EVERSHEDS SUTHERLAND

Managing your workforce in 2024 and beyond

Legal principles and policy considerations in the US and the rest of the world

Wednesday, November 15, 2023

Sophie White
Partner, UK – Eversheds Sutherland

Laura Taylor
Counsel, US – Eversheds Sutherland

ACC Association of Corporate Counsel
CHICAGO

The global remote working landscape

Why is it a hot topic?

Impact of the COVID-19 Pandemic

Benefits for employees and employers

Defining new remote working arrangements

Remote working models

Common scenarios

Employee based in one country/state working at a place other than their main office in that country/state

Employee working remotely from another country or State (permanently or temporarily) to their main office

Employee who is location-independent and uses technology to perform their job from anywhere in the world (Digital Nomads)

Remote working considerations

- Employment and benefits
- Immigration
- Tax
- Protecting legitimate interests

Employment and benefits

Remote work considerations

US

- Be aware of minimum wage requirements and salary thresholds for exempt employees
  - Exempt employee salary thresholds are governed by both federal and state laws
- Be aware of local paid sick leave laws
- Be aware of treatment for vacation time
  - Whether state or local law permits use-it-or-lose-it
  - Whether state or local law requires pay out of accrued vacation time upon termination
- Be aware of remote work expenses that need to be reimbursed
  - During the pandemic, employees had to work remotely, so many costs became reimbursable expenses (for example, internet, cell phone, paper/ink for printer, etc.)
  - Generally, where remote work is an option, the employer need not reimburse expenses other than items used solely/predominantly for the benefit of the employer

Remote work considerations

US

- Be aware of any local family and medical leave laws that require employee or employee and employer contributions
  - Leave laws tend to provide time off due to certain conditions or circumstances, others provide for pay or partial pay during an approved unpaid leave (such as during FMLA leave)
  - Some localities have an employee work-hour requirement or number of employee-threshold for participation
  - Many new laws: CA, CO, CT, DC, DE, HI, ME, MA, MN, NH, NJ, NY, OR, RI, VT, WA, WI
- Required work posters should be transmitted electronically to comply with posting requirements. Refer to requirements in applicable states or under applicable federal laws.

Remote work considerations

US

Remote Work Policies:

- Employees should maintain a safe working environment at their remote location
  - Workers' compensation likely covers them while they work remotely, so employees may be required to allow safety inspection and/or give statement/assurances that the work location is safe (no toys, pets, items to trip on)
  - Ergonomic equipment may be needed at home if also used at the office
- Timekeeping requirements
  - Non-exempt employees should continue tracking and recording all time worked. If supervisor approval is needed before overtime can be worked, that should continue to be the policy for remote work.
  - Exempt employees need not track work time
  - Employees must still call in when sick or using sick time for doctor appointments
  - Employees must still request vacation time in the same manner as when working in the office

Employment law considerations

Cross-border arrangements - Rest of world

- Applicable law
- Contractual requirements
- Providing a safe place of work
- Pay and benefits, including expenses
- Changing/terminating the arrangement

Top tips

- Know where your employees are
- Be clear on applicable law and any regulatory requirements
- Future-proof contracts and policies
- Have a mechanism for assessing H&S
- Don’t forget benefits

Applicable law
Cross-border arrangements - Rest of world

Rome Convention/Rome I (593/2008/EC)(pre/post 7 Dec 2009) – in the UK applicable as retained EU law post-Brexit (UK-Rome I) under the European Union (Withdrawal) Act 2018 :

- choice of law - but: not to deprive employee of protection by mandatory laws of "default" law
- if no choice ("default" law):
  - habitual place of work
  - if no habitual place of work: employer place of business
  - unless closer connection to other country
  - overriding mandatory provisions (public interest)

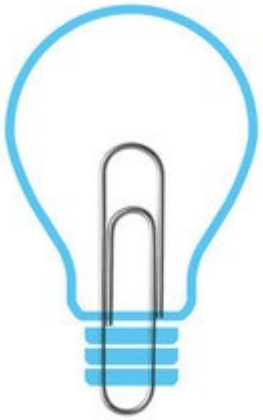
Outside the EEA and the UK: Other conflicts of law rules but typically choice of law in employment contracts restricted to protect the employee.

Benefits

Cross-border arrangements - Rest of world

- For retirement plans, it may not always be possible under home plan terms to continue to cover employees hired by local entity or third-party.
  - Home plan terms may not work for local compensation/employment situation, e.g., different compensation elements or payroll process; and
  - Coverage under local plan may create inequities among employees, tax issues for the covered employee

- For countries that provide employer-sponsored medical coverage (e.g., US), international coverage presents challenges.
- Coverage such as life insurance, disability, and travel accident may not be available for remote workers or employees in certain locations
- Locally-provided coverages may be duplicative or create disparities among employees internationally



Tax

Remote work considerations

US

If employer is doing business for the first time in a new location, be sure:

- To know appropriate withholding for local, state, and federal taxes
  - Employer withholding
  - Non-resident withholding
  - State employment taxes
  - State business taxes
- To know whether the location has additional requirements besides workers' compensation to protect employees:
  - For example, NY requires disability/liability insurance coverage in addition to workers' compensation

Tax considerations
Cross-border arrangements - Rest of world

Income Tax	Social Security	Permanent Establishment
➉will there be a liability in the host country/state ? ➉will tax still be payable in the home country/state ? ➉ ➉who is responsible for paying the tax ?	➉where will social security be payable ? ➉ who will be responsible for paying the social security ?	➉will the employee's presence create a permanent establishment in the host country ? ➉if so, what are the implications ?

Getting it wrong can have adverse implications

Top Tips

- Ensure you know what taxes are payable, where they are payable and by whom
- Make sure applications for exemptions are made in plenty of time
- If possible, design arrangements to avoid permanent establishments being created
- Put in place mechanisms to deal with tax implications e.g. engage a third party payroll provider in the host country or consider moving employment to a local group member or an employer of record to deal with withholding obligations

Immigration

Immigration considerations

Immigration considerations - US

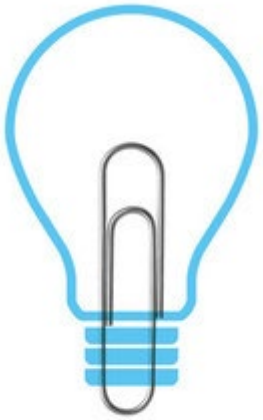
Key issues for consideration:

- Eligibility to work
  - I-9 (verification within first 3 days of hire)
  - E-Verify (required for government contractors and for private employers in certain states based on number of employees)
  - Tourist visas – answering emails, sitting in on meetings
- Overview of USA Immigration Laws
  - Employment Authorization
  - ESTA
  - Political Considerations
- Tax issues from US employment
  - US Source Income
  - Tax Resident Status

A geographically dispersed workforce
Immigration considerations

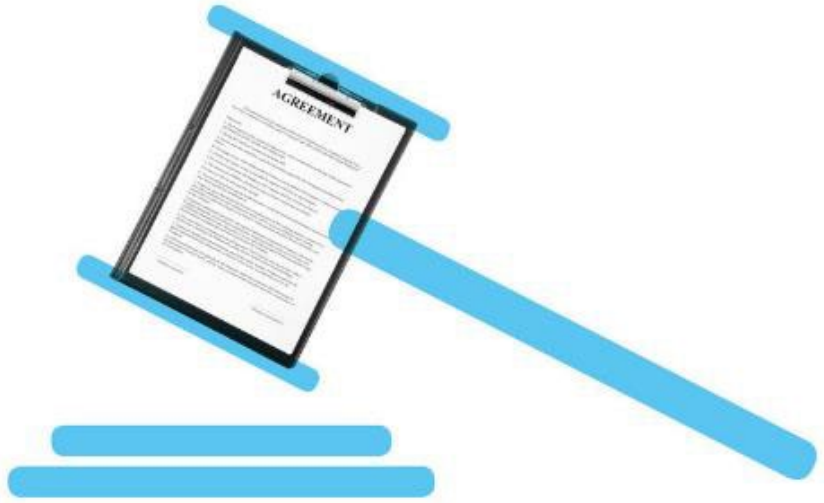
Key issues for consideration:

- Is the employee working or visiting?
- Do they have the an automatic right to work in that location (i.e. are they a national)?
- Is permission required? Digital nomad visa?
- Approach to regulated activities
- Is this is business led request or an employee led request?
- Can this be accommodated now or will it need to be reviewed in future?
- Nuanced local requirements: Consider employment, pensions, health & safety, social security and tax



Failure to obtain the correct permission

- Civil and/or criminal sanctions may be imposed on the individual and/or the employer
- Potential restrictions on both the employer and the individual
- Detention/deportation of the individual by the authorities – distress and inconvenience
- Operational impact, which may include future restrictions on the individual's travel elsewhere
- Reputational risk



For example, in **the Netherlands** failure to obtain a visa can result in:

- for the individual: a requirement to leave the country (in some cases, immediately); and
- for the employer: a fine of EUR 8,000 for each individual in breach (increased by 50-200% for repeat offences within 5 years)

Protecting legitimate interests

Protecting legitimate interests

Global considerations

- Risks and how they arise
- Intellectual property
- Restrictive covenants
- Physical assets

Solutions

What are the potential solutions for remote working?

Remote work considerations

US

Remote Work Policies and Agreements:

- Good to set expectations and boundaries, reserve rights to the employer to make changes as business necessitates
- General policies are appropriate where much of the workforce works a hybrid schedule
- Individual agreements are likely appropriate where an employee works remotely for all work time or nearly all worktime’
- Where employees are able to request remote work, be sure there is a non-discriminatory process in place for requests and approvals

Remote work considerations

US

Some key items to include in remote work policies:

- Employer should consider reserving the right to adjust the hybrid schedule as deemed necessary or desirable in the sole discretion of the employer
- Require that employees inform/receive approval from HR/supervisor if the employee will be working from a location other than their usual/home remote work location
  - Work from a foreign country may cause tax liabilities to the employer (and the employee) if employee works there long enough
  - Work from a foreign country without proper visa can be problematic
- Require protections for confidential information
  - Secure storage and working space at remote work location
  - Secure electronic connectivity
    - No public Wi-Fi; no public USB ports

Remote work considerations

US

Key items to include in remote work agreements:

- Reiterate that all job expectations remain the same whether working in the workplace or remotely
  - Employee must be available and working during business hours unless they have notified the employer otherwise (sick leave, vacation time, etc.)
- Employees continue to be bound by all workplace policies and procedures, including all remote work policies, notification requires for illness or injury (whether time off or workplace injury)
- Employer should consider reserving the right to adjust the hybrid schedule or revoke the remote work arrangement as deemed necessary or desirable in the sole discretion of the employer
- Reiterate at-will nature of employment
- Helpful to reiterate or expand on IT compliance, security, and protection of confidential information (which may include not allowing others – including family members – to use company laptop or other devices)

Remote work considerations

US

Key items to include in remote work agreements:

- May need to expressly state that only company IT can address any issues with company-issued technology, such as laptop and devices; employee may not hire or entrust devices to a third party.
  - Provide contact information for IT assistance
- Agreement to return, and perhaps an itemized list of any equipment provided for remote work (printers, docking stations, cameras, microphones, etc.)
- Reserving the right of the employer to monitor employee's work and productivity remotely
  - Company can use software that counts key strokes
  - Company should NOT activate laptop camera remotely

Approaches to remote working

Work anywhere policies

- Recruitment and retention
- Limitations to manage risk:
  - Countries
  - Time
  - Work authorisations

Individual assessments

- Time and cost implications
- Consistency

Global approach

- Must take account of local nuances, including in respect of recording / tracking working time
- Cybersecurity
- Maintaining culture and values

Approach to international working requests

3 options

Option 1

- **Reject all requests***
- Consistent and easy to apply
- Eliminates all immigration, tax, regulatory and other country employment law risk
- Avoids cyber security issues of working in another country
- Carries some employment law risk
- May be seen as unaccommodating by employees

Option 2

- **Allow request but for up to 30 (or 60) days only**
- Consistent and easy to apply
- Reduces tax, immigration and other country employment law risk
- May not eliminate cyber-security or regulatory risk
- May be regarded by employees as a reasonable benefit but won't work for everyone

Option 3

- **Accept request for maximum period requested**
  - Significant management and administration burden
  - High tax, regulatory, local employment law and cyber-security risk
  - Immigration risks if employee not a national of the country in which working and difficulty returning to the UK
  - Employee friendly

*It may be possible to accommodate such requests in some countries in which the employer operates without giving rise to tax, immigration and regulatory issues

The global approach

	Option 1 – reject all requests	Option 2 – allow request but for up to 30 (or 60) days only	Option 3 – Accept request for maximum period requested
Practicality	Consistent and easy to apply but may be seen as unaccommodating by employees, and employers must take into account any obligations relating to flexible working	Consistent and easy to apply	Significant management and administration burden
Employment law	No change to applicable employment law	Remains likely that home employment law will continue to apply, with small risk that local host laws will apply	Significant risk that other country's laws will apply
Immigration	No immigration issues to consider	Most jurisdictions will allow short periods of working for non-nationals. No immigration law implication if employee is a national of the host country	No immigration law implications if the employee is a national of host country but immigration law implications if not
Tax	No tax issues to consider	Short periods of overseas working carry less risk of triggering tax implications for employee and employer	Likely tax implications for employee and employer

Questions?

EVERSHEDS SUTHERLAND

Sophie White
Partner, Eversheds Sutherland
United Kingdom
+44 20 7919 0717
sophiewhite@eversheds-sutherland.com

Laura Taylor
Counsel, Eversheds Sutherland
United States
+1 202 383 0892
ltaylor@eversheds-sutherland.com

eversheds-sutherland.com

MAN_002-#11352348

EVERSHEDS SUTHERLAND

Emerging class action risks from state legislation

November 15, 2023

Frank Nolan
Partner, Litigation – Eversheds Sutherland

ACC Association of Corporate Counsel CHICAGO

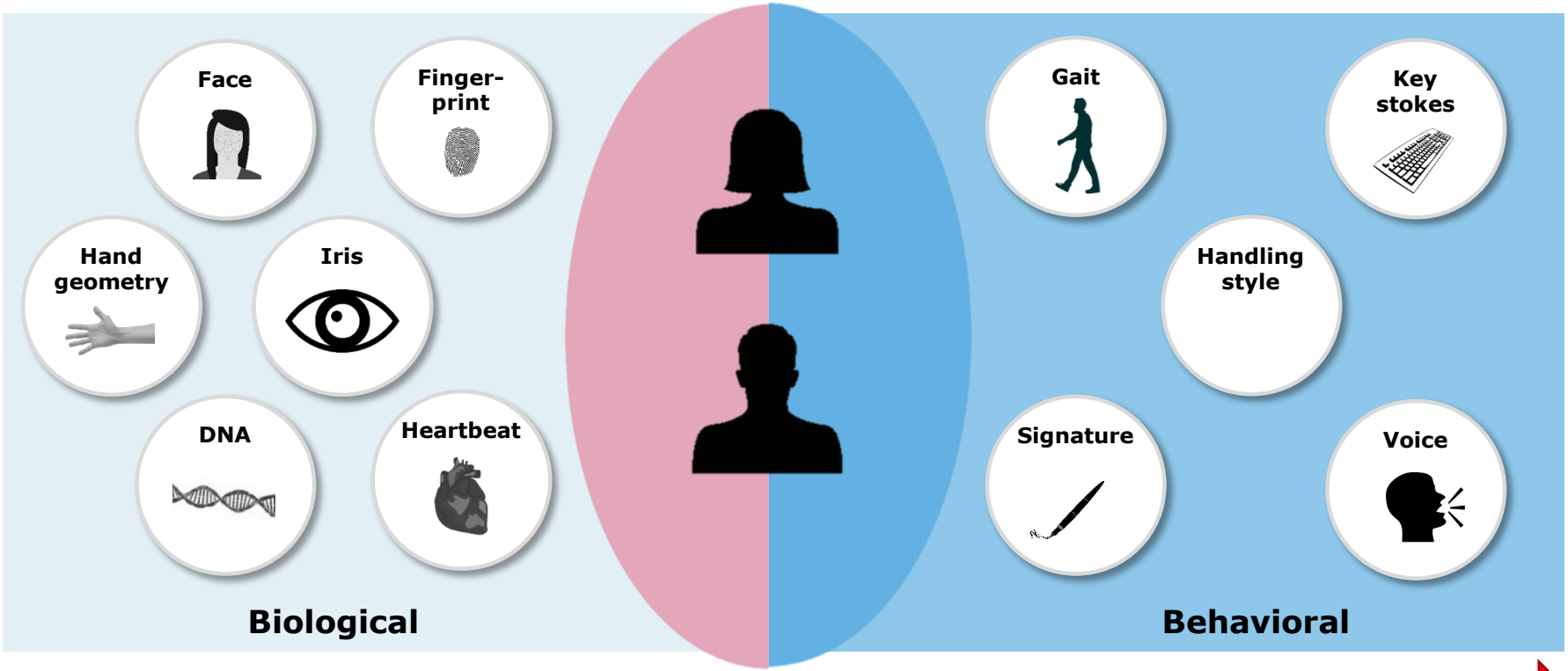
Agenda

1. Illinois Biometric Information Privacy Act (BIPA)
2. Illinois Genetic Information Privacy Act (GIPA)
3. “Mini-TCPAs”

Evaluating the BIPA landscape

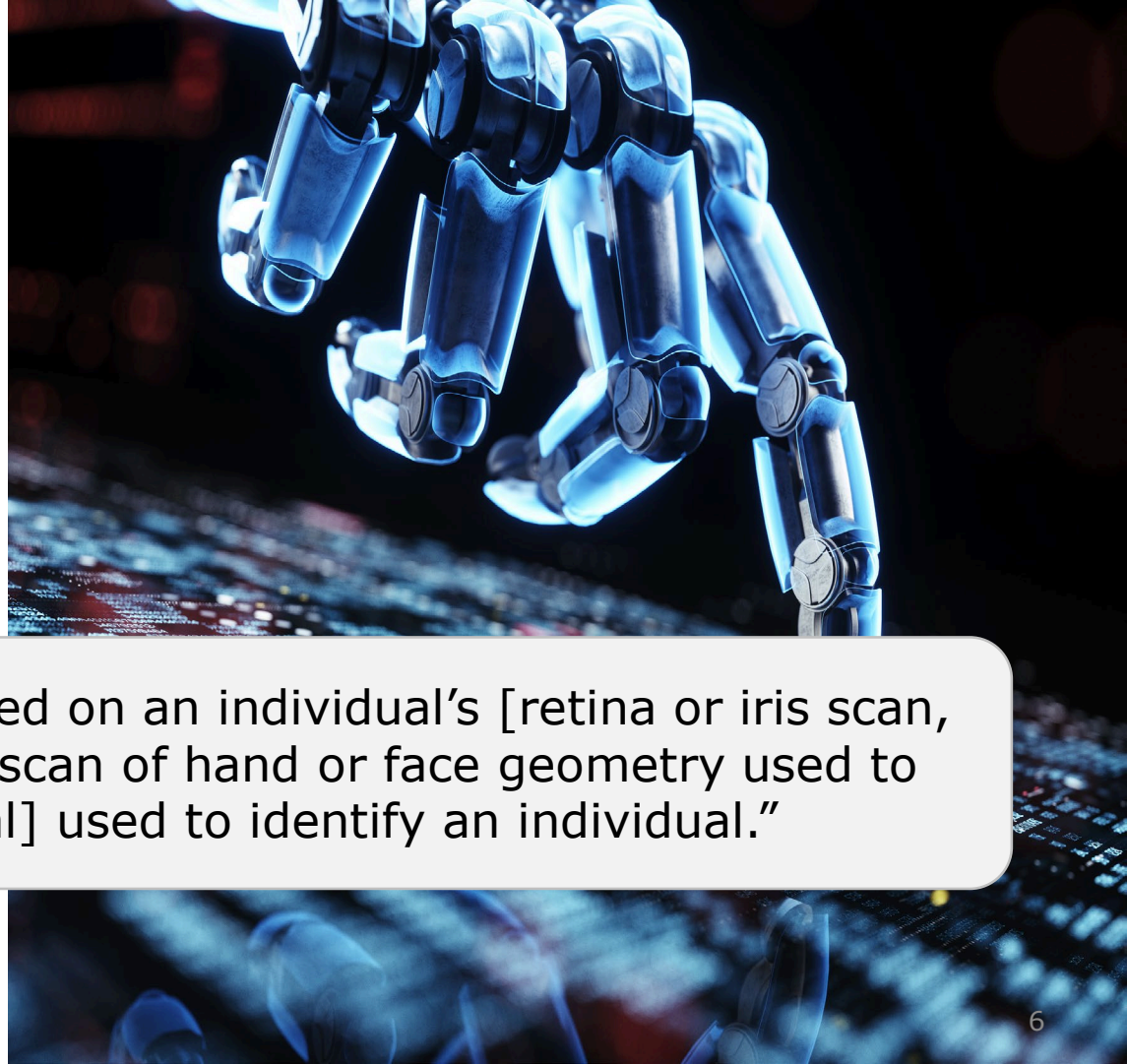
Where do we stand?

Biometrics: The features that make you unique



Illinois Biometric Information Privacy Act (BIPA)

What is "Biometric Information" under BIPA?



"[A]ny information . . . based on an individual's [retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry used to identify an individual] used to identify an individual."

BIPA: History

Concern by lawmakers over use and implementation in the workplace

Enacted in 2008 and requires:

Written consent

Limited disclosure

Prohibition on sale

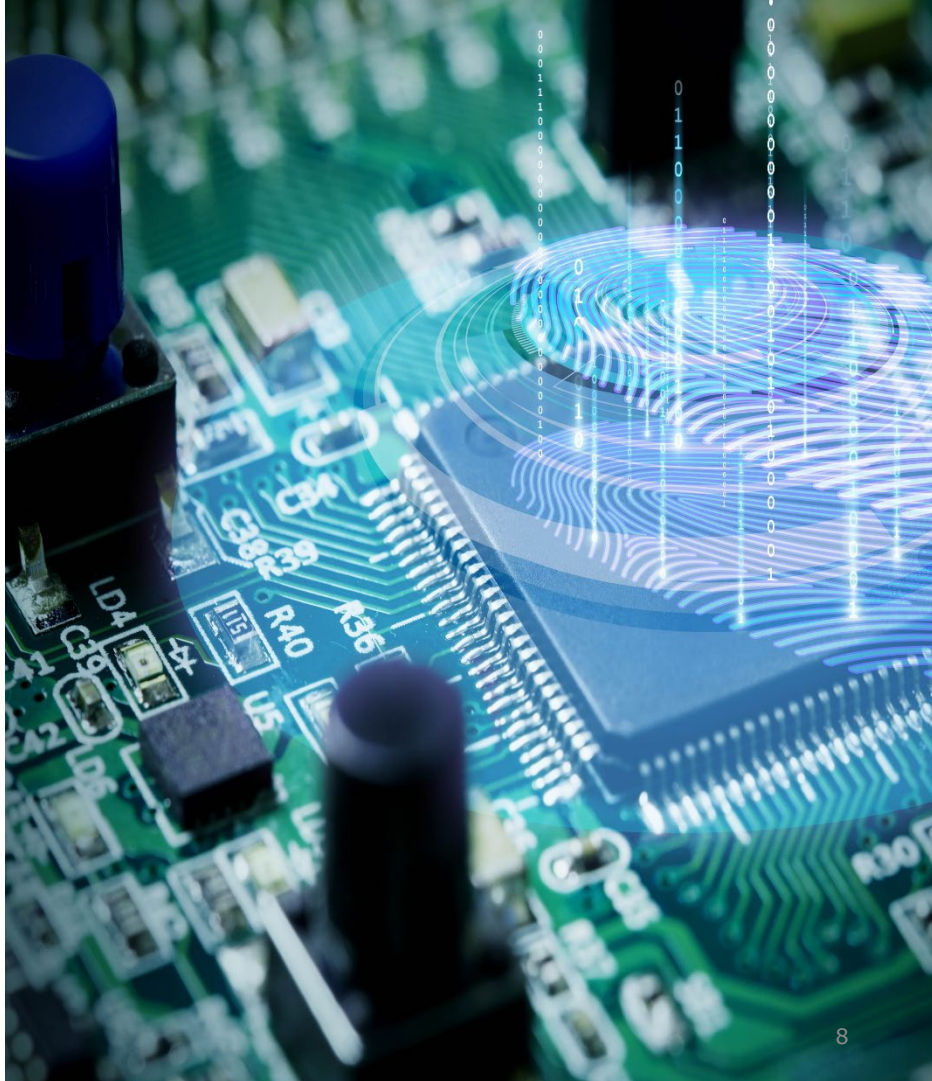
Publication of policies

Security and limited retention periods

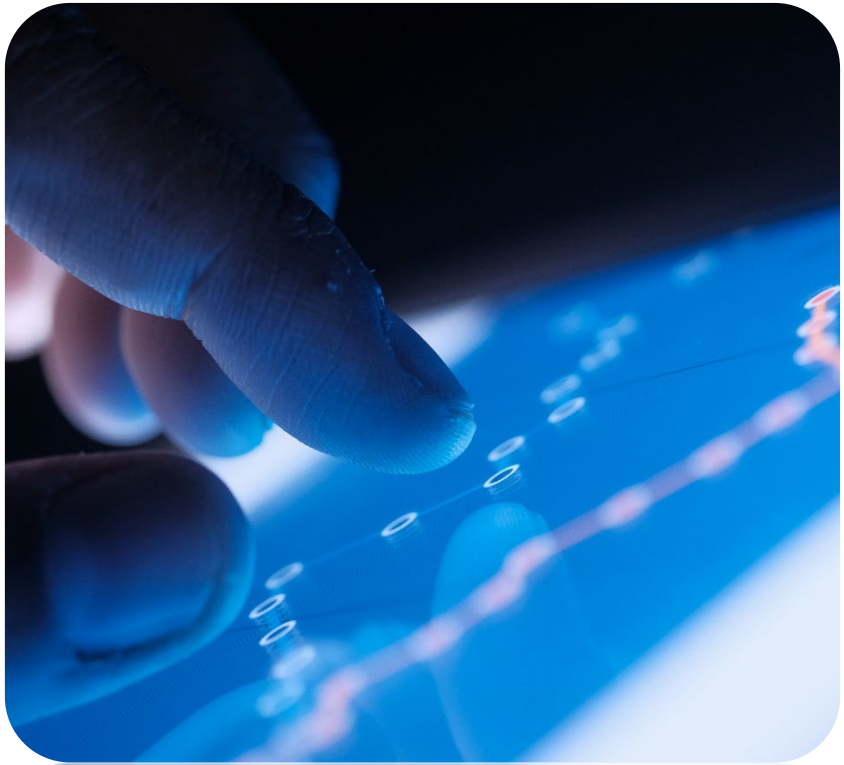
Spike in class actions filed since 2015

BIPA: Private Right of Action

- Negligent violation:
  - $1,000 for each violation; or
  - Actual damages, whichever is greater
- Intentional or reckless violation:
  - $5,000 for each violation; or
  - Actual damages, whichever is greater
- Reasonable attorneys' fees
- Other relief, including an injunction



BIPA: Exemptions



- Government actors
- Financial institutions subject to the privacy notice provisions of the Gramm-Leach-Bliley Act of 1999 (GLBA)

BIPA: Significant decisions

- *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186
  - BIPA: Right of action to "any person aggrieved by a violation"
  - A plaintiff need not have suffered actual damages to bring a BIPA claim
- *Tims v. Black Horse Carriers, Inc.*, 2023 IL 127801
  - Statute of limitations for BIPA claims is five years
- *Cothron v. White Castle Sys., Inc.*, 2023 IL 128004
  - Each violation of BIPA is a separate claim, allowing multiple accruals

Illinois Genetic Information Privacy Act (GIPA)

Illinois Genetic Information Privacy Act (GIPA)

-Encourage voluntary and confidential genetic testing
-Originally enacted in 1998
-Ignored for over 20 years

GIPA: Prohibitions

Involuntary Disclosure by any person

Requests/Use by employers

Underwriting Use by insurers

GIPA: What does it cover?

- Genetic information
- Borrows definition from HIPAA
- Includes
  - an individual's genetic tests
  - an individual's family members' genetic tests
  - **the manifestation of a disease or disorder in an individual or his family members**
  - any request for or receipt of genetic services

GIPA: Private right of action

- Negligent violation:
  - $2,500 for each violation
  - Actual damages, whichever is greater
- Intentional or reckless violation:
  - $15,000 for each violation
  - Actual damages, whichever is greater
- Reasonable attorneys' fees
- Other relief, including an injunction

GIPA: A new tool for plaintiffs’ attorneys?

GIPA: What plaintiffs' attorneys see

Bridges: extends *Rosenbach* to GIPA: "Any person aggrieved by a violation"; procedural violation enough

Private right of action

Statutory damages (triple BIPA's damages)

Broader range of potential defendants (no BIPA exemptions)

GIPA: *Bridges* aftermath and race to the courthouse

- From 1998 to 2002, two cases filed
- From January 2023 until *Bridges* (July), six cases
- From *Bridges* until today, more than forty cases

GIPA: Who are the targets?

Employers	Insurers
• Tyson Foods • Ford • Amazon • FedEx • Caterpillar • Chicago Transit Authority • Union Pacific Railroad • Illinois State Police	• State Farm Life • Pacific Life • AIG • Northwestern Mutual

GIPA: Theories of liability

Employers: Pre-employment physicals with inquiries into family medical histories and/or genetic predisposition to certain diseases

Insurers: Pre-underwriting physical with inquiries into family medical histories and/or genetic predisposition to certain diseases

What’s next for GIPA litigation?

GIPA: Open questions

- Will courts agree that “family medical history” is “genetic information” under GIPA?
- Will they be persuaded by other arguments?
- Will the Illinois legislature clarify the law?
- What is the statute of limitations?

GIPA: Does "genetic information" mean "family medical history?"

- One major retailer is arguing "no" in a motion to dismiss, citing federal GINA case law
- But: *EEOC v. Dolgencorp, LLC*, (N.D. Ala. July 26, 2022)
  - Asking job candidates "Have your grandparents, parents, or children had significant medical problems?" violated GINA
- May depend on specificity of allegations

GIPA: Other arguments and developments

- Must also show discrimination?
- The language of the section applying to insurers is inconsistent
- Statute of limitations?
- Illinois legislative developments

TCPA and state “mini-TCPAs”

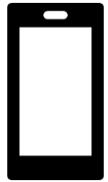
Telephone Consumer Protection Act (TCPA)

- Enacted in 1991
- Regulates telemarketing
  - Automatic dialing systems
  - Prerecorded voice messages
  - Text messages
  - Faxes

Autodialers

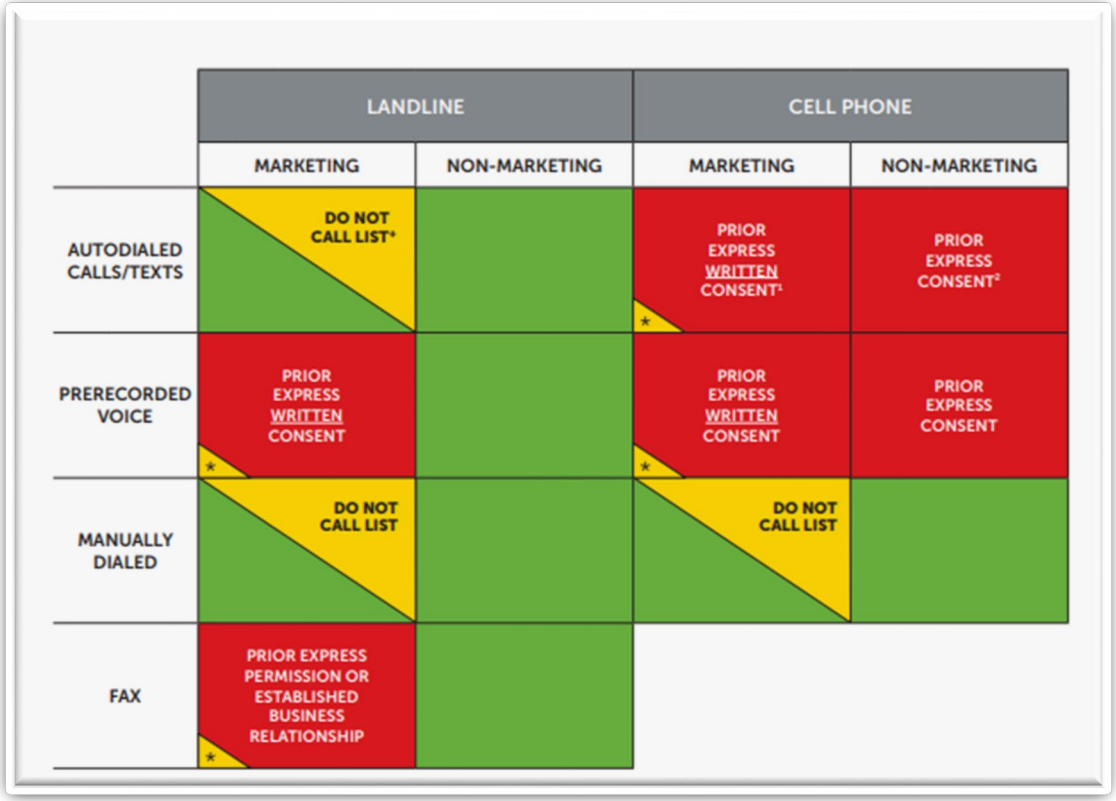
Faxes

Telemarketing



Texts

Eversheds Sutherland's TCPA traffic light

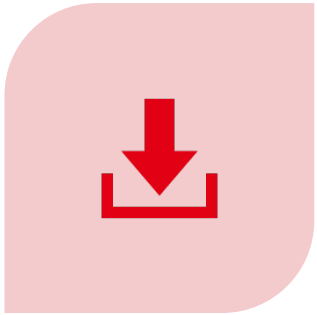


“Do Not Call” (DNC) restrictions/requirements

- Applies to telemarketing
- Restrictions are separate from (**and in addition to**) autodialer rules
- Statutory damages of $500 per violation
  - Each call is a $500 violation, even though consumers cannot sue for <2 calls
- Federal, state, company-specific DNC lists
- Exemptions if (1) consent, and (2) calls based on an “Established Business Relationship” (EBR)

National DNC registry (for telemarketing)

TELEMARKETERS MUST REGISTER AND SCRUB CALL LISTS UPDATED WITHIN PAST 31 DAYS

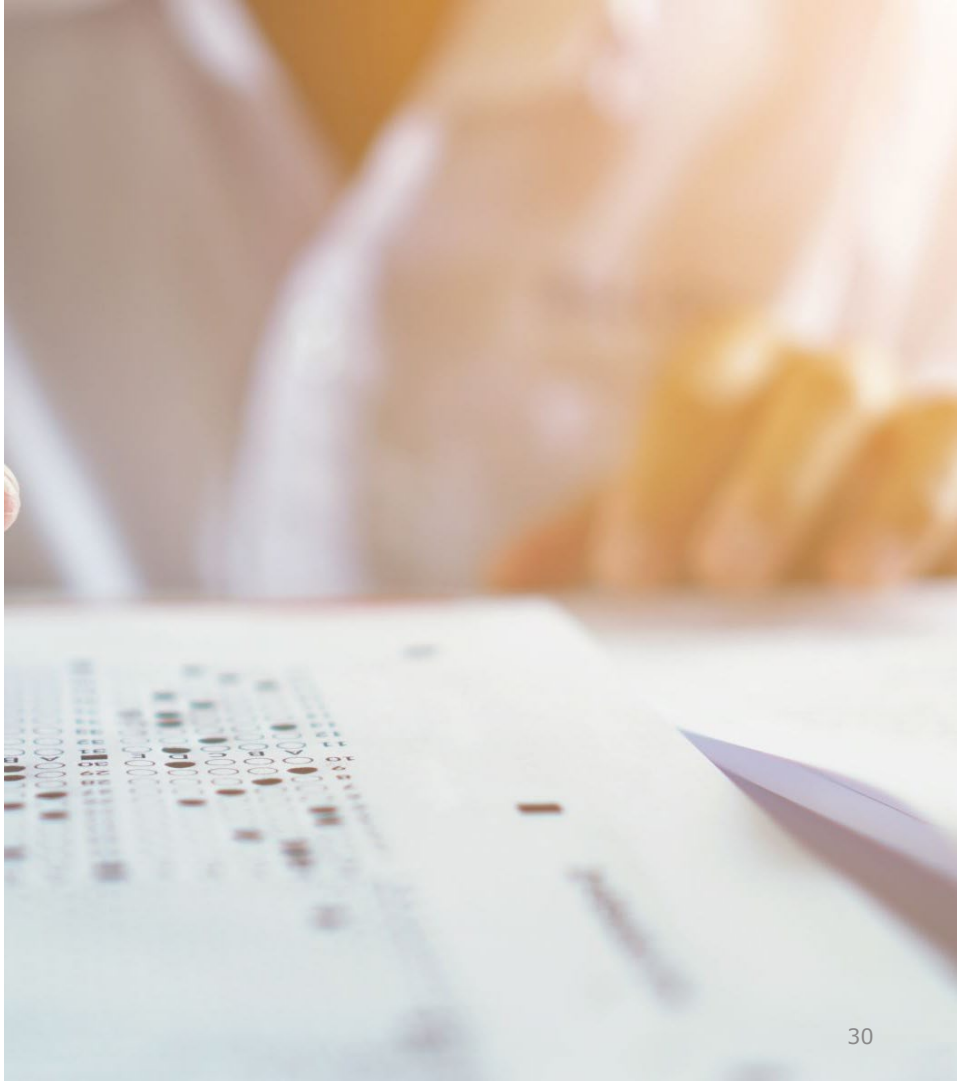


COMPANIES CAN DOWNLOAD THE LIST ONCE EVERY 24 HOURS. THIS IS TO PROTECT SYSTEM INTEGRITY

SEVERAL STATES HAVE STATE-SPECIFIC LISTS (MOST STATE LAWS RELY ON FEDERAL DNC LIST)

DNC list exemptions

- Prior written consent
- Established Business Relationship (EBR)
  - Three months for inquiries (prospective customers)
  - 18 months for past transactions (former customers/current customers)
- Calls by or on behalf of tax-exempt non-profit organizations
- Calls that are not commercial or do not include unsolicited advertisements



State "mini-TCPAs"

❖ **Arizona**	No single call/text safe harbor
❖ **California**	No single call/text safe harbor; no private COA
❖ **Connecticut**	No single call/text safe harbor
❖ **Florida**	Recent amendments to stop flow of class actions
❖ **Maryland**	Expanded auto-dialer definition
❖ **Oklahoma**	Expanded auto-dialer definition
❖ **Rhode Island**	No single call/text safe harbor; no
❖ **Virginia**	Single "solicitation" can trigger
❖ **Washington**	Applies broadly to advertising

Questions?

EVERSHEDS SUTHERLAND

Frank Nolan
Partner, Litigation
(212) 389-5083
franknolan@eversheds-sutherland.com

The Grace Building, 40th Floor
1114 Avenue of the Americas
New York, New York 10036

eversheds-sutherland.com

EVERSHEDS SUTHERLAND

Navigating the AI landscape: Balancing innovation with compliance

November 15, 2023

Dennis Garcia
Assistant General Counsel, Microsoft

Stephen Hopkins
Partner, UK – Eversheds Sutherland

Simon Lightman
Partner, UK – Eversheds Sutherland

Mary Jane Wilson-Bilik
Partner, US – Eversheds Sutherland

ACC Association of Corporate Counsel
CHICAGO

This informative video was
presented during the panel discussion.
Please click **here** to view.

EVERSHEDS SUTHERLAND

The highly-anticipated US Executive Order on artificial intelligence: Setting the agenda for responsible AI innovation

November 10, 2023

On October 30, 2023, the Biden Administration issued the groundbreaking Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence[1] (Order), which sets in motion a comprehensive US strategy for the responsible development and use of artificial intelligence (AI).

The Order goes beyond prior Administration actions on AI in numerous respects. The broad ranging and robust Order directs US executive departments and agencies (agencies) (and encourages independent agencies) to develop standards, frameworks, guidelines, and best practices in anticipation of using their existing authorities to regulate AI. Agencies must take specific steps on virtually every federal law, regulation, and policy that bears on the responsible use of AI.

While recognizing the benefits that can be derived from the use of AI, the Order highlights the numerous known risks associated with AI's potential misuse, ranging from damage to national security, critical infrastructure and privacy to fraud, discrimination and bias to disinformation, and concern over workforce displacement and the stifling of competition.

The Order places urgency on advancing a set of principles, standards, and priorities designed to strike a balance between the need to encourage innovation and the need to build effective guardrails to protect against societal harms and ensure the safe and secure development and use of AI.

Perhaps the most important element of the Order in the short term is the requirement that the Commerce Department put in place by January 29, 2024 (i.e., within 90 days of the October 30, 2023 Order), binding reporting requirements for private sector developers of the most powerful AI models to report to Commerce the results of the model's performance in AI red-team testing.[2] Commerce also must issue proposed regulations on certain transactions with foreign persons with respect to AI

Contacts

- If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed or the Eversheds Sutherland attorney with whom you regularly work.

Mary Jane Wilson-Bilik
Partner
mjwilson-bilik@eversheds-sutherland.com
+1.202.383.0660

Michael Bahar
Partner
michaelbahar@eversheds-sutherland.com
+1.202.383.0882

Jeffrey P. Bialos
Partner
jeffbialos@eversheds-sutherland.com
+1.202.383.0363

Patrick Gilman
Partner
patrickgilman@eversheds-sutherland.com
+1.202.383.0195

Rachel M. Reid
Partner
rachelreid@eversheds-sutherland.com
+1.404.853.8134

Atiana J. Johnson
Associate
AtianaJohnson@eversheds-sutherland.com
+1.202.383.0315

Related People/Contributors

- Mary Jane Wilson-Bilik
- Michael Bahar
- Jeffrey P. Bialos
- Patrick Gilman
- Rachel M. Reid
- Atiana J. Johnson

models that have potential capabilities that could be used in malicious cyber-enabled activity.

Significantly, one of the core principles of the Order recognizes that AI is a global technology and that there is a strong need to develop, with international allies, a framework to both manage AI's risks and unleash its benefits. In effect, the US is taking a leadership role by pioneering its own initial standards and safeguards while engaging with other countries in efforts to structure a more global framework over time. Whether traction can be reached on a more global approach remains to be seen. By adopting certain domestic rules and standards now, the US is seeking to encourage and give shape to global AI rules while assuming some risk that certain parties in the AI ecosystem will seek to move their activities offshore in order to avoid the reach of US AI governance.

Ensuring Safe and Reliable AI: Dual-Use Foundation Models. One of the most notable, and binding, components of the Order is the imposition of reporting requirements on private companies developing "dual-use foundation models," which the Order generally defines as powerful, self-supervising AI trained on broad data with the capacity to perform tasks that pose serious risks to US national defense and critical infrastructure.[3] (Sec. 3(k))

More specifically, under the Order, by January 29, 2024, the Commerce Department must require companies that develop or intend to develop dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records, regarding the following:

1. ongoing or planned activities related to training, developing, or producing such dual-use foundation models, including the physical and cyber security protections taken to assure the integrity of such training against sophisticated threats;

2. the ownership and possession of the model weights of such dual-use foundation models, and physical and cyber security

measures taken to protect those model weights; and

3. the results of any such model's performance in relevant AI red-team testing based on guidance developed by NIST and prior to the development of such NIST guidance, the results of any red-team testing that the company has conducted relating to certain types of specified risks (e.g., lowering the barriers to entry for development, acquisition, and use of biological weapons by non-state actors; the discovery of software vulnerabilities; use of software or tools to influence real or virtual events; the possibility for self-replication or propagation; and associated measures to meet safety objectives). (Sec. 4.2(a))

Commerce also must require reporting by companies, individuals, or other organizations or entities with respect to the acquisition, development, or possession of a potential large-scale "computing cluster," including the existence and location of such clusters and the amount of computer power available in each cluster.

Additionally, the Order requires Commerce, by January 29, 2024, to propose rules that impose a number of reporting and related obligations on US Infrastructure as a Service (IaaS) Providers (i.e., major US cloud providers) with respect to certain of their dealings with foreign persons and in particular foreign resellers of their IaaS Products. (Section 4.2(c)) Among other things, the proposed regulations would require US IaaS Providers to: 1) submit a report to the Secretary of Commerce when a foreign person transacts with such Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity; and 2) require that US IaaS providers prohibit any foreign reseller of their US IaaS product from providing those products unless such reseller also submits a report to the US IaaS Provider that such Provider must in turn submit to Commerce. It remains to be seen when such proposed regulations would become binding, but the fact that the Order requires them to be proposed indicates they will in all likelihood not enter into force and effect on January 30, 2024.

Undoubtedly, the pending Commerce rules will be groundbreaking in nature. Several things can be noted at this juncture:

- The Order invokes the Defense Production Act (DPA), which affords the President certain authorities related to national defense and the protection for critical infrastructure. The DPA has historically been invoked in wartime and sporadically in peacetime to establish defense priorities and resource allocations. It was more broadly utilized during the recent Covid-19 crisis to afford priorities to contracts for development of vaccines and personal protective equipment and address supply chain issues. Its use here to create reporting requirements for AI is novel in nature under the DPA, which generally is used to create priorities in government contract performance; in contrast, the companies involved here are primarily developing AI for the private sector rather than government usage. Nevertheless, the DPA is broad in scope and federal courts are loath to interpret the scope of such national security statutes narrowly in practice. Moreover, other federal statutes also could support such reporting requirements and Congress is currently working on creating a legislative framework for AI.

- The reporting requirements, once issued by Commerce, will need to be closely reviewed by companies for their full scope and application. Numerous definitions relating to the coverage of "companies" and various foreign entities will determine questions such as whether it applies to offshore AI development by US firms, whether foreign firms undertaking development of AI models in the US are subject to the requirements, and so on.

- Significantly, the Order does include some key initial definitions of technical conditions for AI models and clusters subject to the new reporting requirements (Sec. 4.2(b)), and directs Commerce to use these initial de facto standards until it defines and periodically updates its own set of such standards. The definition of a specified quantity of computing power as a reference point for AI models is particularly noteworthy, and can be expected to evolve over

time as AI models become widely available globally and more powerful. This type of quantitative standard is reminiscent of the standards Commerce has employed for many years for the adoption of export controls on computers.

- Finally, the requirement that companies turn over the "results" of a broad range of red-team testing undoubtedly will raise sensitivities by companies who view such materials as highly proprietary in nature. Certainly, Commerce will need to consider putting in place measures to maintain the confidentiality of such information and limit its transmission within the Federal Government. (Sec. 4.2(a)(i)(C))

Ensuring the Safety and Security of AI Technology: With the goal of protecting American's safety and security, this section of the Order sets out a broad range of requirements that will engage dozens of departments and agencies in safeguarding AI's use and development.

- **Guidelines and Standards** – The Order tasks the Secretary of Commerce, acting through NIST, to establish guidelines and best practices for safe, secure, and trustworthy AI systems. Commerce must also develop guidance and benchmarks for auditing and evaluating AI capabilities, with a focus on those capabilities through which AI could cause harm, such as in the areas of cybersecurity and biosecurity. As part of this effort, NIST is also instructed to develop a companion resource to its AI Risk Management Framework, which we summarized here, and the Secure Software Development Framework.[4] (Sec. 4.1)

- **Chemical, Biological, Radiological or Nuclear Risks (CBRN)** – To better understand and mitigate the risks of AI being misused to promote CBRN threats, such as biological weapons, the Department of Energy is instructed to consult with a broad range of experts within the Federal Government and in private AI laboratories, academia, and third-parties to evaluate the potential for AI to be misused

to develop CBRN threats, while considering the application of AI to counter these threats, and provide a report to the President within 180 days. (Sec. 4.4)

- **Cybersecurity and Critical Infrastructure** – The Order directs the heads of each agency with authority over critical infrastructure to provide DHS with an assessment of potential risks related to the use of AI in critical infrastructure, including whether the use of AI makes critical infrastructure more vulnerable to critical failures, physical attacks, and cyber attacks. Independent agencies are encouraged to contribute to this effort. DHS must develop security guidelines for use by infrastructure owners and operators and, with the heads of relevant agencies, DHS must take steps to mandate such guidelines through regulatory or other action, as appropriate. And the Department of Defense and DHS must conduct an operational pilot project to test AI systems, such as large language models, to discover and remediate vulnerabilities in critical US government software, systems, and networks. (Sec. 4.3)

- **Synthetic Content Created or Modified by AI** – In order to improve transparency and increase public trust in synthetic content produced by AI systems, and to establish the authenticity and provenance of digital content, the Order requires the Department of Commerce to identify standards, tools, methods, and practices for authenticating content and tracking its provenance, and detecting and labeling synthetic content, such as using watermarks. (Sec. 4.5)

Protecting Privacy: To mitigate privacy risks potentially exacerbated by AI and to protect against the misuse of personal information and data, the Order tasks the Director of OMB with evaluating the types of commercially available information (CAI) that agencies procure, particularly CAI procured from data brokers, and with assessing how CAI is collected, used, disseminated, and disposed in order to inform potential guidance to agencies. A request for information (RFI) must be issued seeking input on revisions to current guidance on how agencies implement privacy provisions in the E-Government Act

of 2002. Federal agencies must evaluate the effectiveness of their privacy enhancing technologies and the Secretary of Energy is directed to create a Research Coordination Network committed to privacy research and privacy enhancing technologies. (Sec. 9)

Supporting Workers: With the evolving capabilities of AI, there are growing concerns about AI-related workforce disruptions. The Order directs the Council of Economic Advisers to prepare a report to the President within 180 days on the effects of AI on the labor-market. The Secretary of Labor is directed to evaluate the necessary steps for the Federal Government to take to address AI-related workforce disruptions and to submit a report to the President analyzing the ability of agencies to support workers displaced by the adoption of AI. The report must assess how current and former federal programs designed to assist workers facing job disruptions, such as unemployment insurance, could be used to address possible future AI-related disruptions and address potential legislative measures.

The Order further requires that the Secretary of Labor, in consultation with labor unions and workers, develop and publish principles and best practices for employers to use to mitigate AI's potential harms to an employee's well-being. Among other topics, the principles and best practices must cover the implications for workers of employers' AI-related collection and use of data about the workers, including transparency, engagement, management, and activity protected under worker-protection laws. The Order also requires the Secretary of Labor to support employees whose work is monitored or augmented by AI by ensuring that employees are compensated for their time worked. (Sec. 6)

Advancing Equity and Civil Rights: In response to strong evidence showing how the irresponsible use of AI can lead to unlawful discrimination and other harms, the Order mandates the Attorney General to submit a report to the President on the use of AI in the criminal justice system and to recommend best practices, safeguards, and appropriate limits on AI use in such areas as sentencing, parole, bail, police surveillance, prison-management tools, and forensic analysis. Agencies are directed

to use their civil rights and civil liberties offices and authorities to prevent and address discrimination in the use of automated systems, including algorithmic discrimination. The Order calls on HHS to publish a plan addressing the use of algorithmic systems in the distribution of public benefits by states and localities to assess unjust denials, processes to appeal denials to human reviewers, and whether algorithmic systems achieve equitable and just outcomes. (Sec. 7)

Promoting Innovation and Competition: To attract AI talent to the US, the Order instructs the Secretary of State and DHS to streamline the visa process, create a program to locate talent abroad, and initiate policy changes that modernize pathways to immigration for experts in AI and other critical and emerging technologies. The Order directs the NSF to launch a pilot program that implements the National AI Research Resource by creating and distributing an AI-related research resource and tool. The Secretary of Labor is directed to publish a RFI requesting information on AI and STEM jobs that need qualified candidates. (Sec. 5.2(a)(i)) Other provisions include:

- **Creating Institutes and Engines** – NSF must establish one NSF Regional Innovation Engine dedicated to AI-related work and at least four new National AI Research Institutes, and with the Department of Energy enhance training programs for scientists in hopes of training 500 new researchers by 2025 in AI. (Sec. 5.2(a)(ii)-(iii), (b))

- **Mitigate Climate Change** – The Secretary of Energy is directed to publish a report on ways that AI can improve planning, investment, and operations for the electric grid. (Sec. 5.2(g))

- **Patent and Trademark** – The US Patent and Trademark Office is directed to publish guidance for patent examiners and applicants addressing inventorship and the use of AI, including generative AI, in the inventive process. (Sec. 5.2(c)(i))

- **Copyright** – The US Copyright Office is directed to prepare recommendations to the President on potential executive actions relating to copyright and AI that will address the

scope of protection for works produced using AI and the treatment of copyrighted works in AI training. (Sec. 5.2(c)(iii))

Advancing Federal Government Use of AI: AI has the potential to improve governmental agencies' ability to deliver results. The Order advances the coordinated use of AI across the Federal Government by directing the Director of OMB to assemble an interagency council to develop guidance to strengthen the effective and appropriate use of AI by agencies and to manage risks from AI. Each agency must designate a Chief Artificial Intelligence Officer to coordinate their agency's use of AI and implement required risk management practices for the agency's use of AI that impacts people's rights or safety. To advance the responsible and secure use of generative AI, agencies must put appropriate safeguards in place, including limiting access, as necessary, to specific generative AI services based on specific risk assessments and guidelines, training, and the negotiation of appropriate terms of service with vendors. The Order also directs the Federal Government to increase top AI talent at federal agencies. (Sec. 10)

Consumers, Patients, and Students: The Order mandates the development and use of AI in the human-services, healthcare, and education sectors in ways that enhance access and the affordability of resources in an efficient way and that also protects citizens from fraud, discrimination, and threats. At their discretion, independent regulatory agencies are encouraged to take additional steps to protect consumers from fraud and discrimination. (Sec. 8)

Strengthening American Leadership Abroad: To strengthen US leadership of global efforts to meet AI's challenges and potential, the Secretary of State is directed to lead efforts to establish a strong international framework for managing the risks and harnessing the benefits of AI, including by encouraging international allies and partners to support voluntary commitments similar to those that US companies have made. The Secretary of Commerce is directed to advance responsible global technical standards for AI development and establish a plan for global

engagement. To address global AI risks to critical infrastructure, DHS is ordered to lead efforts with international allies and partners to enhance abilities to respond to and recover from potential critical infrastructure disruptions resulting from the incorporation of AI into critical infrastructure systems or malicious use of AI.

What's Next

- Companies developing highly sophisticated dual-use foundation models and US IaaS providers should be on the lookout for requirements from Commerce implementing the private sector reporting requirements under the DFA, and should consider providing their views to Commerce informally as it writes its new rules.

- Expect the various departments and agencies to roll out mandated guidelines, standards, and best practices for responsible AI over the next year, with the strong implication that regulation may follow.

- Companies developing, using, or selling AI-related technology should consider adding flexible terms to their contracts that will accommodate the expected wave of new regulations, particularly with regard to content authentication and guardrails.

- Consider whether Congress in the not-too-distant future will enact a law mandating the private sector to adopt new safeguards to ensure the safe, secure, and trustworthy development and use of AI.

We will continue to monitor developments related to this order and related policies.

_____

If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed or the Eversheds Sutherland attorney with whom you regularly work.

1 The White House: Presidential Actions, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.
2 AI red-team testing must be based on guidelines developed by the National Institute of Standards and Technology (NIST), in coordination with the Department of Energy and the Department of Homeland Security (DHS) and include guidelines related to assessing and managing the safety, security, and trustworthiness of dual-use foundation models. NIST, the National Science Foundation (NSF) and the Department of Energy shall develop and help to ensure the availability of testing environments, such as testbeds, to support these goals, as well as to support the design, development, and deployment of privacy enhancing technologies (PETs). (Sec.4.1(ii))
3 The Order defines dual-use foundation model as "AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters…"
4 NIST, *Secure Software Development Framework*, NIST, https://csrc.nist.gov/Projects/ssdf.

GIR

AMERICAS
INVESTIGATIONS REVIEW 2024

The Americas Investigations Review contains insight and thought leadership from 15 pre-eminent practitioners from the region. Spanning 60 pages, this particular review is part retrospective, part primer, part crystal ball – and 100 per cent essential reading.

Inside you'll read about some of the most important developments affecting international investigations in North and Latin America, supported throughout with footnotes and relevant statistics. This edition focuses on the US and Mexico in particular and has primers on the forensic skills of ESG and crypto-related investigations, and on some sensible precautions to take before releasing AI on your clients.

Visit globalinvestigationsreview.com
Follow @GIRalerts on Twitter
Find us on LinkedIn

A Mayflower Compact for AI: implementing responsible self-governance for US companies

Michael Bahar, Rachel Reid, Mary Jane Wilson-Bilik and Ronald Zdrojeski*

Eversheds Sutherland

In summary

In the absence of clear AI-specific legislation or regulation in the United States, companies should neither heedlessly charge ahead nor timidly wait for greater clarity. Rather, as regulators use existing authorities and private litigants use old laws to bring suits centred on the newest technologies, companies should strongly consider establishing a written internal AI self-governance framework. This framework would institutionalise a focus on accountability, accuracy, fairness, security and other principles while developing or integrating AI tools, and it should include clear contracting guidelines. Through effective governance and responsible practices, companies can leverage AI's potential while greatly mitigating class action and regulatory risks.

Discussion points

- State of AI legislation in the United States and abroad
- Governance and mitigating regulatory and litigation risk
- Pillars of an AI self-governance programme

Referenced in this article

- Electronic Communications Privacy Act
- Computer Fraud and Abuse Act
- California Invasion of Privacy Act
- California Unfair Competition Law
- Illinois Biometric Information Privacy Act
- Illinois Consumer Fraud and Deceptive Business Practices Act
- SAFE Innovation Framework for AI Policy
- EU Artificial Intelligence Act

As companies of all sizes across industries begin to accept, if not embrace, the new world of artificial intelligence (AI), in-house legal departments and operational risk management personnel should be aware of the potential risks associated with using this awe-inspiring technology. Indeed, US regulators are already strongly signalling their intention to regulate first and allow space for innovation later. And government regulators are not alone; private litigants have begun to file class action lawsuits against companies deploying AI technologies.

The best way to insulate from these risks is not just to charge ahead in the belief that the absence of legislation means the absence of boundaries, or to timidly wait for definitive guidance and limits. Rather, it is through an effective self-governance framework – akin to a Mayflower Compact for AI. Acting now to establish an enterprise-wide self-governance framework will put companies on course to successfully navigate and harness this exciting technology, while avoiding its shoals.

From ebullience to trepidation

The sight of new land is exciting, but as the shoreline comes into view, so do the potential challenges.

In March 2023, New York Times columnist Thomas Friedman wrote about AI in terms of a 'Promethean Moment', akin to when fire came down from Mount Olympus to humankind on Earth with its 'awe-inspiring' potential to 'solve seemingly impossible problems'. Two months later, however, Friedman began to adopt a different mythological analogy, referring to generative AI as 'Pandora's Box', Zeus' punishment to mortals and the god who stole fire for them. If we approach generative AI just as 'heedlessly' as we did Web 2.0 technologies, Friedman wrote, 'Oh, baby, we are going to break things faster, harder and deeper than anyone can imagine.'

Two days later, President Biden issued a statement that similarly emphasised AI's risks over its rewards and the government's determination to regulate at once: 'AI is one of the most powerful technologies of our time, but in order to seize the opportunities it presents, we must first mitigate its risks.'

Key US federal regulators also made clear their commitment to investigate and regulate AI in a declarative statement on 25 April 2023, which concluded with their joint 'pledge' to 'vigorously use our collective authorities to protect individuals' rights regardless of whether legal violations occur through traditional means or advanced technologies'.

Private litigants are gearing up as well, with landmark class actions filed the last week of June 2023 alleging privacy violations, intellectual property infringement, illegal wiretapping, unfair competition and a slew of other complaints against OpenAI, the maker of ChatGPT, and other defendants. At the core of plaintiffs'

arguments is the alleged 'rush' to market 'without implementing proper safeguards or controls to ensure that they would not produce or support harmful or malicious content and conduct that could further violate the law, infringe rights, and endanger lives'. The existing laws alleged to have been violated include the Electronic Communications Privacy Act,[1] the Computer Fraud and Abuse Act,[2] the California Invasion of Privacy Act,[3] the California Unfair Competition Law,[4] the Illinois Biometric Information Privacy Act[5] and the Illinois Consumer Fraud and Deceptive Business Practices Act.[6]

Importantly, US federal legislation to set AI guardrails is now on the horizon. On 22 June 2023, the powerful Senate Majority Leader, Charles Schumer, proposed a new bipartisan framework, the SAFE Innovation Framework for AI Policy, to encourage AI innovation while advancing 'security, accountability, foundational values and explainability'. In autumn 2023, Schumer will convene a series of AI Insights Forums that will solicit input on legislative proposals from industry, consumers and researchers, addressing topics such as privacy, intellectual property, workforce and national security, as well as the importance of AI innovation. Schumer has already formed a bipartisan leadership group and instructed committee chairs to identify areas where they can work on AI legislation in a bipartisan fashion. Schumer's goal is to pass legislation in a matter of months, not years.

In addition, governing bodies, regulatory authorities, lawmakers and litigants across the United States are keeping a close eye on legal developments abroad. The EU Artificial Intelligence Act, which is poised to become the world's first comprehensive AI law, would regulate the application of AI using a risk-based approach, similar to cybersecurity regulation. AI systems applied to activities that pose minimal risk (to individuals, communities, the environment, etc) would essentially be unregulated, while those AI systems applied to limited or high-risk activities would be subject to increasing levels of regulation. The use of AI systems in ways that pose 'unacceptable risk' – those systems considered to be a threat to people – would be banned (with limited exceptions).

Outside of the EU, the United Kingdom has published a white paper titled 'A pro-innovation approach to AI regulation'. The proposed UK approach relies on collaboration between the government, regulators and business, and lays out a flexible framework underpinned by five principles to guide and inform the responsible development and use of AI in all sectors: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress.

1 18 USC section 2510, et seq.
2 18 USC section 1030.
3 California Penal Code, section 631.
4 Business and Professionals Code, section 17200, et seq.
5 740 ILCS 14/1, et seq.
6 815 Illinois Comp Statute section 505, et seq.

While the legislative framework for AI governance in other parts of the globe remains in various stages of development, there is a growing degree of regulatory convergence around the underlying principles of AI, especially the OECD's 2018 AI Principles, and the need for companies to develop internal controls to identify and mitigate AI's risks. Regulators – and many companies – also recognise that existing authorities, including, if not especially, privacy laws, already provide strong grounds for enforcement activity.

We discuss the existing authorities in the United States further below, but in short, whether companies are on the leading or following edge of this revolutionary technology, sound self-governance and risk management processes will be key to maximising success and to mitigating the impending enforcement and litigation risks.

Governance and mitigating regulatory and litigation risk

Legal and risk management departments witnessing this rapidly evolving risk profile should take steps now to formalise their approach to self-governance through the adoption of a comprehensive AI programme tailored to their company and its unique risk profile. Adopting detailed principles and policies for AI development, use and deployment, instituting internal guardrails and oversight processes, and providing robust training, will better position companies to comply with regulatory developments and to mitigate new legal and operational sources of risk.

There is not yet any AI-specific legislation in the United States, but regulators are poised to strike, increasing the urgency of self-governance. For example, the Federal Trade Commission (FTC) issued a report evaluating the use and impact of AI in combatting online harms identified by Congress. The report outlined significant concerns that AI tools can be inaccurate, biased and discriminatory by design and incentivise relying on increasingly invasive forms of commercial surveillance.

The FTC also warned market participants that violations of the FTC Act could result from the use of automated tools that have discriminatory impacts, the assertion of claims about AI that are not substantiated, or the deployment of AI technology before appropriate steps are taken to assess and mitigate risks. Finally, the FTC has required firms to destroy algorithms or other work products that were trained on data that should not have been collected.

In addition, the Consumer Financial Protection Bureau, which regulates financial institutions, published a circular confirming that federal consumer financial laws and adverse action requirements apply regardless of the technology used. The circular also made clear that the fact that the technology used to make a

credit decision is too complex, opaque or new is not a defence for violating these laws. Notably, the circular includes the following statement:

> *Creditors who use complex algorithms, including artificial intelligence or machine learning, in any aspect of their credit decisions must still provide a notice that discloses the specific principal reasons for taking an adverse action. Whether a creditor is using a sophisticated machine learning algorithm or more conventional methods to evaluate an application, the legal requirement is the same: Creditors must be able to provide applicants against whom adverse action is taken with an accurate statement of reasons.*[7] *The statement of reasons 'must be specific and indicate the principal reason(s) for the adverse action.'*[8]

The Department of Justice (DOJ) filed suit against a social media company, alleging that through its design and its use of AI for ad targeting categories based on user demographics or other characteristics, it had 'intentionally discriminated on the basis of race, color, religion, sex, disability, familial status, and national origin'. Significant for DOJ was the company's apparent intent, which means that regulators will look to external and internal statements to assess whether the company's AI use is inappropriate. The case was eventually settled, and the settlement included requirements to stop using certain AI tools and to engage an independent third party to assess new AI systems for bias and discrimination.

In a separate case, the Department of Justice's Civil Rights Division filed a statement of interest in federal court explaining that the Fair Housing Act applies to algorithm-based tenant screening services. In reference to such statement, the Assistant Attorney General of the Justice Department's Civil Rights Division, Kristen Clarke, stated that 'housing providers and tenant screening companies that use algorithms and data to screen tenants are not absolved from liability when their practices disproportionately deny people of color access to fair housing opportunities.' Clarke went on to state that 'this filing demonstrates the Justice Department's commitment to ensuring that the Fair Housing Act is appropriately applied in cases involving algorithms and tenant screening software.'

The Equal Employment Opportunity Commission (EEOC), in addition to its enforcement activities on employment discrimination related to AI and automated systems, issued a technical assistance document explaining how the Americans with Disabilities Act (ADA) applies to the use of software, algorithms and AI to make employment-related decisions about job applicants and employees. In this document, the EEOC explained that the most common ways an employer's use of algorithmic decision-making tools could violate the ADA are by:

7 15 U.S.C. 1691(d)(2)(A), (B); 12 CFR 1002.9(a)(2)(i), (ii).
8 12 CFR 1002.9(b)(2).

- failing to 'provide a "reasonable accommodation" that is necessary for a job applicant or employee to be rated fairly and accurately by the algorithm';
- relying on 'an algorithmic decision-making tool that intentionally or unintentionally "screens out" an individual with a disability, even though that individual is able to do the job with a reasonable accommodation'; and
- adopting 'an algorithmic decision-making tool for use with its job applicants or employees that violates ADA's restrictions on disability-related inquiries and medical examinations'.

In New York City, Local Law 144 now threatens civil enforcement of between US$500 and US$1500 per day for employers located in New York City or with candidates or employees in the city, who use automated employment decision tools to evaluate job candidates or employees for employee decision purposes if those tools have not been audited for bias and if notice and website disclosure requirements are not met. On 6 April 2023, the final rules promulgated pursuant to Local Law 144 were adopted, with enforcement beginning on 5 July 2023.

Self-governance helps avoid these risks by requiring active and sustained systems and processes to monitor, manage and mitigate various sources of risk throughout the AI lifecycle. Importantly, while ethical pronouncements and principled statements of values are an important first step, standing up accountability mechanisms and structuring hierarchies of decision-making, review and oversight are pivotal to cultivating a true culture of compliance and risk management around the use of AI.

Whether a company is currently using machine learning algorithms or looking to implement natural language processing or another generative AI system, companies should strive to align their AI self-governance programme with their current and possible future uses of both predictive and generative AI technologies.

An AI self-governance programme should include, at a minimum, four primary pillars – governance, assessment and monitoring, privacy and data security and third-party contracts.

.

Pillar 1: AI governance

Given the complexity of AI systems and their associated risks, governance should start at the highest level within an organisation, such as the board of directors or a committee thereof. The board or responsible committee should designate the senior leader at the company with accountability for the AI programme, and the senior leader should then assign responsibilities to the appropriate functional leaders. A set of robust policies and procedures should be drafted and implemented, including the company's processes for designing and developing AI systems, conducting AI risk assessments, cataloguing AI systems, evaluating

data sets used for AI and contracting for third-party AI systems. AI governance documents should also clearly set forth decision-making authority for AI systems, including which decisions are reserved for senior management and the board of directors.

Pillar 2: assessment and monitoring of AI systems

Prior to developing or deploying any AI systems, companies should adopt standards and principles that will guide how AI systems will be assessed and monitored, including how the company will identify and mitigate potential risks and liabilities.

These AI assessment principles could include:

- reliability and accuracy: AI systems should perform consistently and provide accurate results across varying conditions;
- safety: AI systems should prioritise human safety and avoid causing harm. Any risk associated with the use of AI systems should be mitigated to the greatest extent possible;
- transparency and explainability: the AI systems should be transparent in their operations, and their decisions should be explainable and interpretable to users; and
- fairness: AI systems should operate in a fair manner, avoiding biases that could lead to discriminatory outcomes. This includes ensuring that AI-assisted decision-making is equitable and does not disadvantage any individual or group.

The decision to deploy and integrate an AI system into a business function should be made thoughtfully based on the specific needs of the organisation and with an understanding of the requirements for ongoing testing and monitoring. Both the algorithmic model itself, as well as the data inputs, should be assessed regularly for potential non-compliance with the principles adopted by the company, as well as non-compliance with existing laws, such as those regarding privacy, intellectual property, discrimination and consumer protection.

For companies actively bringing AI-driven tools to the market, testing throughout the product development lifecycle should prioritise verification, modification and transparent reporting of results at various stages of training the model. Companies that can label and document with confidence the safety, security, reliability and validity of their models, and demonstrate their commitment to responsibly built AI solutions will promote greater trust with regulators, consumers and users alike.

As new tools and products enter the AI market, companies should continuously adapt their governance frameworks, re-evaluate risk profiles, manage potential liabilities and align their oversight systems with best practices. As

looming regulations come into effect, companies that proactively implement accountability structures and responsibly manage their AI product integrations and offerings will be able to navigate new compliance demands efficiently and effectively.

Pillar 3: privacy and data security

Data – and, principally, personal data – is the lifeblood of AI systems. Generative AI systems, in particular, rely on vast amounts of data to learn and make decisions, and companies should consider privacy law compliance and the impact on individual privacy in the context of AI. The complex patchwork of existing privacy laws in the United States regulates how personal data is collected, used, processed and shared in any context, including throughout an AI system's lifecycle, as well as the rights of the individuals to whom personal data relates. Performing a data privacy impact assessment on all data collected by or shared with an AI system can help companies evaluate each AI system's compliance with applicable privacy laws. In addition, companies should implement and maintain reasonable administrative, physical and technical safeguards to protect all personal data collected by and shared with an AI system, as required by applicable data protection laws and regulations. Security considerations around AI should also include data loss prevention and the protection of propriety technology and confidential information.

All data used by an AI system to fulfil its purposes or to improve or advance the AI system's capabilities must be lawfully acquired, which typically requires the informed consent of the data subject. Providing clear, comprehensive and transparent disclosures about the potential uses of data and obtaining informed, opt-in consent from the data subjects will help shield companies from liability and build trust with consumers. Imposing internal restrictions on the use of certain types of data – such as sensitive personal data – in connection with an AI system can further protect against potential privacy violations.

Pillar 4: allocating risk and responsibility in third-party contracts

AI systems are often marketed as bespoke solutions for companies. Therefore, it is important for both developers and licensors of AI systems, as well as those companies acquiring third-party AI systems, to assign responsibilities and allocate liability in a written contract.

As the legal and regulatory landscape specific to AI continues to evolve quickly, establishing clear roles and responsibilities of the parties – including with respect to compliance with future laws and regulations – can help avoid disputes and incentivise both sides to engage in responsible AI development

and adoption from the outset. The contract should include, at a minimum, provisions addressing the following:

- restrictions on any external data sets and other inputs used with the AI system, including those that may be restricted due to privacy or intellectual property law considerations;
- requirements around transparency and explainability of the AI system;
- security and resiliency standards both for the AI system and for any integrated or inter-connected systems and technology;
- responsibility for compliance with applicable privacy and data protection laws;
- ownership rights in the inputs and outputs of the AI system and any restrictions on use of the same;
- ownership of intellectual property rights in the AI system and liability for any infringement of third-party intellectual property rights as a result of the use or operation of the AI system;
- rights and obligations of the parties with respect to changes in law; and
- responsibility for ongoing testing and monitoring of the AI system, including testing and monitoring for fairness and accuracy, transparency and explainability, security and safety, and potential bias or discrimination.

Contract language should also take into account the ongoing development of new international AI standards that will underpin an evolving assurance infrastructure, standards such as ISO/IEC 42005 on AI System Impact Assessments, as well as any licensing requirements that may be put in place for highly capable foundation models, which include those used in generative AI and their cloud providers. Special provisions will be required for any contracts involving 'frontier' models, which are models having different architectures or mixes of scale and capabilities than the average model that could pose unique risks and are less well understood by the research community. Consideration should also be given to requiring vendors to certify their alignment with recognised frameworks for AI risk assessment, such as the National Institute of Standard and Technology's AI Risk Management Framework.

Parties on both sides of an AI system transaction should also consider insurance coverage to protect against potential losses arising from the use of the AI system.

Conclusion

The shoreline of the new world of AI is enticing yet craggy; the wilderness is not as ungoverned as it may appear. Despite the absence of AI-specific legislation, regulators and private litigants are hyper-focused on testing whether a company has an appropriate AI governance programme, one that can adequately explain the AI system, its inputs and its outputs, its risks as well as its opportunities.

Therefore, companies should resist any temptation to race to beat the law, or to wait on the sidelines for bright-line clarity, and instead implement a reasonable, thoughtful and responsible AI self-governance programme.

Ultimately, regulators and private litigants will be looking for accountability the same way they do with privacy and cybersecurity. Who, in any particular organisation, 'owns' AI, and who is charged with ensuring that AI systems are operating responsibly, not just efficiently?

Indeed, efficiency cannot be AI's sole goal. Rather, accuracy, fairness, reliability, predictability, explainability, security and resiliency should all share the stage, and regulators will expect clear guidelines and guardrails on these points, with humans responsible for each.

With a self-governance AI programme that translates principles into practice, companies can use effective governance, assessments, privacy and data security and third-party contracts to safeguard against the legal risks of AI, while pursuing new opportunities to integrate and innovate this powerful technology ethically, responsibly and profitably.

**The authors would like to acknowledge associate Chris Bloomfield and summer associate Jeremy Bloomstone for their contributions to the article.*

Michael Bahar

Eversheds Sutherland LLP

Michael Bahar is a litigation partner in the firm's Washington, DC, office and the co-lead of the firm's global cybersecurity and data privacy practice, consisting of over 160 lawyers across 35 countries.

He provides highly responsive, pragmatic and comprehensive cybersecurity and privacy advice to some of the world's largest companies. He has particular experience in helping companies across industries efficiently navigate the rapidly evolving threat, regulatory and litigation environments. His business-focused advice is designed to mitigate risk and maximise opportunities, especially as clients look to enter new markets, develop or adopt revolutionary technologies and products, monetise data and transfer data across borders.

Rachel Reid

Eversheds Sutherland LLP

Rachel Reid has more than 20 years of experience advising financial services and technology companies on a wide range of legal and regulatory matters, including data privacy and security, artificial intelligence, risk management, operations, corporate governance, complex commercial transactions, technology transactions and outsourcing.

Rachel has helped lead high-growth companies through complex regulatory environments and acquisitions, while providing guidance to senior leaders in large, global public companies, including members of the C-suite and the board of directors.

Mary Jane Wilson-Bilik

Eversheds Sutherland LLP

Mary Jane Wilson-Bilik is a technology, privacy and insurance regulatory law partner at Eversheds Sutherland (US) in Washington, DC, who serves as head of the firm's US AI practice in financial services, and co-chair of its global AI in financial services practice.

For more than 25 years, MJ has advised her financial services and technology clients on privacy and innovation issues. Her recent focus has been to assist clients perform AI impact assessments and develop robust risk management, governance and vendor management policies for their AI efforts, including generative AI. She counsels clients on assessing AI risks on a cross-sector basis, monitoring for bias, privacy, cybersecurity, intellectual property and specialized regulatory risks, and implementing effective governance measures-and guardrails.

Ronald Zdrojeski
Eversheds Sutherland LLP

Ronald Zdrojeski is a litigation partner in the firm's New York office. With decades of trial experience, Ronald Zdrojeski's practice focuses on counselling and defending businesses in complex commercial litigation, including market manipulation, fraud and other white collar matters. Ron has litigated in 48 of the country's 50 states, defending Fortune 500 companies, insurers and corporate officers in criminal and civil investigations, including class action, toxic tort, trade secret, intellectual property, environmental and maritime litigation.

EVERSHEDS SUTHERLAND

Eversheds Sutherland provides the full range of legal services to a global client base ranging from small and mid-sized businesses to the largest multinationals, acting for 79 of the Fortune 100, 65 of the FTSE 100 and 134 of the Fortune 200. With more than 3,000 lawyers, Eversheds Sutherland operates in more than 70 offices in over 30 jurisdictions. Eversheds Sutherland is a global legal practice and comprises two separate legal entities: Eversheds Sutherland (International) LLP (headquartered in the UK) and Eversheds Sutherland (US) LLP (headquartered in the US), and their respective controlled, managed, affiliated and member firms.

999 Peachtree St NE #2300
Atlanta, GA 30309
United States
Tel: +1 404 853 8000

1114 6th Ave
New York, NY 10036
United States
Tel: +1 212 389 5000

700 6th St NW
Washington, DC 20001
United States
Tel: +1 202 383 0100

www.eversheds-sutherland.com

Michael Bahar
michaelbahar@eversheds-sutherland.com

Rachel Reid
rachelreid@eversheds-sutherland.com

Mary Jane Wilson-Bilik
mjwilson-bilik@eversheds-sutherland.com

Ronald Zdrojeski
ronzdrojeski@eversheds-sutherland.com