Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

Introduction
Alan Charles Raul
Sidley Austin LLP

practiceguides.chambers.com

INTRODUCTION

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

The Wait for Comprehensive Federal Data Protection in the United States Continues, While Global Governance of Artificial Intelligence Is Just Beginning

Well, it is 2023 and the United States is still waiting for a comprehensive, federal privacy law. The wait is not all bad, though, as the proposed legislation is still stuck on the question of whether a new federal law should pre-empt the state privacy laws, such as those already enacted in California, Virginia, Colorado, Connecticut and Utah – with more of the same in line to be adopted in other states this year.

While the state laws diverge in some substantive ways, they are much more similar than they are different – and all emulate the general concept of data subject rights established under the EU General Data Protection Regulation (and the US Privacy Act of 1974).

Differences among the laws include:

- whether or not employee data and business contact information are covered by a state's law (covered in California, but not in the other states);
- what data is exempt from the laws (including varied exceptions for entities and data that are subject to HIPAA and GLBA);
- what rights are afforded to individuals (such as between the right to opt-out of the sale or sharing of personal information in California and the right to opt-out of sale or targeted advertising in Virginia, Colorado, Utah and Connecticut);
- the content and structure of required privacy notices and policies;
- whether specific assessments and/or audits are required; and
- whether there is a required right to cure period following notification of an alleged violation with the law (which California no longer mandates as of 1 January 2023).

None of the state laws authorises a private right of action for individual consumers or data subjects to enforce the states' privacy laws (except that California allows private litigation over data breaches resulting from a company's lack of "reasonable security). All of the states contemplate enforcement by their states' Attorney General, and in the case of California, also by the newly created California Privacy Protection Agency.

Whether to authorise a private right of action is another major factor that has impeded enactment of a federal privacy law. While essentially all factions agree that the Federal Trade Commission should have more power and resources to enforce whatever new federal law is ultimately enacted, business and consumer advocacy groups, and their respective partisans in Congress, come down on different sides of private enforcement of privacy violations.

When it comes to enforcing against relatively intangible "informational injuries", a case can be made that public officials – such as Attorneys General and the FTC – may be better placed than plaintiffs' lawyers to exercise prosecutorial discretion to make appropriate judgments about what harms are substantially injurious enough to warrant enforcement against companies engaged in (arguably) standard commercial activity. This is especially true where the FTC must apply a statutory cost-benefit analysis to enforce against allegedly "unfair" business practices (namely, that the unfair practice causes

substantial injury that cannot be reasonably avoided by the consumer, and that is not outweighed by countervailing benefits to consumers or competition). To enforce against "deceptive" practices, the FTC must conclude that the alleged deception is material – ie, that a reasonable consumer's conduct or decisions would be affected by the deception.

Other sticking points in current drafts of federal legislation include possible incorporation of a "duty of loyalty" that would impose data minimisation and other specific limits on data processing, but which duty might be extended to the even more contentious notion of a generalised "fiduciary" duty on the part of businesses that collect and use personal information. Notably, while current draft legislation includes civil rights protections that specifically prohibit discriminatory collection or processing of data, it also contains a specific exception that would allow discrimination which is implemented for the purpose of diversity – ie, diversifying applicant, participant or customer pools.

FTC Regulatory Actions

Perhaps 2023 will be the year to break the logjam on a US national privacy law. Or perhaps not.

In any case, while Congress deliberates, the FTC has signalled aggressive regulatory (as well as enforcement) initiatives. In particular, in August 2022, the Commission published an advanced notice of proposed rulemaking (ANPR) on what the agency characterised "commercial surveillance" and "lax data security" practices. This is the first step in what will necessarily be a lengthy process concerning standards and requirements for information security, the ways in which companies collect and process data in commercial contexts, and whether any practices related to the transfer, sharing, selling, or other monetisation of personal information should be categorised as unfair or deceptive.

The FTC broadly defined "commercial surveillance" as the "business of collecting, analyzing, and profiting from information about people" and expressed concerns about the volume of consumer data collected as part of the modern digital economy. The FTC is especially worried about passive or relatively opaque collection of information from or about consumers. Additional FTC concerns relate to the possible effects from automated systems that rely on large volumes of data that may be potentially subject to error and discriminatory biases.

The ambitious regulatory scope of the ANPR is highly controversial. The FTC has been criticised for stretching its existing, general consumer protection authority to prohibit "unfair or deceptive acts or practices" beyond breaking point – or, more specifically, beyond what the Supreme Court will approve under the so-called "major questions doctrine." This doctrine holds that administrative regulations that would entail "vast economic or political significance" for society may only be upheld if Congress has clearly authorised such action in statutory text. One general clause in the FTC Act, substantially intact since the law was first adopted in 1914, is not likely to be deemed sufficient by the current Supreme Court to authorise the FTC's proposed overhaul of the digital economy.

Recent and Forthcoming EU Data Protection Governance

With regard to the global focus on digital governance of new technologies, the European Union continues to be the leader in proposing new rules for technology. It has adopted or is considering:

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

- the Digital Markets Act (competition rules for major internet platforms that are deemed "gatekeepers");
- the Digital Services Act (imposing liability, transparency and takedown rules on internet intermediaries such as cloud providers, search engines and social media companies);
- the Data Governance Act (rules for required reuse of certain data along with principles for data "altruism");
- the Data Act (fostering data sharing between and among businesses and with government);
- the AI Act (assigning AI applications to different risk categories subject to different legal compliance, transparency and impact assessment obligations); and
- numerous new cybersecurity and resiliency legislative initiatives as well.

The AI Act

Political agreement on the AI Act was reached by the Council of the EU on 25 November 2022 and the European Parliament is scheduled to vote on the draft by the end of March 2023.

At a high level, the AI Act is constructed around a set of four risk categories (unacceptable, high risk, limited risk and minimal/no risk) and regulates the use of AI in accordance with those risks.

Unacceptable risk

"Unacceptable" risk means that the use of the AI system for that purpose is prohibited. Examples include activities relating to social scoring by governments. A categorisation of unacceptable risk means the AI system cannot be placed on the EU market, be put into service in the EU, or used in the EU.

High risk

"High risk" means an AI system that is itself considered to be part of a "high-risk" category of products, or that acts as a safety components of such high-risk products, or is used for certain high-risk purposes or applications.

Examples of high-risk AI systems include those used for or in:

- medical devices and in-vitro diagnostic devices;
- educational or vocational training;
- remote biometric identification;
- critical infrastructure (digital infrastructure, road traffic and water, gas, heating and electricity supply);
- essential private and public services and benefits (decision-making around creditworthiness or life/health insurance, allocation of first emergency response services, etc); and
- employment, workers' management and access to self-employment (eg, CV-sorting software).

High-risk systems are required to comply with a number of restrictions under the AI Act both (i) before they can be put on the EU market or used and (ii) throughout their lifecycle, including the performance of a conformity assessment to demonstrate that the AI system is compliant with the AI Act. Those responsible for high-risk systems must also maintain adequate record-keeping, establish a quality and post-marketing monitoring and risk assessment system, comply with restrictions in relation to data sets used to train the AI, report serious incidents suffered by the AI system, and ensure appropriate human oversight.

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

Limited risk

"Limited" risk AI systems are those systems that do not fall under a high-risk or prohibited risk category, but that are intended to interact with individuals – eg, chatbots. Such systems are only subject to obligations pertaining to transparency – ie, the requirement that individuals are to be informed that they are interacting with an AI system as opposed to a human.

Minimal or no risk

"Minimal or no" risk AI systems are all systems that do not fall under one of the risk categories above – eg, video games or spam filters which use AI, and are not regulated under the AI Act.

General purpose

The AI Act also identifies a specific subcategory of "general purpose" AI systems – eg, speech and voice recognition systems, which are not generally regulated or restricted under the AI Act except where they are used for high-risk purposes, as described above, or are incorporated into a high-risk AI system.

Though the EU appears to be committed to legislating reams of new rules for technology, reality suggests that new laws may be neither necessary nor sufficient to achieve effective governance of the digital realm. For example, Chatham House, the London-based think tank famous for its eponymous Rule, offers a particularly thoughtful perspective on the complex tapestry of standards that will comprise "technology governance": namely, "shared principles, norms, rules, decision-making procedures, and programmes that shape the use of information technology and the internet worldwide."

Of course, the deployment of artificial intelligence across sectors – and especially generative AI – has attracted acute public interest and mounting regulatory attention everywhere. This attention has resulted in the emergence of a variety of nascent policy frameworks in the United States, European Union, and the United Kingdom.

Evidence-based dialogue about the risks associated with AI and appropriate remedies will be important to support the culture of responsible AI that will be necessary to preserve human rights and important shared values. As AI technology rapidly advances, co-operation and cross-fertilisation among global regulators, companies and civil society with respect to AI governance will be essential.

While the EU's AI Act is perhaps the farthest ahead in setting regulatory policy, the USA and UK are also well along in thinking about how to assure society receives the optimal benefits from AI innovation and its applications. Optimising the social benefits of this game-changing technology will of course require identification and prevention, plus mitigation, of potential harmful ensuing consequences.

A Blueprint for an AI Bill of Rights and the AI Risk Management Framework

In the USA, the White House Office of Science and Technology Policy (OSTP) published a Blueprint for an AI Bill of Rights in October 2022. The AI Blueprint consists of a set of five principles that could be used as voluntary guideposts for the development and deployment of AI systems:

- safe and effective systems;
- algorithmic discrimination protections;
- data privacy;
- notice and explanation; and
- human alternatives, consideration and fallback.

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

Taken together, these principles counsel companies to consider and evaluate how AI may negatively impact individual rights, opportunities, and access to critical resources.

In January 2023, the US Department of Commerce's National Institute of Standards and Technology (NIST) followed up the White House AI Blueprint with an AI Risk Management Framework (AI RMF).

The AI RMF is a non-binding framework developed in response to a Congressional mandate and in collaboration with the private and public sector. It is organised around a set of four functions designed to support an organisation's effective AI risk management: govern, map, measure, and manage.

Govern
Organisations should foster a culture of risk management when interacting with AI systems – eg, by establishing policies and accountability structures.

The framework also articulates characteristics of trustworthy AI that may be integrated into governance programs: valid and reliable, safe, secure, resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair (with harmful bias managed).

Map
The map function establishes the context to frame AI risks – eg, by categorising AI systems within an organisation.

The AI RMF defines "risk" as the "the composite measure of an event's probability of occurring and the magnitude or degree of the consequences of the corresponding event."

Measure
Organisations should employ quantitative, qualitative, and/or mixed-method tools to assess and monitor AI risk.

Manage
Organisations should leverage practices in all other categories to treat identified risks and decrease the likelihood of negative impacts.

NIST also published an accompanying, highly detailed "AI RMF Playbook" providing practical guidance on how to navigate and use the framework to operationalise trustworthy AI.

UK Information Commissioner's Office Guidance on AI and Data Protection
The UK Information Commissioner's Office has provided helpful "Guidance on AI and data protection", including a summary of the accountability and governance implications of AI. It covers the management of risk that use of AI poses to the rights and freedoms of individuals, including:

- automation bias and the lack of interpretability;
- ongoing compliance with data protection requirements, including data protection impact assessments for AI systems; and
- steps to ensure lawfulness, fairness, and transparency, as well as privacy, in AI systems.

Among other factors, the ICO stresses the need to mitigate potential discriminatory effects associated with either (i) imbalanced training data or (ii) training data that reflects past discrimination by, for example:

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

- establishing clear policies and good practices for the procurement and lawful processing of high-quality training and test data;
- assigning senior management responsibility for signing off the chosen approach to manage discrimination risk;
- undertaking robust testing of any anti-discrimination measures and monitoring AI/ML system performance on an ongoing basis.

Most recently, in July 2022, the UK's (currently named) Department for Science, Innovation and Technology evolved its national AI strategy toward establishing a pro-innovation approach to regulating AI. Characteristics of the UK's pro-innovation regulations include:

- focusing on high-risk concerns rather than hypothetical or low risks associated with AI to avoid placing unnecessary barriers in the way of innovation;
- being coherent such that it is easily navigable by industry; and
- being proportionate and adaptable – ie, early-stage proposals should take a light touch by issuing guidance or voluntary measures that can be more easily amended to support innovation.

Developing Your Own AI Governance Framework

Distilling the common elements of the AI governance frameworks discussed above, along with those previously articulated by the Organisation for Economic Co-operation and Development (OECD) and the EU's High-level Expert Group on Artificial Intelligence, suggests that organisations developing their own governance frameworks for AI may be well served to take into account consideration of these parameters:

- development, deployment, and assessment of relevant evidence/empirical data;
- optimisation of risks and benefits;
- transparency, explainability, accountability;
- bias, accuracy, and fitness for purpose;
- privacy and data protection;
- other social impacts;
- surveillance, disinformation and deepfakes;
- auditing outcomes (internally and externally);
- review boards, strategic oversight and internal responsibility; and
- the roles of law, regulation, guidance, ethics, and morality.

***

Developing meaningful and effective AI governance frameworks will call for careful, ongoing monitoring of the inputs and outputs of AI applications, insistence on rigorous, evidence-based scrutiny of empirical developments, and accountability for understanding, authorising and overseeing intended purposes, processes and outcomes. Technology risks must be anticipated, but they should not be presumed.

Governments, companies and civil society will all have critical roles to assure that the future of AI best serves society.

INTRODUCTION

Contributed by: Alan Charles Raul, **Sidley Austin LLP**

Sidley Austin LLP is a global law firm with 2,000 lawyers in 20 offices around the world. The firm's privacy and cybersecurity group has more than 70 professionals across offices in the USA, London, Brussels, Geneva, Hong Kong, Munich, Shanghai, Singapore, Sydney and Tokyo. Sidley Austin represents clients in a broad range of sectors, including financial services, life sciences and healthcare, tech, communications and media, information service providers, professional services and internet companies. The firm undertakes highly sophisticated legal counselling and advocacy, and provides actionable legal advice on challenging and novel questions of privacy and information law. Sidley's lawyers focus on privacy, data protection, information security, digital governance, internet and computer law, e-commerce, consumer protection, outsourcing, competitive intelligence and trade secrets, information management and records retention, and responding to cybercrimes and network intrusions. The team also handles litigation and government investigations; crisis management and incident response; compliance and regulatory counselling on all data protection laws, such as the GDPR and CCPA; legislative and policy developments; and international data transfers.

Contributing Editor

Alan Charles Raul is the founder and leader of Sidley's privacy and cybersecurity practice. He represents companies on US and international privacy, cybersecurity and technology issues. Alan advises on global regulatory compliance, data breaches, and crisis management. He also focuses on issues concerning national security, constitutional and administrative law. He handles enforcement and public policy issues involving the FTC, State Attorneys General, SEC, DOJ, FBI, DHS/CISA, the intelligence community, as well as other federal, state, and international agencies.

Alan previously served in government as vice chairman of the White House Privacy and Civil Liberties Oversight Board, General Counsel of the Office of Management and Budget, General Counsel of the US Department of Agriculture, and Associate Counsel to the President. Alan serves as a lecturer on Law at Harvard Law School, where he teaches a course on Digital Governance: Privacy and Technology Trade-Offs. He is a member of the Technology Litigation Advisory Committee of the US Chamber Litigation Center, the governing Board of Directors of the Future of Privacy Forum, and the Council on Foreign Relations.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com