of external frameworks at their disposal, they need to determine what works best in terms of the culture, risk profile, and maturity of their organizations. In the future, these efforts can be leveraged to meet more stringent AI regulatory requirements, such as the risk management system contemplated by the EU AI Act.

USA: Privacy legislation blooms in busy spring

Bart W. Huffman
Partner
bart.huffman@hklaw.com
Holland & Knight LLP

Rachel Marmor
Partner
rachel.Marmor@hklaw.com
Holland & Knight LLP



Kevin Angle
Data strategy, security
and privacy Attorney
Kevin.Angle@hklaw.com
Holland & Knight LLP

With the unofficial start of summer having arrived, legislatures across the country are closing up shop, leaving privacy attorneys to assess the many new developments in the space.

In just five months, the US has seen significant activity at the state as well as federal levels, including some important deviations from past models that, though implemented at the state level, will impact businesses nationally. Three developments are of interest in particular: First, Maryland passed a comprehensive consumer privacy law containing a strict data minimization standard that restricts data collection and flatly prohibits the 'sale' of sensitive data. This standard was quickly copied by Vermont. Second, numerous states and Congress debated the potential harms of artificial intelligence (AI), culminating in Colorado becoming the first US state to adopt legislation specifically focused on preventing algorithmic discrimination. Third, children's privacy has been a hot topic across the country, with many legislatures acting to increase the ages covered by existing protections to 18 and imposing new duties to design products and services to mitigate risks to minors. At the federal level, legislators are moving forward with a comprehensive privacy bill and have adopted a new law, not to be overlooked, that has the potential to restrict some data transfers.

This article provides an overview of the most significant legislative developments in privacy and data in the US in 2024 to date. We do not purport to capture all nuances or even baseline requirements of the laws discussed herein. Some state legislatures remain in session.

The existing landscape for 2024

Before legislatures even began their 2024 sessions, the year was slated to be one of noteworthy evolution on the privacy front. Washington's My Health My Data Act (MHMD) went into effect on March 31 (applicable to 'small businesses' beginning June 30), along with a copycat Nevada law; both implemented strict consent requirements for the collection and sale of 'consumer health data.'

Comprehensive consumer privacy laws go into effect in Texas and Oregon on July 1, and Montana on October 1. The first 'age-appropriate design code' laws go into effect in the US in 2024, as new rules in both Connecticut and Maryland become operational on October 1 (California's Age-Appropriate Design Code Act, which was scheduled to go into effect on July 1, was ruled unconstitutional by a federal district court and an appeal is pending). Florida's Digital Bill of Rights will also go into effect on July 1, but the applicability of most obligations in this law is limited to companies with $1 billion+ in revenues who meet additional narrow criteria. A Florida law related to the protection of children on social media and gaming platforms also goes into effect on July 1; it includes some privacy obligations.

Federal privacy legislation makes progress: APRA and new requirements for data brokers

With so many varying regimes at the state level, federal privacy legislation that would potentially preempt some state laws has long been the white whale of the privacy community. Early this year, it appeared that there was little hope that comprehensive federal privacy legislation would move forward, with legislators focused instead on narrower bills like the Children and Teens' Online Privacy Protection Act (COPPA 2.0) addressing children's privacy. That all changed in April when Senate Committee on Commerce, Science and Transportation Chair Maria Cantwell and House Committee on Energy and Commerce Chair Cathy McMorris Rodgers proposed the American Privacy Rights Act (APRA).

1. American Privacy Rights Act

The bi-cameral, bi-partisan APRA shares many similarities with 2022's American Data Privacy and Protection Act (ADPPA), including its extensive requirements around data minimization and inclusion of standard rights like the rights to access and delete personal data. The APRA would require businesses to employ privacy or security officers, and 'large data holders,' businesses with over $250 million in revenue meeting data volume thresholds, would be required to meet administrative and accountability requirements such as annual certifications and Privacy Impact Assessments. Importantly, like the ADPPA, the APRA would preempt many state laws, including the California Consumer Privacy Act (CCPA). The APRA, like the ADPPA, would also include a private right of action, but only for actual damages. The APRA's private right of action would apply to violations related to transparency, sensitive data, biometric and genetic information, and data breaches.

Although there is momentum behind the APRA given its prominent support from leading committee chairs from both parties, it has also met notable opposition. Many in the industry oppose its private right of action, while some privacy advocates and state regulators oppose preemption of state requirements providing an arguably higher ceiling for privacy rights. It is likely the APRA will undergo a lengthy process of evaluation and amendment if it moves forward at all.

2. Protecting sensitive data from foreign adversaries

Although the APRA will likely have a long road ahead, Congress moved quickly in passing the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFAA), which was signed into law on April 24, 2024. PADFAA will restrict the transfer of 'sensitive personal information' by 'data brokers' to Russia, China, Iran, and North Korea, as well as entities with ties to those countries, including some individuals or businesses domiciled in one of those countries as well as businesses in whom such persons have a 20% stake or that are subject to the direction or control of such persons. As a result, PADFAA will require many businesses to conduct counterparty diligence prior to making such transfers.

'Sensitive personal information' is defined quite broadly. In addition to standard categories like health, race, and ethnicity data, it includes things like

- histories of online activity over time;
- information about children under 17;
- information about video content; and
- calendar and address book information maintained for private use.

Violations of the PADFAA will be an unfair or deceptive act or practice enforceable by the Federal Trade Commission (FTC) under §18(a)(1)(B) of the FTC Act (15 U.S.C. 57a(a)(1)(B)). The law will take effect on June 23, 2024, giving businesses little time to put in place compliance programs.

New state comprehensive consumer privacy bills adopted

In the absence of a congressional consensus on federal legislation, state legislatures across the country have continued to move forward with enacting comprehensive consumer privacy legislation. If bills currently pending gubernatorial signatures in Minnesota and Vermont pass, 19 States (excluding the limited Florida law) will have enacted comprehensive consumer privacy laws - seven in 2024 alone.

1. New Jersey, New Hampshire, Nebraska, and Kentucky

Four laws passed in 2024 - in New Jersey, New Hampshire, Nebraska, and Kentucky - largely follow the Virginia model, with only minor variations.

For example, New Jersey requires businesses to collect opt-in consent to process personal information of children aged 13 to 17 for profiling in furtherance of decisions that produce legal or similarly significant effects; of previously enacted laws, only Oregon required consent for such profiling, for children aged 13 to 15. As another example, Nebraska follows the Texas model for defining business subject to the privacy law - namely, that all businesses that process any personal information of the State's residents are covered, except for small businesses that do not sell sensitive personal information.

2. Maryland

Maryland stands to change the game significantly when the Maryland Online Data Privacy Act (MODPA) goes into effect in October 2025. MODPA will implement strict data minimization standards, requiring businesses to limit their collection of personal information to what is 'reasonable necessary and proportionate to provide or maintain a specific product or service requested by the consumer.' Sensitive data may not be collected or processed unless 'strictly necessary' and may not be sold (with no option to get consent). Consent is required for collecting personal information for the 'sole purpose' of content personalization or marketing, as well as for the sale or processing for targeted advertising of personal information relating to a consumer between ages 13 and 17.

3. Vermont

Vermont passed legislation in mid-May that would significantly expand the existing slate of privacy laws with the Vermont Data Privacy Act (VDPA). As of this writing, the Vermont Governor has not stated whether he will sign or veto the law, and an official version has not yet been published. The core provisions of the Vermont Act become effective on July 1, 2025. The VDPA would follow Maryland in requiring strict data minimization and, unique among the current wave of privacy laws, would include a private right of action. As a political compromise for enactment, the private right of action was watered-down somewhat and would be applicable only against data brokers or 'large data holders' (which have processed 100,000 or more Vermont residents' data - i.e., data of approximately 1/6 of all Vermonters - in the preceding calendar year). In particular, beginning January 1, 2027, an aggrieved consumer can bring an action to recover actual damages sustained in the processing sensitive data without consent, processing sensitive data in violation of COPPA, selling sensitive data, or violating the act's provisions concerning the confidentiality of consumer health data. The private right of action is to be studied by the Vermont Attorney General and will sunset in January 2029. A primary concern throughout the legislative process has been that unjustified litigation would unduly burden Vermont businesses.

4. Minnesota

The Minnesota Consumer Data Privacy Act (the Minnesota Act), passed in May, and will take effect in July 2025. The act generally follows the trend of other state comprehensive privacy laws. However, it includes a novel accountability measure in the form of a requirement to maintain specific records with respect to policies and procedures adopted to comply with the Minnesota Act (including contact information for responsible individuals). Making an implicit requirement explicit, the Minnesota Act requires that controllers must maintain a personal data inventory. Also, instead of the term 'precise geolocation' as a category of sensitive data, the Minnesota Act defines 'specific geolocation data,' which includes a street address derived from geographical coordinates or a location established by geographical coordinates with an accuracy of more than three decimal degrees. In a manner similar to the draft California and enacted Colorado regulations, the Minnesota Act provides consumers with the right to challenge and ask questions about automated profiling, including the data used and the decisions made based on such profiling.

Children's data rules expand

The US has seen a shift in the past year from a notice and consent model with regards to data that may belong to children to an 'age-appropriate design code' model, where companies must assess whether children are likely to use their products and services, conduct Data Protection Impact Assessments (DPIA), and implement strict privacy settings by default. This model was first enacted in the UK, where the Age Appropriate Design Code, a set of standards for the processing of children's data that is enforceable under the General Data Protection Regulation (GDPR), took effect in 2020.

1. Maryland

The first such age-appropriate design code in the 2024 class, the Maryland Kids Code (officially named the Maryland Age-Appropriate Design Code Act), applies to 'covered entities' that offer any 'online product' that is 'reasonably likely to be accessed by children.' This definition includes products that are directed to children as defined by COPPA but goes further, capturing products that have design elements known to be of interest to children as well as where the covered entity knows or should have known that the user is a child. The child is defined as an individual under 18, further expanding from the COPPA baseline. The Maryland law has a short on-ramp to compliance, as it becomes effective on October 1 of this year.

The Maryland Kids Code does not contain any consent requirements (those are found in MODPA) but does impose certain restrictions on processing children's data. Such data cannot be processed in a way that is inconsistent with the best interests of children, and profiling of children is prohibited unless necessary to provide a product, appropriate safeguards to protect children are in place, and the profiling is in the best interest of children. Processing precise geolocation is prohibited unless strictly necessary for the product and for a limited time, and default privacy settings must be configured to offer a high level of privacy unless there is a compelling reason why a different setting is in the best interest of children. The Maryland Kids Code also requires DPIAs for all online products reasonably likely to be accessed by children to document whether the product is designed in a manner consistent with the best interests of children.

Following the passage of the Maryland law, Colorado and Virginia amended their comprehensive privacy laws to add new requirements related to the processing of children's data. Virginia amended the definition of child in the VCDPA to cover persons younger than 18, resulting in the law requiring consent for any processing of personal information for individuals under 18, including the sale of personal information and targeted advertising. Virginia will also require consent to process precise geolocation and additional documentation in the DPIA of the assessment related to an online service, product, or feature where the business has actual knowledge of child users. Colorado also amended the definition of a minor to extend to individuals under 18 and added a new 'duty of care' to avoid heightened risk to minors where the business has actual knowledge that minors are users of an online service, product, or feature. Consent is required to process a minor's data for targeted advertising or sale, and to collect precise geolocation. Colorado similarly will add new assessment criteria to DPIAs when data of known minors will be processed.

AI: First AI-specific laws targeting algorithmic discrimination

Although having wider applications than only in the privacy space, states and the Federal Government have moved forward with AI-related bills that could significantly impact businesses using personal data. In particular, these laws will likely apply to uses that are carved out of many 'comprehensive' consumer privacy laws, such as evaluations of employees (currently, only California's 'comprehensive' law applies to employee data). In addition to the laws described below, states such as California have pending issues like algorithmic discrimination and AI safety standards.

1. Colorado: SB 205

In May, Colorado became the first state to adopt a law focused on AI with specific requirements intended to mitigate the risk of 'algorithmic discrimination' applicable to both developers and deployers of AI. The law, which could provide a model for other states, also requires developers and deployers to label AI products that interact directly with consumers. The law's novel algorithmic discrimination requirements apply to systems making decisions in an enumerated set of situations considered to be 'consequential,' such as employment, education, lending, financial services, and healthcare. The law applies to both the developers and deployers (i.e., users) of AI, and requires both to adopt reasonable procedures to avoid algorithmic discrimination, which is a use of AI that 'results' in 'unlawful differential treatment or impact' that disfavors particular protected classifications.

Some of SB 205's other requirements include making public disclosures, adopting risk management procedures, conducting impact assessments, and, importantly, notifying the State Attorney General in the event algorithmic discrimination is identified. The latter requirement could increase the likelihood of investigation and scrutiny, although businesses should also consider a proactive approach to engaging with regulators to help them

> In just five months, the US has seen significant activity at the state as well as federal levels, including some important deviations from past models that, though implemented at the state level, will impact businesses nationally.

better understand the risks and benefits of their AI products. Compliance with these requirements creates a rebuttable presumption that a business has adopted reasonable procedures, and businessesalso have the ability to cure violations they detect where the business follows designated AI frameworks. The law will be enforced by the state attorney general.

2. Utah: SB 149

Although not as comprehensive as Colorado, deployers of generative AI tools that interact with consumers should not overlook the Utah Artificial Intelligence Policy Act (SB 149). That law went into operation on May 1, 2024, and requires businesses using generative AI to interact with Utah residents, such as businesses using AI chatbots, to inform the individual that they are interacting with AI and not a human if asked or prompted. Businesses that provide services in a 'regulated occupation,' which is an occupation requiring licensure or certification in the State such as a physician, must affirmatively disclose the use of AI whether or not prompted. In practice, many businesses may opt to label chatbots and other AI tools that interact with consumers whether or not the consumer makes a specific request for that information.

Biometrics privacy continues to be a focus

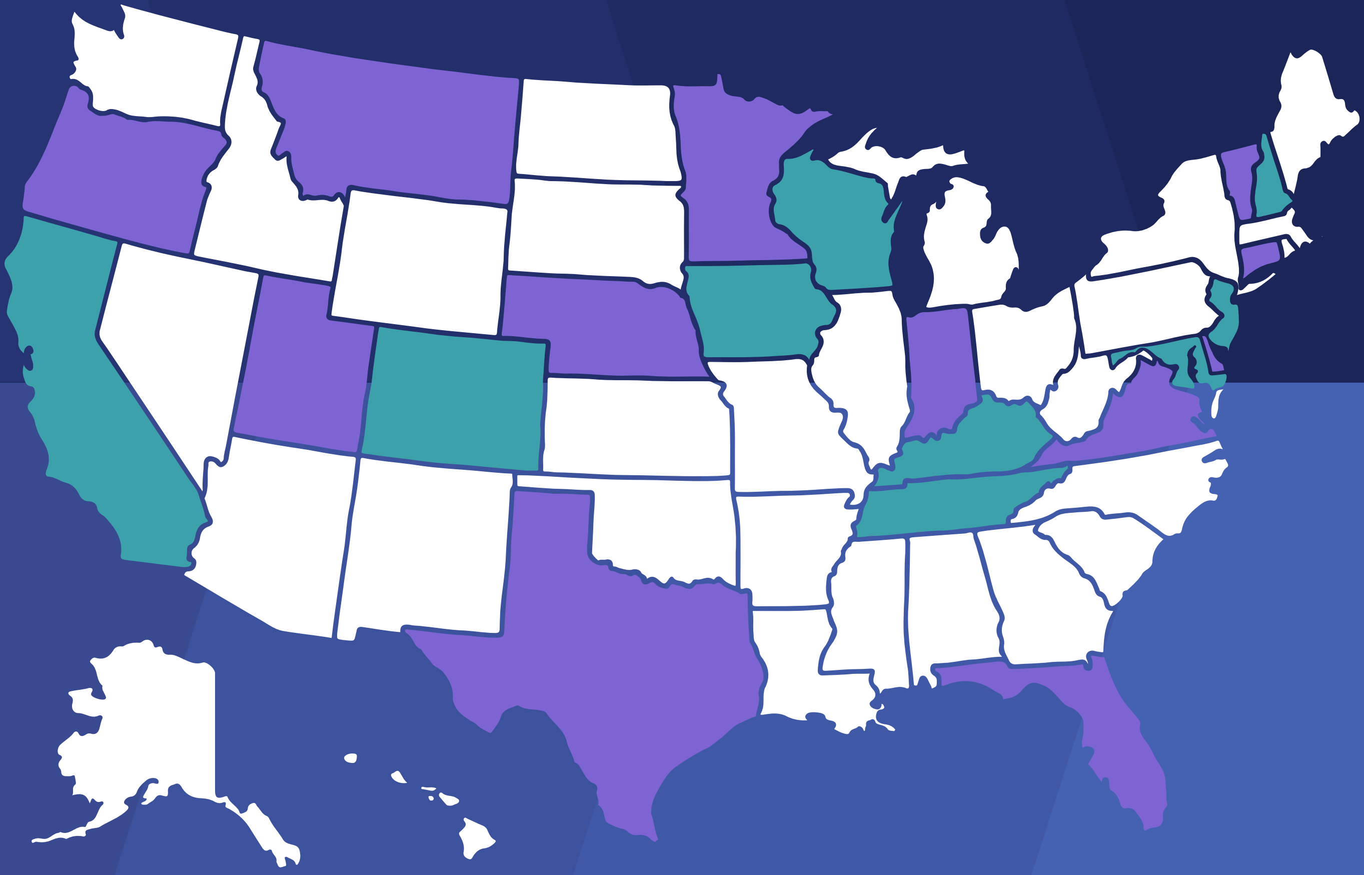
Colorado passed an amendment to its privacy law in April that adds and incorporates various biometric data provisions such as §6-1-1314 of the Colorado Revised Statutes. Biometric data was already addressed as sensitive data within the Colorado Privacy Act, but this new law adds the typical policy, security, and data retention (as well as consent) requirements featured in other biometric laws. Notably, the requirements apply to present or former employees as well as consumer data. The statute includes limitations on conditioning consumer access to services or eligibility for employment on consent to biometric data; in the employment context, the limitations can be bypassed to some extent through 'reasonable expectations' established in a job application.

There is no private right of action, and the new provisions apply to biometric data collected or otherwise processed on or after July 1, 2025. For most purposes, the biometric data provisions apply to any entity doing business in or directing goods or services into Colorado, regardless of size or volume of data processing but subject to the existing exceptions that are already in the Colorado Privacy Act (e.g., for financial institutions subject to the Gramm-Leach-Bliley Act (GLBA)).

In addition to Colorado, biometric privacy would be addressed in the federal APRA, if adopted. In Illinois, the legislature approved SB 2979, which would limit exposure under the Biometric Information Privacy Act's (BIPA) statutory damages provision to one violation per person, overruling an Illinois Supreme Court holding that violations would incur each time a biometric identifier is scanned, potentially multiple times per day. At the time this article was drafted, that bill is currently awaiting signature from the State's Governor. Although the bill would somewhat mitigate the potential for 'annihilative liability,' in practice, businesses facing BIPA lawsuits will still be forced to contend with significant potential damages awards.

Final thoughts

Data law has picked up speed in the hands of state legislatures that are working hard to plug holes and raise guardrails. While the 'laboratories of democracy' framework has worked to push the law forward, it has also resulted in a landscape that is full of stark differences and subtle nuances from state to state, creating challenges when the technologies and services that legislators are seeking to regulate are offered nationally and often globally. The pace of legislative development will likely slow during the second half of 2024 as politicians focus on elections, but the push and pull between regulation and enabling innovation is likely to spill over into the next sessions.



Country profile: India

A primer on India's new data privacy law

Arun Babu
Partner
arun.babu@bgl.kochhar.com
Kochhar & Co., Bangalore

Introduction

On August 11, 2023, the Indian Government enacted India's new data privacy law, the Digital Personal Data Protection Act 2023 (DPDPA). The DPDPA has however not come into force as of now. Once implemented, the DPDPA will supersede India's current data privacy laws.

India presently has minimal data privacy laws which only apply to the processing of a special category of personal data termed Sensitive Personal Data or Information (SPDI). SPDI refers to passwords, biometric information, sexual orientation, medical records and history, and health-related information, and an entity processing SPDI is solely obligated to implement reasonable security practices and procedures to protect such data.

The DPDPA is India's first comprehensive data privacy law, and it seeks to enable the processing of personal data in a manner that balances the right of individuals to protect their personal data and the need to process such personal data for lawful purposes.

Applicability of the DPDPA

The DPDPA applies to the processing of all personal data maintained in digital form. The DPDPA has extra-territorial applicability, and in addition to the processing of personal data within India, it applies to the processing of personal data outside India where such processing is in connection with any activity aimed towards providing goods or services to individuals within India.

The DPDPA however does not apply in case of certain processing scenarios. The DPDPA does not apply to personal data processed by an individual for any personal or domestic purposes. The DPDPA also does not apply to the processing of publicly available personal data made so available by the data principal (akin to a data subject under the General Data Protection Regulation (GDPR)) or by any person obligated under any Indian law to do so. There is also an exemption from the applicability

of the DPDPA where personal data is processed by a notified government agency for purposes related to national security or for preventing an offense, or where processing of personal data is necessary for research, archival, or statistical purposes and if such processing is performed in a prescribed manner.

Except for the processing scenarios mentioned above, the DPDPA applies to the processing of digital personal data for all other purposes, and such processing must be based on a lawful ground prescribed under the law.

Lawful grounds for processing

Consent is the primary lawful basis for processing personal data under the DPDPA. Consent under the DPDPA must be free, specific, informed, unconditional, unambiguous, and indicated using a clear affirmative action. This means that there needs to be a clear and unambiguous statement of why the personal information is being collected and there must be a consent obtained for that specific purpose. Interestingly, the consent requirements under the DPDPA are almost identical to those under the GDPR. Therefore, in the absence of any further guidance from the Government, India would likely follow the same jurisprudence in relation to consent as under the GDPR, which would make obtaining valid consent extremely difficult. However, in contrast to the GDPR, the DPDPA does not include other lawful grounds such as legitimate interest, contractual necessity, etc.

The DPDPA however permits processing without consent for certain 'legitimate uses' of personal data. These include, among others, processing for purposes related to employment and to prevent loss or liability to an employer; processing in case of medical emergencies, breakdown of public order, disaster management, or for performance of statement functions; and processing where a data principal voluntarily provides personal data to a data fiduciary (akin to a data controller under the GDPR) for a specified purpose.

Children's personal data

The DPDPA prescribes additional obligations and safeguards for processing children's personal data. A child is defined under the DPDPA to mean a person aged less than 18 years. A data fiduciary is obligated to obtain verifiable consent from a child's parent or lawful guardian before processing his/her personal data. The manner in which such verifiable consent must be obtained is however not prescribed under the law, and the Government is empowered to notify rules stipulating the same.

Further, data fiduciaries are obligated to not undertake any processing that is likely to cause any detrimental effect on the well-being of a child, and unless exempted by the Government data fiduciaries are prevented from undertaking tracking or behavioral monitoring of children or targeted advertising directed at children.

Rights and duties of data principals

The law includes typical rights of data principals such as the right to access what personal data is being processed and processing activities undertaken in relation to such data; the right to correction, updating, and deletion of personal data; and the right to grievance redressal. Notably, the DPDPA includes a right to a data principal to nominate an individual who shall exercise rights of such data principal under the law, in case of death or incapacity of such data principal. The law however does not include rights such as the right to data portability, and the right to be not subjected to automated and processing activities undertaken in relation to such data; the right to correction, updating, and deletion of personal data; and the right to grievance redressal. Notably, the DPDPA includes a right to a data principal to nominate an individual who shall exercise rights of such data principal under the law, in case of death or incapacity of such data principal. The law however does not include rights such as the right to data portability, and the right to be not subjected to automated decision-making.

Interestingly, the DPDPA prescribes duties for data principals. These include duties to comply with applicable laws while exercising rights under the DPDPA, not register false or frivolous grievances or complaints with a data fiduciary or with the data protection board, and to furnish only verifiably authentic information while exercising their right to correction or deletion.

Data security safeguards and data breach notifications

The DPDPA obligates data fiduciaries to implement reasonable security safeguards to prevent a personal data breach, and to put in place appropriate technical and organizational measures to measures to comply with their obligations under the DPDPA. However, the DPDPA does not prescribe any such specific safeguards or measures. Data fiduciaries may therefore implement security safeguards, and technical and organizational measures, which are comparable to industry best practices and are commensurate to deal with risk associated with processing undertaken by them.

A personal data breach is broadly defined under the DPDPA to mean any unauthorized processing or accidental disclosure, use, alteration, destruction, or loss of access to personal data that compromises its confidentiality, integrity, or availability. The DPDPA requires all personal data breaches to be reported to the affected data principal and the data protection board (proposed to be established under the DPDPA) and does not prescribe any impact thresholds or criteria for reporting personal data breaches. The law also does not prescribe the timeline and the modalities for breach reporting and empowers the Government to prescribe rules in this regard.

Data localization

There are no data localization restrictions under the law. The Government is however empowered to notify a blacklist of countries to which data transfers would be restricted.

The DPDPA states that it shall not restrict the applicability of any other Indian law that provides for a higher degree of protection for, or restrictions on, cross-border transfer of personal data from India. In this regard, it is relevant to note that India has data localization restrictions under various sector-specific laws that apply to regulated entities operating in sectors such as payments, digital lending, telecom, securities, and insurance.

Data storage limitations

The data storage limitations under the DPDPA are applicable only where personal data is processed based on consent. In such case, unless there is a data retention obligation under any other applicable law, data fiduciaries are obligated to delete personal data once consent is withdrawn or if the purpose for which it is collected is served.
It is relevant to note that the law deems the purpose of collection to be fulfilled if the data principal does not approach the data fiduciary for the performance of the purpose for which the data was collected and for exercise any of the data principal's rights in relation to such processing for a period to be specified by the Government.

Data processors

There are no specific obligations on data processors, and almost all compliance requirements under the DPDPA apply to data fiduciaries. Further, the DPDPA obligates a data fiduciary to ensure their data processors' compliance with the law in respect of any processing undertaken by them on behalf of such data fiduciary. Data fiduciaries are also obligated to execute a data processing agreement with their data processors.

Penalties

The DPDPA prescribes monetary penalties for non-compliance. For instance, a penalty of up to INR 2.5 billion (approximately $30 million) is prescribed for failure to implement reasonable security safeguards to prevent a data breach. There is however no provision under the law that enables payment of compensation to data principals affected by a violation of the law.

Way forward

The DPDPA unfortunately does not prescribe any timelines for implementation or a gestation period for organizations to ensure compliance with the DPDPA, and empowers the Government to do so. When the DPDPA was enacted in August last year, the Government had stated that it expected to implement the law within 10 months. The implementation of the law was however delayed due to India's ongoing federal elections. Nevertheless, it is expected that the DPDPA will come into force by the end of this year and the rules implementing the DPDPA will be notified within the next 2-3 months. Given that India presently has minimal data privacy laws and low privacy standards in general, it is also expected that the Government will provide organizations with a reasonable timeframe to prepare for and start complying with the new law.

Infographic

onetrust
DataGuidance

An overview of the EU AI Act

Goal

Foster the development, use, and uptake of AI in the market while also protecting health, safety, and fundamental human rights

Scope

The EU AI Act applies to:

- AI systems, defined in line with international organizations, namely the OECD
- AI systems made available on the Union market
- AI systems located in a third country, where the output of the system is used in the Union
- Providers, deployers, importers, and distributors of AI systems
- All industries (Some are considered higher risk than others)

Definitions

AI system
A machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments

Provider
A natural or legal person, public authority, agency, or other body that develops an AI system or a general purpose AI model or that has an AI system or a general purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge

Deployer
Any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity

Authorized representative
Any natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or general purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation

Risk levels

Unacceptable risk - Prohibited
Social scoring systems, real-time remote biometric verification, with limited exceptions

High risk – Conformity assessment required for use
Credit scoring or creditworthiness systems, automated insurance claims

Limited risk – Transparency required for use
Chatbots

Minimal risk – voluntary code of conduct for ethical use
AI-enabled video games, spam filters

Enforcement and penalties

Non-compliance with prohibited AI practices are subject to fines of €35m or, if a company, up to 7% of their global worldwide turnover from the previous year, whichever is higher.

Non-compliance of an AI system with any provisions related to operators or notified bodies are subject to administrative fines of €15m or, if a company, up to 3% of their global worldwide turnover for the previous year, whichever is higher.

Track developments and understand the EU AI Act

OneTrust DataGuidance Research

California: Is California poised to blaze its own trail toward regulating automated decision-making technologies?

Alex Altman
Senior Associate
alexander.altman@
arnoldporter.com
Arnold & Porter Kaye,
San Francisco

Introduction

California has recently taken steps to shape the regulatory landscape for businesses employing automated decision-making technologies (ADMT). Specifically, the California Privacy Protection Agency (CPPA) is considering draft regulations pursuant to its rulemaking authority under the California Consumer Privacy Act (CCPA). The California legislature is additionally considering no fewer than five pieces of legislation targeting ADMTs, with several others targeting generative artificial intelligence (AI) as well. This regulatory push is taking place even as other jurisdictions have established (or are working to establish) their own ADMT rules. As is so often the case when California flexes its regulatory muscle, a key question affected businesses will want to answer is whether the State is blazing a unique trail, thus requiring compliance with differing - or even divergent - sets of rules across jurisdictions. Will California's regulation of ADMTs require businesses to consider complex, jurisdiction-specific compliance programs? Will businesses be best served by adopting a 'lowest common denominator' approach to ensure their implementation of ADMTs complies across jurisdictions? Or will California's regulation of ADMTs amount to no more than a distinction without a difference, requiring only minimal efforts to harmonize compliance efforts?

Background

California's drive to regulate ADMTs is perhaps unsurprising, given the State's place in the global economy as a source of tech innovation, particularly with respect to ADMTs and other AI technologies. Indeed, California's culture of innovation (coupled with its unique lawmaking process) was widely credited for spurring the drafting and passage of the first-of-its-kind state consumer privacy law, the CCPA, in 2018. In the wake of the CCPA, no fewer than 15 other states have passed their own consumer privacy laws, with most other states - and the U.S. Congress - considering broad consumer privacy legislation. While most of these laws are roughly modeled on the EU's General Data Protection Regulation (GDPR), the CCPA uses unique terminology

and a unique regulatory framework. Companies that had established GDPR-focused compliance programs have sometimes found themselves struggling to adapt to the CCPA. Others, however, have seen that the principles underlying the CCPA (e.g., transparency and consumer rights) largely mirror the GDPR, and that many differences were either cosmetic or required only modest adjustments to existing compliance efforts. Whether California's efforts to regulate ADMTs create similar challenges remains to be seen, but there are several areas in which potential incongruities may arise.

California's efforts to regulate ADMTs

The CPPA's rulemaking activity under the CCPA represents the most mature effort to regulate ADMTs in California thus far. In 2020, the California Privacy Rights Act (CPRA) was passed by ballot measure and amended the CCPA in a number of key aspects. Importantly, the CPRA required the eventual promulgation of rules 'governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling.' Interestingly, the CPRA did not define automated decision-making technology, nor did it explicitly state that businesses must provide specific notice and opt-out rights with respect to ADMTs. Rather, it left the contours of the definitions and recognition of these rights to the rule makers, i.e., the California Attorney General and subsequently the CPPA. This is precisely what has taken place. Preliminary rulemaking began in December 2023, with the CPPA board considering an initial draft of ADMT rules. The CPPA board met on March 8, 2024, voting to take the next step toward advancing a revised draft of the proposed ADMT rules (the Draft ADMT Rules) to formal rulemaking, which is expected to begin later this year, and likely will not be complete until sometime in 2025. In broad strokes, the Draft ADMT Rules provide that:

- businesses must conduct a risk assessment before using ADMTs 'for a significant decision concerning a consumer or for extensive profiling', or for certain use cases for processing personal information to train automated ADMTs;
- ADMT-related risk assessments must identify, inter alia:
  - how the business plans to maintain the 'quality of personal information' processed by the ADMT;
  - the logic of the ADMT; and
  - whether the ADMT has been evaluated to ensure it works as intended and does not discriminate based upon protected classes;
- a business using ADMTs must provide a 'pre-notice' informing consumers of:
  - how the business uses ADMTs;
  - the consumers' right to opt out of, and to access information about, the business's use of ADMTs; and
  - the logic used in the ADMT, including intended 'outputs;'
- businesses must provide two or more designated methods for submitting requests to opt out of the use of ADMTs; and
- businesses must, upon request, provide consumers with access to information regarding how the business has used their personal information for ADMTs, including the outputs generated by the ADMTs and how the business used those outputs.

The California legislature is independently considering a number of bills that may regulate ADMTs - some of which may overlap with or diverge from the Draft ADMT Rules, for example:

- AB 2930 would require businesses implementing (and developing) ADMTs to complete annual impact assessments, comply with notice provisions, and prevent the release of biased algorithms.
- AB 2877 would amend the CCPA to prohibit developers of ADMTs from collecting and using the personal information of consumers under the age of 16 for training ADMTs and other AI tools without first obtaining the express consent of the consumer (or their parent). Even with such consent the training data would be required to be de-identified and aggregated.

- AB 3204 would amend the CCPA to require a business that uses personal information to train AI (which would likely include many ADMTs) to publicly register with the CPPA, pay a registration fee, and provide information regarding the business and its AI-training practices.
- SB 892 and SB 1220 would additionally regulate how the State itself may deploy ADMTs, including by requiring the promulgation of rules surrounding risk assessments and restricting the use of ADMTs that eliminate or automate core job functions of workers.

While it is far from certain that these bills will ultimately be enacted (particularly in their current forms), they represent an appetite for California to push ADMT regulation into areas that have not generally been considered, and in ways that may burden businesses in unique ways, including by potentially requiring jurisdiction-specific compliance measures.

Key consideration: Scope and the level of human involvement

The fundamental question businesses will need to grapple with when developing programs to comply with disparate ADMT rules is all about scope. When does a decision-making process become an ADMT, and thus become subject to the relevant regulations? In this respect, the Draft ADMT Rules are seemingly expansive, defining an ADMT as 'any technology that processes personal information and uses computation to execute a decision, replace human decision-making, or substantially facilitate human decision-making.' Draft legislation can seem similarly broad, with AB 2930 regulating ADMTs that have been developed to 'make, or be a substantial factor in making, consequential decisions.'

The inclusion of technologies that 'substantially facilitate human decision-making' arguably expands the scope of the Draft ADMT Rules beyond other regulatory regimes. For example, the rules promulgated under the Colorado Privacy Act (CPA) require businesses to allow consumers to opt out of 'human reviewed automated processing' and 'solely automated processing,' but not 'human *involved* automated processing' (i.e., any ADMT 'where a human (1) engages in a meaningful consideration of available data used in the processing or any output of the processing and (2) has the authority to change or influence the outcome of the processing.'). Other state laws, such as the Virginia Consumer Data Protection Act (VCDPA), set forth requirements for profiling based on 'automated processing,' but do not define that term or otherwise make clear what level of human involvement will take a given processing activity out of the realm of profiling or an ADMT subject to additional obligations.

The VCDPA's definition of profiling is drawn directly from the GDPR, which additionally provides in Article 22 that, subject to certain exceptions, data subjects 'shall have the right not to be subject to a decision based *solely* on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.' Recital 71 to the GDPR additionally clarifies that processing personal data for profiling 'should be subject to suitable safeguards, [including] the right to obtain human intervention.' It would seem, therefore, that there is a potential disconnect between the GDPR and the Draft ADMT Rules as to whether human involvement in decision-making makes a process not an ADMT. Under the GDPR, injecting human involvement would seem to take a processing activity out of the scope of ADMTs, but human involvement may not be enough to escape obligations in California under the Draft ADMT Rules. The seeming difference between the two regimes' approaches, however, may not be as significant as it might first appear. In April 2023, the Amsterdam Court of Appeal ruled on a case against Uber B.V. brought by Uber drivers who alleged that the company violated Article 22 of the GDPR by failing to notify the drivers that the company used ADMTs to make decisions to deactivate the drivers' accounts for suspected fraudulent activities. Uber argued that, although the suspected fraudulent activity was identified through automated processing, the final decision to deactivate the suspect accounts was made by human members of its operational risk team and that, therefore, the decisions were not 'based solely on automated processing.' With respect to some of the drivers, however, the court faulted Uber for failing to adequately explain how the human involvement in the deactivation decision was 'meaningful,' and thus ruled that Uber's lack of transparency with respect to its ADMT violated Article 22.

Some state consumer privacy laws, such as the Texas Data Privacy and Security Act (TDPSA), track the language of the GDPR, regulating profiling only to the extent it consists of 'solely automated processing.' Whether this will, in practice, sweep in activities where some human involvement exists remains to be seen.

Conversely, the Draft ADMT Rules appear to align with recent insights gleaned from enforcement activity by the Federal Trade Commission (FTC). In a December 2023, the FTC published a proposed settlement with Rite Aid resolving allegations that Rite Aid violated §5 of the FTC Act, 15 U.S.C. §45, by using facial recognition technology to identify shoplifters in an unfair manner that harmed consumers. Under the settlement, Rite Aid would be limited in its use of any 'automated biometric security or surveillance system,' which includes certain biometric ADMTs 'notwithstanding any assistance by a human being.' Similarly, under the draft American Privacy Rights Act (APRA), special obligations would apply to the use of 'covered algorithms,' which include certain ADMTs 'that make[] a decision or facilitate[] human decision-making.' It is also worth noting that, as currently drafted, APRA would preempt the CCPA and thus render the Draft ADMT Rules a dead letter.

California's push to regulate ADMTs may arguably sweep in activities that would be exempt under other regulatory regimes, but its scope may ultimately hew closer to existing and proposed regulations. In either event, businesses implementing

> The California legislature is additionally considering no fewer than five pieces of legislation targeting ADMTs, with several others targeting generative AI as well.
>
> **Alex Altman**
> Senior Associate

ADMTs will want to carefully calibrate the level of human involvement in their decision-making processes to determine whether they are subject to applicable ADMT regulations.

Consent: Opt-in or opt-out?

Under California's Draft ADMT Rules, consumers would have the right to opt out of businesses using their personal information for certain ADMTs. This aligns with approaches under the CPA, the VCDPA, the TDPSA, and consumer privacy laws enacted in Connecticut, Delaware, Indiana, Kentucky, Montana, Nebraska, New Hampshire, New Jersey, and Oregon. Consumer privacy laws in Iowa, Tennessee, and Utah do not require consent - either opt-in or opt-out - for businesses to use personal information in ADMTs. Importantly, California's proposed approach contrasts with the GDPR, which, subject to certain exceptions, prohibits controllers from using personal data in ADMTs without affirmative, opt-in consent.

Consent management has long been a challenge for businesses operating across jurisdictions with varying privacy laws. This challenge will invariably be exacerbated where differing consent models are adopted with respect to ADMTs. Nevertheless, California's proposed opt-out model would comport with other state laws, which should lessen the burden of administration.

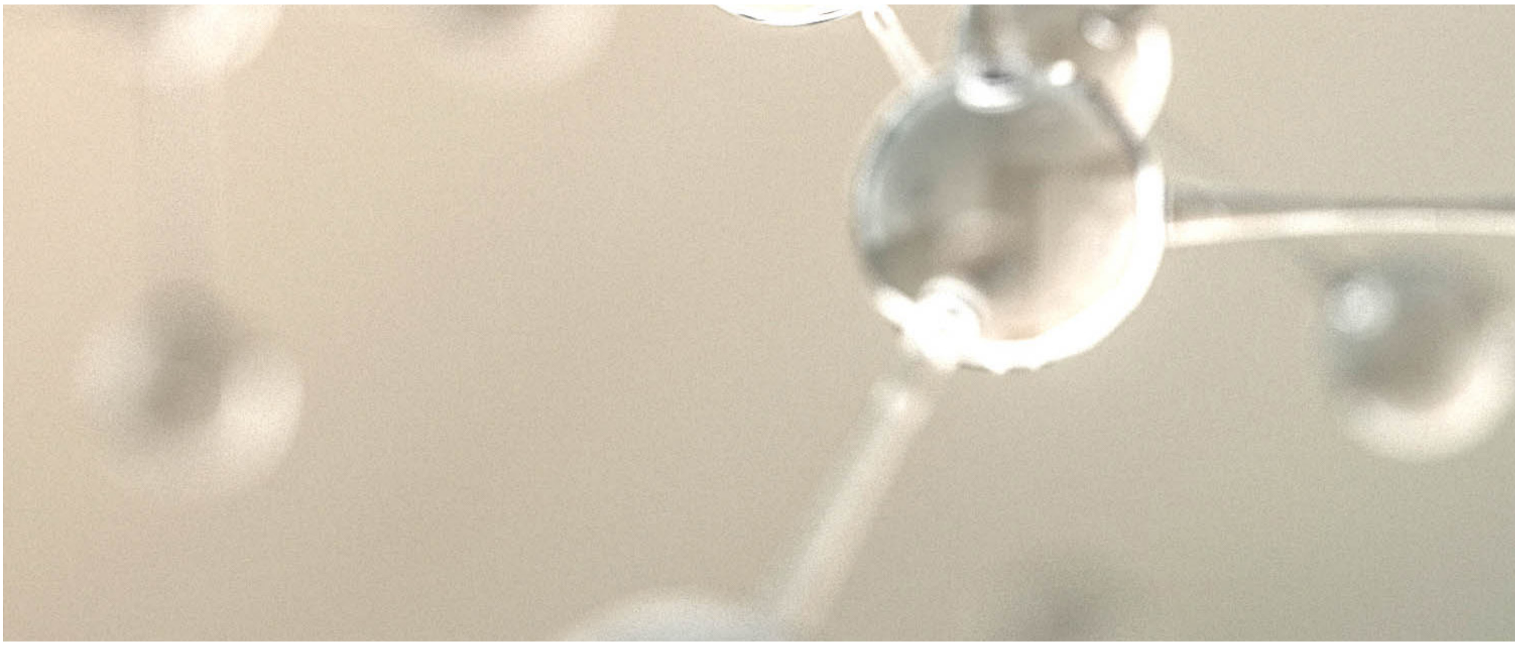
Risk and impact assessments

Most laws purporting to regulate ADMTs require that businesses conduct some sort of risk or impact assessment before deploying the relevant technology. In this respect, California's Draft ADMT Rules are not particularly unique. The devil, of course, is in the details. The Draft ADMT Rules are highly specific with respect to risk assessments generally, and even more so for ADMT-related risk assessments. For example, risk assessments for ADMTs must include consideration of measures a business takes to maintain 'quality of personal information,' which encompasses 'completeness, representativeness, timeliness, validity, accuracy, consistency; and reliability of the sources of the personal information.' Risk assessments must also consider the logic of the ADMT and the outputs of the technology. They must also include an assessment of whether the ADMT discriminates against protected classes. If enacted, AB 2930 would separately require deployers and developers of certain ADMTs to conduct impact assessments with elements that arguably overlap with most of those required for risk assessments under the Draft ADMT Rules. AB 2930, however, would additionally require a description of safeguards intended to address 'reasonably foreseeable risks of algorithmic discrimination' in the ADMT as well as a description of how the ADMT will be used by natural persons to make decisions.

With the exception of the rules promulgated under the CPA (and, potentially, requirements for covered algorithm impact assessments under APRA), rules surrounding risk assessments for ADMTs in jurisdictions outside of California are far less detailed, giving businesses greater flexibility in understanding and documenting the risks of implementing ADMTs in various situations. California, therefore, may impose substantial additional burdens on businesses implementing ADMTs. Nevertheless, businesses with a history of assessing ADMTs in other jurisdictions may already be considering the specific elements that could be required under the Draft ADMT Rules and AB 2930. Ultimately, however, California is likely to step into the regulatory vacuum left by the lack of specificity in other regulatory regimes, potentially setting the standard for ADMT risk and impact assessments in other jurisdictions.

Conclusion

As with the CCPA, California appears to be blazing its own trail when it comes to regulating ADMTs. The Draft ADMT Rules and proposed legislation have the potential to impose upon businesses a set of obligations when implementing ADMTs that may not be necessary under other jurisdictions' laws. The expansive scope of these measures to include ADMTs that have a substantial impact on human decision-making goes beyond some state laws, and possibly beyond the GDPR. Those businesses deploying ADMTs across jurisdictions will also have to contend with the familiar burden of consent management, but the prevalence of opt-out consent in the US may make it easier to adopt a uniform consent mechanism. Finally, although most laws regulating ADMTs require some sort of risk or impact assessment, proposed regulations in California are particularly prescriptive, and it is quite possible that California's requirements will become the template for risk assessments in other jurisdictions. Businesses developing and implementing ADMTs, therefore, should keep a close eye on developments in the Golden State to anticipate where the trail of ADMT compliance may lead.



Q&A: Building for trust in AI

Shane Wiggins
Director, Product Management
swiggins@onetrust.com
OneTrust

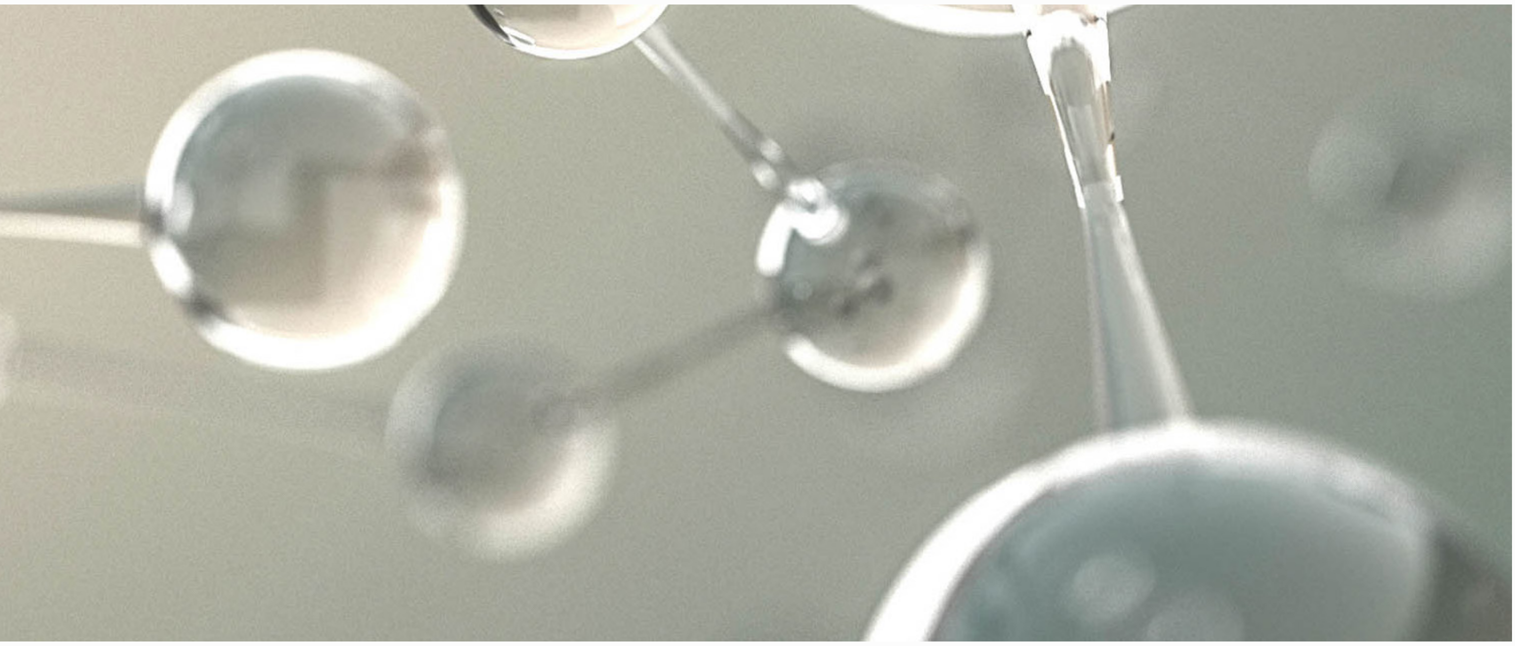
Shane Wiggins is a Director, Product Management and leads OneTrust's Responsible AI and Data Discovery products. Shane holds a Master of Science in Computational Data Analytics and serves on OneTrust's AI Governance Committee. In this article, Shane shares his thoughts and experiences on the developing AI regulatory landscape, its impact on organizations, and the frameworks and strategies they are adopting in building trustworthy AI.

How will the EU AI Act change the way businesses look at developing and implementing AI?

Success and scaling of AI projects require leaders to address strategies and methods related to fairness, transparency, explainability, reliability, privacy, and security. Businesses are increasingly recognizing the importance of adopting a holistic approach to AI use, development, and deployment. This involves collaboration with various stakeholders, such as those responsible for privacy, ethics, legal, and security. By involving these cross-functional teams, companies can ensure that their AI systems adhere to principles of responsible AI and meet regulatory requirements.

Extending on delivering the principles of responsible AI, transparency in model development is becoming essential. Companies are expected to provide clear explanations of how their algorithms are programmed and thoroughly evaluate the datasets used to train, refine, and augment AI models. Additionally, businesses must clearly indicate when customers are interacting with AI systems and provide mechanisms for users to control the use of these technologies. These transparency measures are crucial for establishing trust, ensuring accountability, and enabling explainability in AI systems, aligning with the pillars of regulatory frameworks.

Furthermore, businesses are advised to carefully assess whether AI is truly necessary to address specific use cases, avoiding unnecessary implementation and potential risks. By implementing responsible AI practices, companies can build



trust not only with regulators but with customers and society at large and position their business for success in the AI-driven future.

What are the key issues that you are seeing arise for companies targeting compliance with the EU AI Act?

There's the challenge of understanding where AI development and use is occurring within the organization. This necessitates comprehensive knowledge of all areas where AI is throughout the business. 'Shadow AI' is a term describing unsanctioned or ad-hoc use of AI, commonly generative, within an organization that's outside IT governance. The rate of advancement in the technology and the lowered barriers to access compound this challenge.

Secondly, there's a need to clarify roles concerning AI systems, whether a company is acting as a provider, deployer, importer, distributor, or affected party. This becomes particularly complex with the increasing availability of democratized third-party generative AI capabilities, which can be easily integrated into existing products and services which are then promoted downstream. Organizations will need to do a review of their uses of AI to determine if they are in scope of the AI Act and if so whether they qualify as a provider or a deployer.

Lastly, optimizing the review process for conducting risk evaluations of AI systems is crucial. This involves streamlining procedures to efficiently assess the potential risks associated with AI, ensuring compliance with the requirements set forth by the EU AI Act, while ensuring the adoption of AI is not hindered. Each level of risk has an associated obligation that must be carried out. Understanding what these levels are and where they exist in your organization will help ensure you meet those obligations and protect against high and unacceptable risk. AI continues to provide unprecedented opportunities to businesses and it's important to build processes to enable that innovation.

Where do you see opportunity for organizations to build efficiencies across the various programs and stakeholders that may already be established?

One of the primary hurdles in the realm of AI governance lies in bridging the gap between the data science team and the business. This challenge is addressed through the integration of Machine Learning Operations (MLOps) tools like Azure Machine Learning, Amazon SageMaker, Google Vertex, or MLflow, facilitating traceability and audits during the development lifecycle of AI. Integrations with these tools and risk and compliance software streamline processes for technical stakeholders, ensuring seamless operation within their daily tooling environments, saving time, and ultimately minimizing the friction. This integration is essential as the technical teams often develop and deploy models without oversight from compliance and risk management, necessitating readily available model information for governance standards adherence.

Where do you see technology playing a role in managing and mitigating risk, as well as building trust?

Monitoring and observability are essential, particularly in the realm of AI where probabilistic systems introduce randomness and uncertainty. This involves continuously tracking system behavior to identify potential deviations from intended use and scope. Beyond ongoing monitoring once deployed, data discovery and governance tools assist in risk mitigation by labeling data for sensitivity and identifying key data quality characteristics, which helps prevent unfair or discriminatory outcomes by addressing biases within the data during the training process. Data classification can also be leveraged at the model input layer to prevent sensitive data exposure and prompt injections during interactions with the AI. Additionally, technology enables the generation of artifacts like model or system cards, providing stakeholders with transparent insights into how the AI system was developed and the system's decision-making processes. Ensuring thorough documentation when building AI systems (playing offense) helps end users of those AI systems adopt the technology quicker given trust in the technology (playing defense). Technology will continue to play a pivotal role in helping to establish increased transparency and accountability.

Is there a model that is emerging for what a strong AI governance program looks like?

To effectively govern AI and mitigate the risks to different populations, organizations must establish diverse AI governance committees to establish policies, define risk levels and organizational risk posture, evaluate use cases, and ensure human involvement for high-risk processes. AI governance committees are a growing trend driven not just by regulatory scrutiny and risk prevention, but also the need to reinforce trust with stakeholders that an organization is adopting AI responsibly. It involves establishing a diverse team with representatives from key functional areas like Legal, Ethics & Compliance, Privacy, Information Security, Product Management, and Engineering. This committee leverages cross-functional knowledge sharing to address AI governance challenges holistically. A shift left mentality ensures that responsible AI principles are ingrained from the outset, oftentimes led by technical stakeholders such as product managers, data scientists, and engineers.

How do you see the regulatory landscape evolving, particularly with respect to the benefits that other standards and frameworks may bring such as ISO 42001?

Proposed AI regulation and guidance adhere to OECD-defined core principles, focusing on human rights, sustainability, transparency, and effective risk management, supported by the G20. Adopting a risk-based approach, these jurisdictions tailor regulations to AI-related risks such as privacy, non-discrimination, transparency, and security, with compliance obligations scaled according to risk levels. Recognizing the diverse applications of AI, they advocate for both sector-agnostic and sector-specific rules to address varying needs across industries. Actions addressing sensitive areas such as healthcare, financial services (lending, insurance, housing), work force practices (discrimination), and child safety are more likely. The challenge will continue to be getting the balance right between innovation and societal risk.

What are your top priorities for the year ahead in continuing to build products and services to support customers in their AI journeys?

We're dedicated to not just enabling but accelerating the AI journey for businesses. One of our key strategies involves streamlining the often intricate and time-consuming AI review process, making it not only efficient but also empowering businesses to leverage AI's full potential while minimizing operational burdens. Furthermore, we're committed to establishing a standard framework for evaluating AI use cases against responsible AI principles. By providing clear guidelines and benchmarks, we ensure that businesses have a consistent and structured approach to assess the risk and potential impact of AI initiatives. This standardization not only fosters clarity but also enhances collaboration and decision-making, ultimately leading to more successful AI implementations. Recognizing the critical importance of regulatory compliance in the AI landscape, we're taking proactive steps to embed regulatory intelligence directly into our products. This means that our customers can navigate the ever-evolving regulatory landscape with confidence, knowing that they have access to up-to-date information and guidance at their fingertips. By staying ahead of regulatory requirements, we empower businesses to innovate responsibly, mitigating risks and ensuring ethical AI practices. Finally, we're living in a world driven increasingly by data. We are continuing to invest in capabilities to ensure enterprises can protect personal and sensitive data in the next wave of AI, complying with data privacy and security regulations around the world.

5 minutes with...

Timothy Dickens

Timothy Dickens
Partner
tjldickens@draju.com
DR & AJU LLC, Seoul

Tell us a bit about your job role and how you have progressed in your career?

I am currently a Partner at DR&AJU LLC based in Seoul, South Korea. I have been with the firm for 11 years and head up our firm's Data Protection and Africa teams. I started out my career in South Africa with a firm called Lovius Block, based in Bloemfontein which is the judicial capital in South Africa. I was focused on commercial transactions and litigious matters. I then decided that I wanted more international exposure and made the move to London to do my cross-qualification for the UK bar. I was fortunate enough to work with Linklaters and was part of their disputes team which, at the time, was handling the News of the World group litigation matter. With the signing of the EU-Korea FTA, the legal market in Korea was opened for foreign firms and with this development there was also a need for foreign qualified lawyers in the local Korean law firms. I had a couple of friends who were Korean and they suggested coming over and working in Seoul. I made the move over and the rest, so to say, is history.

As far as my data privacy practice is concerned, I never imagined that I would be advising on tech-related type matters, especially considering that I did not have much interest in this field as when I started practicing, we were still using dictation for letters and submissions and emails were still not the preferred choice for sending correspondences. However, due to a large number of our international clients seeking advice on data privacy compliance, the data practice grew organically and I decided to focus and dedicate a niche team within our firm to this practice area. It has flourished and with it my interest and enjoyment in all data-related matters which spilled over into IT/tech related matters. It was further fueled by Korea having quite rigorous data privacy laws and being a country where tech and IT matters are very relevant and important parts of the economy. It has been an interesting professional progression and I have been very blessed to have worked in great firms across three different countries.

What alternative job would you have if you had not gone into law? That's easy, a sports agent. I remember watching Jerry Maguire when it came out in 1996. I was in high school at the time and thought that it was a very appealing job as I am sports mad and wanted to be involved in sports in some way or another. I figured that to be a sports agent I would need business marketing and management qualifications to be able to manage and market sports stars while at the same time needing a legal background to be able to draft and negotiate contracts. I then decided to study a Bachelor of Commerce degree with marketing management as my major and LLB to get my legal knowledge. In the end, the law and being a lawyer became more appealing and I could still advise on sports matters, and in fact did a number of sports-related contracts and disputes, so I was fortunate enough to get the best of both worlds.

What do you love about your job and what do you find challenging?

I love meeting and being introduced to so many new people from such a variety of industries and sectors. I find it so interesting that there is literally a blue ocean of sectors/industries and companies out there of which we have no idea until being introduced to them. This means that every matter has a uniqueness to it as we need to learn andunderstand the company and their specific operation and how this would be relevant to the issues at hand, whether it's for compliance or whether we are looking at commercial issues. One of the most challenging parts is that it is never constant and that there are always changes in legislation and decrees and regulations so one has to constantly be aware of staying abreast of developments and how these may possibly impact your client and their business. In addition, often for multinational companies it's hard to make specific exceptions for particular jurisdictions to ensure the continuity of the companies' systems and programs, so often it is more about risk mitigation and taking business risks on certain issues. The challenge is to find the sweet spot between practicality and legality.

Where is your favorite place on earth?

I have a very soft spot for Africa and in particular Zimbabwe at the Victoria Falls Kariba Dam and the Hwange National Park. The pure magic of being in the wild and being part of nature is something one cannot describe unless you have been there.

Who would play you in a film about your life?

I have been told I look like Hank Azaria... so I would guess him. Personally though, I would like Colin Firth to play me.

What is your favorite book?

Lord of the Rings - Tolkien was born in Bloemfontein of all places which is my hometown originally.

What is some advice you would give to others starting off in your industry?

As a young lawyer I would advise the following:

1. Build your knowledge across a number of sectors when you are young. Expose yourself to commercial, criminal, labor, dispute matters, etc. Get a solid understanding of a number of areas of law before starting to specialize. When we are faced with legal matters, inevitably there is always a crossover of a number of legal issues and practice areas, so you will be able to better understand how all the pieces fit together and have an impact on one another. A solid base is the foundation on which to build your specialty.
2. Build your network from a young age. Growing up, I never would have imagined that a lawyer would need to cover business development, but it is a massive part of our work too. Like all things in life, the market is super competitive and we need to rely on our relationships, networks, and contacts to build our practice and best serve our clients. The bigger and better your network, the more chance you have of building your practice and ensuring the best advice and assistance for your clients. As the old adage goes, it's not what you know but often who you know!

Who is your inspiration?

My wife - she is my absolute rock and the person who I respect and admire the most. Especially with the birth of our daughter recently, she inspires me to be the best dad and husband that I can be. I truly am blessed in this respect.

onetrust
DataGuidance

Data Protection Leader is published bi-monthly by OneTrust Technology
Limited, Dixon House, 1 Lloyd's Avenue, EC3N 3DS, London, United Kingdom

Website: www.dataguidance.com
Email: DPL@onetrust.com