IN-DEPTH

Privacy, Data Protection and Cybersecurity

EDITION 10

Contributing editor
Alan Charles Raul
Sidley Austin LLP

LEXOLOGY

Published in the United Kingdom
by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.thelawreviews.co.uk

ISBN 978-1-80449-214-7

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON LLOYD

ANJIE BROAD LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS LAW FIRM

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

JACKSON, ETTI & EDU

KALUS KENNY INTELEX

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Chapter 1

GLOBAL OVERVIEW

Alan Charles Raul[1]

For the forthcoming transformation from 'privacy' to 'digital governance', universal digital norms will be imperative.

This very year, 2023, could turn out to represent the beginning of a transformation for global regulation of 'privacy'. Given the enormous (potentially existential) implications for society of large language models, generative AI and self-teaching/self-replicating applications, GDPR cookie banners and US data breach notification letters may start to seem just a tad banal. Fortunately for privacy devotees – and human data subjects – the future of privacy may very well be grander than its past, and the present will certainly remain quite dynamic.

Going forward, though, neither 'privacy' nor 'data protection' will be fully up to the task of describing the relevant subject matter. I nominate the term 'digital governance' as a more fitting rubric to capture the need for understanding, assessment, management and integrity of ubiquitous data collection and processing algorithms, powerful learning machines, critical software quality, cyber defences in depth, autonomous and automated decision-making and other indispensable and sensitive information technologies. All this, and quantum computing waiting in the wings.

Use of the concept 'governance', and not just plain old 'regulation', is purposefully elastic. While some government rules will always be necessary, comprehensive government regulation of AI and sensitive digital technologies will not be sufficient, desirable, nor even possible. If public policymaking was ever in need of a new paradigm, the digital era surely is that time.

Protecting personal information will continue to be a very important part of this governance, but not the only area of concern. Sometimes looking through the prism of old-school personal data privacy may actually blur the substance. For example, the risks of manipulative or biased algorithms are really more a matter of digital fairness than of personal privacy or data protection.

Accordingly, new digital norms as much as clear and consistent laws and regulation are going to be essential. Companies as much as government agencies will need to be responsible; and militaries and academies will have to engage in norm development as well. Digital governance needs to show up just about everywhere. Leadership and support for the necessary norms is or soon will be the province of boards of directors, cabinet secretaries (and presidents), military chiefs of staff and university presidents. Democratic countries must achieve consensus on the governing norms, as well as on a consensus how to constrain non-democratic countries from egregious disregard of those norms.

1 Alan Charles Raul is a partner at Sidley Austin LLP and lecturer on law at Harvard Law School.

Digital governance leaders will be obligated to demand education and explanations about the opportunities and risks of the AI and sensitive technologies their organisations are using, and those that are in development for possible future deployment.

Algorithmic and automated decision-making are often largely opaque (i.e., unintelligible to humans) and surprising – even to their creators. For that reason, the governance taking place inside organisations is going to be at least as crucial as outside regulation of visible activity and outcomes. Responsible organisations will establish and continuously refine channels for internal inventorying, monitoring, testing and retesting, reporting and auditing the fitness and integrity of their digital investments, research activity and active deployments.

Corporate compliance frameworks under the venerable *Caremark* fiduciary standard will remain the lodestar for digital accountability. The substantive standards will have to include applicable laws, and evolving digital norms. There are not too many areas of public policy where reliance on internalised organisational ethics and philosophical (and perhaps also moral and cultural) principles will be as indispensably intrinsic to 'compliance' as for digital governance. If general purpose AI turns out to be as powerful as currently predicted, then organisational self-restraint based on internalised norms is absolutely vital. But for 'norms' to be sufficiently compelling to warrant internalisation, they will need to be nearly universal and essentially unassailable.

Not the easiest task in this day and age.

A promising new paradigm, however, was articulated in June 2023 by the US Senate Majority Leader Charles Schumer. He describes AI as 'world-altering', but with real dangers including 'job displacement, misinformation, a new age of weaponry, and the risk of being unable to manage this technology altogether'. Senator Schumer's 'north star' for governing AI, though, is innovation and protecting IP rights, along with regulatory guardrails that 'align with democracy'. Senator Schumer calls his initiative a SAFE Innovation Framework. 'SAFE' is an acronym for the key elements he says are necessary to assure AI safety: 'Security, Accountability, Foundations [of liberty] and Explainability'.

Senator Schumer stresses that bipartisanship is the *sine qua non* of tackling AI successfully. Perhaps this reflects a recognition that society-wide norms as well as laws will be needed, and that before norms can be universal, they need to be at least bipartisan.

The SAFE Innovation Framework is not yet codified in a legislative draft. Instead, he is calling for a 'new and unique approach' that can handle the speed of AI development. But first will come educating senators deeply – and promptly – about AI before they try to regulate it. A series of AI Insight forums, beginning in September, will guide the development of rules through a consciously bipartisan process. The forums seek to invite top AI experts to come to Congress and participate in a new approach for developing legislation. And while Senator Schumer has involved the chairs and ranking members of the relevant committees, he has also signalled the normal congressional time frame will not work for AI policy making.

The development of the technology is moving so fast that Congress simply has to move faster than it ever does, and lay aside conventional partisanship. It appears that Senator Schumer recognises that for AI governance norms to be as universally compelling, normal partisan small-mindedness and gamemanship must be suspended.

Also notable for a leader from the more traditionally pro-regulatory and precautionary side of the political aisle, Senator Schumer has emphasised not only the imperative of bipartisanship, but also the imperative to approach policy making with a mandate to protect and promote 'innovation'. This is necessary to derive the optimal benefits to society from the development and deployment of increasingly advanced applications of AI.

But identifying and dealing with the risks to society are critical too. Like many other thought leaders on the governance of AI, Senator Schumer enumerates the dangers posed by conceivable and not yet conceivable uses of AI for our national security, democratic values, economic interests in maintaining employment levels and the less existential but concrete and damaging risks of privacy abuses of personal information, implicit bias leading to discriminatory outcomes, deepfakes and other misinformation.

The overall thrust of the initiative is that AI, in the words of Senator Richard Blumenthal after attending the third briefing in August 2023, is about the 'tremendous positive benefits of AI, the variety of what AI is, and overwhelmingly the need to invest and for the federal government to be involved'.

Time (but not much time) will tell whether Senator Schumer's SAFE AI Initiative is a worthy new paradigm to address powerful digital developments. We can certainly hope it will be.

In the meantime, governments as usual have in fact generated considerable policy frameworks, blueprints, guidance and even many good ideas. And, in the case of the EU, many, many regulatory tomes and requirements.

This overview is not a place to discuss all of the different governmental governance materials, but it is worthwhile to briefly highlight some notable international developments.

As suggested above, the EU leads the pack in drafting legislation. The Digital Markets Act, Digital Services Act and AI Act, as well as the Data Act, Data Governance Act Digital and Operational Resilience Act, are intended to regulate essentially every dimension of digital, cyber and information technology. It cannot be said that each and every such proposed digital regulatory provision is misguided or suffocating, but it is likely fair to describe the overall approach as being more invested in assuring precaution than promoting innovation. Many would say this same criticism applies to GDPR. To be sure, however, the EU's focus on the need for digital operators to conduct impact assessments for deployments of data, algorithms and technology that could result in high risk to the rights and freedoms of data subjects and other humans, does not seem unreasonable in principle.

In contrast, the UK's approach to AI and digital technology has been expressly pro-innovation and more practical-minded. The intended regulatory approach is contemplated to be decentralised and sectoral (like US federal privacy law today) rather than omnibus or comprehensive. UK government papers have highlighted the following regulatory principles for AI:

a context-specific;
b pro-innovation and risk-based (with a focus on real-life application and real, identifiable unacceptable levels of risk);
c coherent (i.e., simple, clear, predictable and stable);
d proportionate and adaptable (i.e., asking regulators to consider lighter touch options such as guidance or voluntary measures);
e safety, security and robustness;
f appropriate transparency and explainability;
g fairness;
h accountability and governance; and
i contestability and redress.

Alongside the broad principles crafted by the government, the UK's Information Commissioner has published extensive, actionable guidance on AI auditing and other governance techniques for companies to consider.

The US has also been energetic, beyond Senator Schumer's initiative, in thinking about and providing guidance and practical frameworks to address AI. Specifically, in October 2022 the White House issued a normative Blueprint for an AI Bill of Rights; Making Automated Systems Work for the American People, and in January 2023, the Commerce Department's world-respected National Institute for Standards and Technology (particularly famous for its Cybersecurity Framework), published a highly functional, how-to guide: the NIST AI Risk Management Framework. Several US states are innovating with legislation around AI, profiling and automated decision-making.

In all, with the new India privacy law being adopted this year, the proliferation of new US state privacy laws, the prodigious DMA/DSA/AIA/DA/DGA/DORA, etc., work product from the EU, and the first-principles approach to AI from the White House and Congress (with a very practical assist from NIST), 'privacy' compliance and digital governance will capture ever more enormous commitments of research, deployment and compliance investments by companies around the world this year and for a very long time.

A further closing thought on the prospect for a global, democratic consensus on universal norms for AI: it has never been clearer that free countries are facing dangers from hostile authoritarian states that are particularly keen – and expert – in manipulating digital technologies to attack 'the West' with misinformation, deep fakes, cyberattacks and other intrusive and abusive digital conduct. And they use such techniques to subjugate and oppress their own peoples as well. But as Russia's invasion of Ukraine has (most recently) taught, united alliances can and will rise above mundane differences to protect their fundamental interests when they need to.

Alignment of values and practices in the digital realm, therefore, will be intrinsic to developing consensus on critical, universal norms for AI and sensitive digital technologies.

There is ground for hope.

For example, in December 2022, under the auspices of the Organization for Economic Cooperation and Development (OECD), in a Declaration on Government Access to Personal Data Held by Privacy Sector Entities, 38 OECD democracies and the EU agreed that they shared more in common regarding fundamental commitments to the rule of law, privacy and limits on governmental electronic surveillance, than separated them in terms of bureaucratic differences on how to regulate data protection.

The principles expressed in the recitals to the OECD Declaration could constitute a role model for how the development of universal norms on acceptable AI could be realistic. Here are some key excerpts from how the OECD democracies approached the governance of electronic surveillance bases on 'common values':

> *WE RECALL our shared commitment to upholding democracy and the rule of law, protecting privacy and other human rights and freedoms, promoting data free flow with trust in the digital economy, and maintaining a global, open, accessible, interconnected, interoperable, reliable and secure Internet.*
>
> *WE RECOGNISE that ongoing digital transformation is creating more data, including personal data, as digital technologies are used across all sectors of the global economy.*

WE FURTHER RECOGNISE the central role of data in the functioning of our societies and economies, and that cross-border data flows underpin international trade and global commerce and economic co-operation and development; greatly contribute to innovation and research and development across sectors; and are necessary to conduct business and to advance economic and societal goals.

WE RECALL the 1980 Recommendation concerning OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, last revised in 2013 [OECD/LEGAL/0188] (hereafter, "OECD Privacy Guidelines"), which provides a basic common reference point for the protection of personal data, whether in the public or private sector, and promotes and facilitates the transborder flows of personal data while upholding democratic values, the rule of law and the protection of privacy and other human rights and freedoms.

WE RECOGNISE the sovereign duty and responsibility of every country to protect the safety of its population by preventing, detecting and confronting criminal activity and threats to public order and national security, in adherence to democratic values, the rule of law, and the protection of privacy and other human rights and freedoms.

WE ACKNOWLEDGE that government access to personal data held by private sector entities is recognised in our national legal frameworks as essential to meeting these sovereign duties and responsibilities, and that law enforcement and national security authorities are therefore vested with powers to lawfully access such data.

WE REJECT any approach to government access to personal data held by private sector entities that, regardless of the context, is inconsistent with democratic values and the rule of law, and is unconstrained, unreasonable, arbitrary or disproportionate. Such approaches violate privacy and other human rights and freedoms, breach international obligations, undermine trust and create a serious impediment to data flows to the detriment of the global economy. By contrast, our countries' approach to government access is in accordance with democratic values; safeguards for privacy and other human rights and freedoms; and the rule of law including an independent judiciary. These protections also contribute to promoting trust by private sector entities in meeting their responsibilities in this context.

WE EMPHASISE, taking into account the justified exceptions to the OECD Privacy Guidelines on grounds of law enforcement and national security, the importance of enhancing trust based on a common understanding of the protections that our countries apply when accessing personal data held by private sector entities in these circumstances.

WE RECOGNISE that our existing practices and safeguards, in this regard, while not identical to one another, are founded upon similar principles that reflect a shared commitment to protecting privacy and other human rights and freedoms.

WE NOTE stakeholders' calls for additional work and engagement to identify existing common safeguards in OECD Member countries to protect privacy and freedom of expression, and therefore

> *promote trust, in the context of purchasing commercially available personal data, accessing publicly available personal data, and receiving voluntary disclosures of personal data by law enforcement and national security authorities.*
>
> *WE REITERATE our ambition to build a shared understanding among like-minded democracies of protections for privacy and other human rights and freedoms in place for law enforcement and national security access to personal data held by private sector entities in order to better inform efforts to promote data free flow with trust.*

If the OECD Declaration in December constituted a consensus in principle on the important norms for electronic self-restraint by democratic governments, the EU–US Data Privacy Framework (DPF), finalised in July 2023, represented a consensus on similar issues in practice. The US and EU agreed they share and reciprocate substantially the same values on privacy digital transfers of data across the Atlantic – despite the shallow differences that are in reality swamped by common values.

If the OECD Declaration in December constituted a consensus in principle on the important norms for electronic self-restraint by democratic governments, the EU–US Data Privacy Framework (DPF), finalised in July 2023, represented a consensus on similar issues in practice. The US and EU agreed they share and reciprocate substantially the same values on privacy digital transfers of data across the Atlantic – despite the shallow differences that are in reality swamped by common values.

On AI, there has been important, recent consensus to take action at the highest international level. On 7 September 2023, the leaders of the G7 group of democracies agreed to create an AI international code of conduct. While the guidelines will voluntary, the resulting principles on generative AI and other sensitive technologies could form the basis for unified, and thus universal, norms for AI governance. The G7 specifically committed to working together with companies to stop potential harms to society created by new deployments of AI, and to establish risk management systems to govern potential misuse. Output from this process could be expected as soon as November 2023.

This recent consensus on fundamental standards and reciprocity of obligations was achieved on digital data transfers across border by democracies choosing to act in alignment with their most important, fundamental principles, and of course manifest self-interest. The same alignment and self-interest may allow democracies to govern AI in the overall best interest of humanity.

ISBN 978-1-80449-214-7