# Dining out on Data: Ethics, Value, and the Calculation of Risk Appetites

# Tsvetelina Hristova and Liam Magee

Data ethics and AI ethics constitute an increasingly contested terrain where scholars, activists, state institutions, and industry actors compete to define principles for ethical practice. While mechanisms like state-sanctioned ethical frameworks, activist- and scholar-led initiatives like the FAIR data principles,[[1]](#footnote-1) and industry projects like Microsoft’s Aether Committee have been widely discussed, international standards, as one of the governmental technologies that influence how data ethics is understood and practiced, remain largely out of the focus of researchers. In this chapter, we examine the role of a series of interconnected standards on risk management that have grown to play a significant role in shaping a particular understanding of data ethics.

We begin with an introduction to several of these global standards, whose connections to each other and to precedent national standards can be difficult to untangle. Based on the Australian and New Zealand standard for risk management AS/NZS 4360-2004, which serves as the foundation for the international standard for risk management ISO 31000, these standards codify a specific relationship between risk and value. This relationship foregrounds how states and industry actors imagine the social dimensions of data use as well as their own role in the global digital economy. The Australian standard AS/NZS 4360-2004 and ISO 31000 introduce a new framework of risk management, where risk is conceptualized as ambivalent: positive in some cases and negative in others. The ambivalence of risk leads to an approach to risk management based on the ‘risk appetite’ of organizations and institutions — i.e. their readiness to take risks informed by expected gains. This framework of risk management is incorporated in the work of the new ISO subcommittee ISO/IEC JTC 1/SC 42, which develops standards for artificial intelligence. ISO/IEC JTC 1/SC 42 is part of a larger initiative for the development of standards for AI led by a special sub-committee of the joint technical committee for standardization in the field of information and communication technologies, JTC 1. JTC 1 formed in 1987 to combine standardization efforts of two major international standard bodies, the International Standards Organisation (ISO) and the International Electrotechnical Commission (IEC). The ISO/IEC JTC 1/SC 42 sub-committee, formed more recently in 2018, has been tasked with the role of developing standards in the field of artificial intelligence. The significance of such a project cannot be underestimated — IEC and, in particular, ISO have established what scholars have termed a ‘global governance by consensus’,[[2]](#footnote-2) and their respective global standards impact most industries through the need of compliance in a multitude of ways. As part of the series of standards developed by the subcommittee, the group is also working on a standard of risk management in AI, ISO/IEC DIS 23894, which is explicitly based on ISO 31000 as stated in its introduction:

This document is intended to be used in connection with ISO 31000:2018. Whenever this document extends the guidance given in ISO 31000:2018, an appropriate reference to the clauses of ISO 31000:2018 is made followed by AI-specific guidance, if applicable. To make the relationship between this document and ISO 31000:2018 more explicit, the clause structure of ISO 31000:2018 is mirrored in this document and amended by sub-clauses if needed.[[3]](#footnote-3)

Beyond the mere replicability of standards, the case of ISO 31000 suggests an emerging socio-technical configuration where risk becomes conducive to how ethics and governance are imagined and enacted in relation to data subjects. Users and companies alike are imbued with inherent ‘risk appetite’ that allows for varying degrees of contingency to be permissible in the context of big data and AI and charts the boundaries of expected and allowed data practices. Data subjects also become implicated in the complex interplay between technological standards and the geopolitical ambitions of nation states; an interplay in which the purpose of local data and AI regulation is to serve as a testbed for global frameworks of governance.

Standards occupy a complex position with regards to this political and economic space. Keller Easterling[[4]](#footnote-4) uses specifically the example of ISO to propose the concept of ‘extrastatecraft’: a characterization of technological and economic mechanisms for the rearrangement of relations of power, control, and production that are not guided exclusively by nation state governments and that can reshape the political structure and the spatial dimensions of power within and across states, cities, or continents. Andrew Barry[[5]](#footnote-5) makes a similar argument, suggesting the notion of technological zones which are defined not by the traditional political power of state governments but by complex technological infrastructures and relations. For both scholars, the play of forces within networks of extrastatecraft and technological zones is shaped by the interconnectedness of technical infrastructures, protocols, and economic and political power. Standards occupy this extrastatecraft space of regulation outside of the norms of political governance by forging alliances between companies and state institutions, and by introducing the principles of consensus-making and technical constraints as modes of exercising control and shaping a space that enables certain economic flows and relations while restricting others.

While their explicit entanglement with ethics is comparatively recent, technical standards have long formed a key part of the socio-technical assemblages[[6]](#footnote-6) within which data is defined and put to use in different calculations and statistical operations. They have historically played an important role in how data infrastructures and networks are governed,[[7]](#footnote-7) how different digital file formats are defined[[8]](#footnote-8) and how the key principle of interoperability, which allows for the circulation of data across different systems, is conceived and enacted.[[9]](#footnote-9) Standards have been instrumental in generating the conditions for big data collection, exchange, and analysis. And as we have noted, alongside their role in defining data formats and network infrastructures, in a more general sense standards occupy an ambiguous space where they shape political and economic processes through what are essentially ‘extrastatecraft’[[10]](#footnote-10) methods of consensus-building and technocracy. We see standards like ISO 31000 as part of the complex and shifting socio-technical assemblages of data and algorithms through which the relation of data to risk is determined. While data has been extensively studied as part of the instrumentarium of risk management in algorithms for preemptive control and policing),[[11]](#footnote-11) ISO 31000, through the new AI standard ISO/IEC DIS 23894, positions data and AI themselves as objects of risk evaluation and mitigation.

These standards are instrumental in articulating a relationship between risk and value which, as part of the socio-technical regime of control that standards establish, becomes increasingly important for how data use and ethics are imagined, and for how institutions and states see their role in the governance of big data and AI. As we discuss below, one interesting aspect to the control extended from the technical to the imaginary is the standardisation of a ‘risk’ vocabulary. For example, a significant role in this process is afforded to the construed notion of ‘risk appetite’, and to related terms, which together forge an alternative institutional imaginary, one that already devotes to data a distinctive moral as well as economic agency.

The new ways in which risk features in the calculation of how to govern and benefit from a digital economy have consequences for how it is understood and operationalised across different domains and by different geopolitical actors. This is especially notable in the technologies of ‘governing through consensus’, such as standards and guidelines, which allow room for negotiation and translation of practices across the domains of private business, national agendas, and international collaboration and influence. The case we focus on here, the risk management standard ISO 31000, is a prominent example in this sense, not only because it reaffirms the language of risk-taking and risk appetite as essential for successful governance but also because the life of this standard reveals the stakes and hopes that underpin the formulation of guidelines for ethics and risk in AI.

As an international standard, ISO 31000 becomes a signifier for a new way of carving out influence and leadership in data-intensive industries, through the development and lobbying for standards and ethical norms by different national or local actors. It suggests that risk, along with its changing meaning and functions, exercises transformative effects not just through the adoption of the principles of risk appetite, but also through the specific geopolitical and geoeconomic ambitions that lie at the heart of initiatives for standard-making. Contrary to a colloquial understanding of technical standards as ones grounded in the objectivity of measurements, science, and rationality, standards do play an important role in shaping and articulating geopolitical and geoeconomic ambitions and borders. Even when standards are developed by non-governmental bodies, the geographical origin of the standard and the composition of the organisation behind it are seen as representing specific national interests. As we show elsewhere about cases where technological standards have been utilised in geopolitical and geoeconomic struggles,[[12]](#footnote-12) political state power and technological zones are often entangled in shaping and reshaping the reach of a standard. The perception that certain countries gain influence by the international adoption of standards supported by them is very much part of how these entanglements are enacted.

## Standardizing Risk in the New Data Economy

Risk has traditionally been conceptualized in a range of ways, according to the scale and site of its application. One well-accepted definition comes from disaster management: a combination of *hazard*, *exposure,* and *vulnerability.*[[13]](#footnote-13) Organizational risk is often defined in similar terms: as a combination of *likelihood* (comparable to hazard) and *severity* (combining exposure and vulnerability). But risk is seen to have a much more profound role in social and political life. For example, Georg Simmel in *The Philosophy on Money* connects risk to an essential relation between abstract economic value and a social register of trust. He argues[[14]](#footnote-14) that in economies of currency and credit, where there is an underlying element of uncertainty (or social risk), trust becomes an integral part of how value is produced by constructing the necessary context of an ethics of sociality that can accommodate and offset the dangers of risk-taking. Reflective of the ways risk was later to become itself the explicit object of organizational attention, Ulrich Beck[[15]](#footnote-15)argues risk management has developed as a defining feature of governance in the postmodern age. Risk positions, he argues, supplant class positions as the key to contemporary existence and the production, management, and containment of risk have come to replace earlier governmental concerns with value and value distribution.

In the past two decades, in managerial discourse and in the family of standards related to ISO 31000, risk now appears as an ambivalent rather than purely negative presence. ISO 31000 establishes a terminology where risk is defined as an ‘effect of uncertainty on objectives’ and further explained as being ‘a deviation from the expected [... that] can be positive, negative or both, and can address, create or result in opportunities and threats’.[[16]](#footnote-16) This interpretation, widely adopted thanks to the significant clout of the International Standards Organisation, casts risk as a field of uncertainty that can be productive of gains and value for companies and institutions. The allure of risk reaffirms the core objectives that the standard sets for the principles of risk management: value creation and protection.

If risks create opportunities, then there is an imperative to pursue risk-taking. The accompanying ISO Guide 73:2009 formulates this imperative through the concept of ‘risk appetite’—‘the amount and type of [risk](https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en:term:1.1) that an organization is willing to pursue or retain’.[[17]](#footnote-17) In the subsequent interpretation of risk appetite by the global consultancy firm Deloitte[[18]](#footnote-18) the metaphor of consumption is taken even further, and becomes integrated into a framework of different levels of risk that leave a company either hungry, satiated or overfed with the amount of risk it takes on. However strained, the digestive metaphor reminds us of the historical figurations of the economic organization *as a body*: a corporation that is also corporeal, that lives and breathes, that warrants its own legal protections, and that consumes even as it produces. Even the language of university risk management statements can illustrate how closely its governance resembles a comparable decision-making framework to gambling consumption: calculating odds, then placing bets on low or high-risk outcomes depending upon an organizational appetite.

The adoption of these concepts of risk appetite and risk tolerance in the global ISO 31000 standard becomes a replicable model in all other standards related to risk management, including the standard for information technology security management ISO/IEC 27001 and the abovementioned standard for risk management in AI. The notion of risk and the parameters of risk management in the context of national, corporate and international governance have been significantly transformed by this standard, which introduces new understanding of how risk should be handled. The concept of acceptable risks and risk appetite also becomes influential in the way public institutions think of their duties with regards to state-collected data. For instance, the 2017 *Data availability and use* report published by the Royal Productivity Commission in Australia largely encourages the sharing of data between public and private entities and, specifically, the sharing of public datasets for the purposes of encouraging the economic growth and innovation in the local digital industry. Notably, it builds its argument for a more liberal approach to data sharing around the notion of risk appetite and the increased tolerance of risks related to the sharing of personal data in society. The report argues that as societal standards of privacy have shifted—due in no small part to the role of social media companies in normalising new practices of data sharing—so federal agencies should also adopt greater organisational risk in the sharing of data.

The emergence of AI risk management standards related to ISO 31000 suggests an intensification of attention to data and its value. Yet the economisation of data—by which we mean here the production of value, measured either through direct financial gain or through indirect reputational, HR or political benefit—is by no means novel. We situate our discussion here with the emergence of AI in the 2010s from its so-called ‘winter’ in prior decades. According to LeCun,[[19]](#footnote-19) Chief Scientist at Facebook and a pioneer of AI, this emergence was the product of an alignment between hardware (specifically, the adaptation of GPUs to parallel data processing), software (open source libraries like Facebook’s *PyTorch* and Google’s *TensorFlow*), research refinements (in particular, the use of neural networks, stochastic gradient descent and back propagation) and the accumulation of large text, image and other media data sets. For technology companies like Facebook, Google, Baidu, and Alibaba—leaders in AI research as well as, by far, the largest monetizers of online advertising—the connections between data and value materialize both through the efficiencies of delivering relevant ads to consumers, and through the range of AI-driven services, from search results to content moderation, they offer to those consumers. Less conspicuous in terms of value is the ability to secure prominent data scientists, like LeCun and Geoffrey Hinton (Google), on the promise of being able to work with massive data sets to solve social and computational problems and produce ‘state-of-the-art’ AI research. In a period where the algorithmic paradigm appears to be shifting from large code bases to smaller code models training on plentiful data, the prevalence of data not only serves to produce economies of scale and differentiate organisations to advertisers and consumers, but also functions as a key HR attractor.

For the new titans of capitalism, and indeed for other private and public institutions, the governance of data is core business. Its very presence also produces risk to the value it creates. Data can be stolen, revealed, misused, corrupted, ignored, and skewed. Though far from the only subject for risk management, the centrality of data to organisational operations has meant that it is no less critical to the progressive formalization of risk through procedures, reviews, and standards in the twentieth and twentieth-first century.[[20]](#footnote-20) And varied data crises, from famous security breaches to the mobilisation of social network graphs for targeted political messaging,[[21]](#footnote-21) also have inadvertently produced an avowedly ethical organisational subject, committed through terms, conditions, principles, charters, pledges, policies, and standards to protecting data within its orbit of control. As we argue here, at the same time as this subject places its ethics on display as one among so many paraded virtues, it also prepares for it to be placed at risk in the production of value. Thus, the growing number of initiatives for the development of ethical frameworks of AI are not necessarily indicative of an attempt to minimise the risk of data harms. On the contrary, they can similarly speak of a turn towards embracing and socialising these risks.

This changing landscape of how risk is operationalized in the data economy and in the regulation of AI means that we are faced with a different constellation, in which notions of ethics are established and enacted. In this new context, data, automation, and artificial intelligence are not just reinforcing a mode of governance devoid of doubt and uncertainty.[[22]](#footnote-22) They are also deployed in economies of risk where risk is acceptable within certain levels and is even sought after because of the crevice of uncertainty and ambiguity it opens and the possibilities for economic gain and other forms of value to be realised from it. This characterization resonates with early theorizations of the relationship between risk and entrepreneurship, innovation and capital, as argued, for example, by Brouwer,[[23]](#footnote-23) who discusses the varied characterizations of the risk-taking entrepreneur by Weber, Schumpeter and Knight. But whereas these theorists, and despite their differences, each imagined early-stage capitalist risk eventually giving way to the rationalistic and monopolistic late-capitalist organization, in the present data economy it is possible to see risk as being deliberately reinjected by those organizations themselves, as a sort of energizing device to lift flagging rates of profit. In other words, risk is a feature of established and highly rationalist market incumbents as much as of disruptive entrepreneurs.

With the adoption of risk appetite by economic actors, ethics becomes key for negotiating the boundaries of extractivism and profit-making with regards to a highly socialized resource like data. This is done not only through an obvious contention with ethics codified into law and governance (see below, where we discuss Floridi’s distinction between hard and soft ethics), exemplified in the numerous cases of law-skirting and infringement by Facebook, Google, and other actors. It is also evident in the corporate territorialization of the ethical field itself: developing AI ethics groups, making interventions in scholarly and activist debates (e.g. Facebook’s FAIR group, or Microsoft’s Aether committee), and developing the very standards by which AI and data use is judged and governed.

As we have argued, attempts to define what ethics of artificial intelligence entails are indicative of the role that ethics acquires in the international competition for AI leadership. The example of ISO 31000 and its provenance from a local Australian standard to a global standard whose model is replicated and referenced is a case in point: it not only shows the geopolitical stakes of exerting influence over the framing of key concepts related to risk and ethics, but also demonstrates that infrastructures like standards can operate alternately as extrastatecraft and as advancing the interests of specific nation states.

## Risk Infrastructures and the Geopolitics of AI Ethics

The case of ISO 31000 feeds into a particular national imaginary and geopolitical ambitions in Australia. Since the notion of risk outlined in the Australian standard for risk management AS/NZS 4360:2004 has been adopted in ISO 31000, it forms the basis of subsequent interpretations of risk in the text of documents regulating the use of artificial intelligence and, specifically, the risk management standard ISO/IEC 23894 and the standards for trustworthiness of AI.[[24]](#footnote-24) This connection serves as a sort of claim of the Australian state of its involvement in shaping the global regulatory frameworks of artificial intelligence and provides a paradigmatic model for how to reproduce and assert this type of influence again. Standards Australia itself is part of the working group of ISO/IEC JTC 1/SC 42 and has, in addition, established a local Mirror Committee IT-043 that replicates the work on the international one and introduces the finished standards to Australia. The composition of the local chapter and the statements of Standards Australia can lead us to assume that acquiring a distinctive profile in shaping the ethics of AI is one of the key objectives of Australia in the international committees. It is indicative of these ambitions that the chair of the Mirror Committee, Aurelie Jacquet, is heavily involved in work on ethics and trustworthiness of AI. As she explains, ethics and the establishment of ethical norms and regulations form a central part of the tasks of her group.[[25]](#footnote-25)

This novel extension of standards into the domain of the ethical may be welcomed, as an acknowledgement of the work by many critical scholars and activists to foreground ethical considerations in AI. But the case of ISO 31000 and the ambitions around it reveal how the extrastatecraft space of technological zones can be imbued with local national aspirations. Through these entanglements, risk is operationalised and incorporated within new geopolitical constellations and economic objectives with respect to AI and its emerging ethical frameworks. In some of its latest documents, the Australian standard-setting organisation—Standards Australia (SA)—outlines a very specific path for the country to claim leadership in the AI innovation space. In its 2020 report *An Artificial Intelligence Standards Roadmap: Making Australia’s Voice Heard,* SA argues that Australia can take a different path to ensuring a leading position in the emerging economy through leading the development and implementation of standards, especially ones concerned with risk and ethics. The document discusses this possibility through the language of international markets, outlining the fact that Australia is not in a position to export AI technology, which is the more obvious path to gaining clout and prestige in the global AI race. Musing on this perceived deficiency of the national AI industry, SA sees the export of standards and guidelines as an alternative economic and political strategy. It specifically sees the example of ISO 31000 as a case that can be replicated in the future—a homegrown standard that is exported and becomes an influential global standard. The reference to the ISO 31000 model suggests that, in the development of AI strategies and standards, risk is operationalised not only as a concept but also through already existing models of capitalising on frameworks of risk management. The standard for risk management is seen as a model that should be replicated—as a case of exportability and, importantly, as a case of rethinking the role and function of the nation state in international politics of standard-making.

This last point is a key part of the deliberations of SA. The idea of exporting a standard is articulated through the possibility of construing Australia as a test bed for the development of new standards:

International Standards continue to provide the optimal channel for the design, development, deployment and evaluation of AI in a consistent manner. However, given the significant activity being undertaken within academia, consulting and some businesses on proposing, developing and trialling approaches to risk management and auditing of AI systems, there is an opportunity to codify some of these learnings, producing documents that can attest to Australian expertise, experience and workable solutions. This might subsequently form the basis for an International Standard. There is precedent for this, with Australian stakeholders having played a significant role in the development of AS/NZS 4360 (Risk Management), which was subsequently refined and adopted as an International Standard (ISO 31000:2009, Risk management – Principles and guidelines). A dedicated hub within Standards Australia, which brings disparate expertise together, would be the best way to achieve this. It could provide a test-bed, of the kind alluded to in the NIST Roadmap, where specific propositions, which could form the basis of content for Standards, could be tested with industry and other stakeholders.[[26]](#footnote-26)

By entertaining the possibility of framing Australia as a test bed or an experimental hub for the development of global AI standards in areas like ethics and risk management, SA suggests a model that itself operationalises risk at multiple levels. The very idea of treating the country as a test bed is ridden with the contentious relationship between experiment and risk. Melinda Cooper[[27]](#footnote-27) in her work on clinical trials and experimental labor argues that post-Fordist capitalism embraces a new political economy of risk that, especially in the IT and biomedical sectors, reframes risk as a source of value. This new approach to risk ties together experiment, innovation and the surpluses unlocked by the risks that workers and experimental subjects are expected to undertake. Cooper’s conclusions may appear less relevant in a comparatively highly regulated nation like Australia, with respect to the fields of health and medicine. However, in nascent economic domains like data extraction, the country’s combination of relatively poor protection and high digital uptake make it an ideal site for experimentation. We can easily see how the ambition to establish Australia as a test bed for standard development and the notion of risk appetite introduced by SA in 2004 are both consistent with this new economy of risk and experiment in late capitalism—an economy characterized by distinct geopolitical contours that enable capital to exploit specific ideal meeting points of regulatory environment, data accumulation, and declared ‘risk appetite’.

The proposition of SA does, however, also introduce a new understanding of how the state relates to its subjects through a reconceptualization of risk as a technology of governance. Namely, this reframing happens through the notion of a test bed for innovation—an idea that has long found wide acceptance in the IT industry through various forms of launchpads, innovation hubs, and other experimental zones supported by state governments. The state as an experimental space carries the legacy of the entanglement of risk and containment that is at the heart of the very foundation of Australia as a settler colonial state and a penal colony,[[28]](#footnote-28) and echoes other ‘radical’ policy experiments in the 2000s and 2010s with border control and mandatory detention, disastrously exported to Europe and other zones where human travel has become increasingly surveilled and militarized. Indeed, the standardization of risk management produces a generalizable model of political and economic calculation that can traverse institutional types (state, corporate, supranational, or otherwise ‘extrastate’) as well as objects of calculation (both human subjects and human-related electronic data about them). What is significant here at a geopolitical level is the role of middle-power countries that seek to embed themselves into the dynamics of AI superpower rivalry by performing specific critical functions, such as the elaboration of technical standards, that also can be framed within these high-risk manoeuvres as benign and politically neutral.

In this context ethics acquires a specific role as part of a complex tripartite market device that relates it to risk and value. In policy documents and standards-setting efforts the need to regulate AI and impose some level of ethical oversight through concepts like trustworthiness and ethics is tightly linked to the ambition of claiming leadership in the global space of AI economy. In 2019, the National Institute for Standards and Technology at the US Department of Commerce claims that ‘United States global leadership in AI depends upon the Federal government playing an active and purpose-driven role in AI standards development’.[[29]](#footnote-29) This entanglement of standard-building and leadership in AI is echoed in a 2020 report of Standards Australia where the notion that standards can help shape national leadership in the field of artificial intelligence is reinforced in the title: ‘An Artificial Intelligence Standards Roadmap: Making Australia’s Voice Heard’. A similar ambition is expressed in the Digital Strategy of the European Union where the proposed legal framework on AI is seen as a means to ‘position Europe to play a leading role globally’.[[30]](#footnote-30) Albeit not directly articulated in the same terms, the Chinese Ethical Norms for New Generation Artificial Intelligence (The National New Generation Artificial Intelligence Governance Specialist Committee 2021) are also largely interpreted in Western analysis as a sign of leadership ambition in the field of machine learning and artificial intelligence on the side of the government of China.[[31]](#footnote-31)

These documents articulate national and regional ambitions for leadership in innovation in a global territoriality mapped across the still-emerging contours of machine learning and automation. At the same time, through definition, standardisation and operationalisation these frameworks also act to construct implied universal parameters of AI ethics that define and serve to hedge the risks that crystallise along these frontiers of innovation. Less a contradiction, these two purposes organise a specific relationship between ethics and risk. Moreover they help to explain why middle powers like Australia can occasionally receive such prominence in standard-setting arrangements: comparatively out of sight, they act as testing grounds or laboratories where successes can be scaled up through negotiations with countries with major technology interests, like China, the US, and the EU. Countries sponsoring such experimentation benefit through direct ‘breakthrough’ technologies (like WiFi in the case of Australia) and temporary elevation from periphery status in cycles of technological innovation.

Nonetheless, standard-setting arrangements for ethical AI, and AI for the most part unfold close to centres of research and development. This link between a leading position in the economy of data and the construction of specific parameters of what ethical AI is does not act to inhibit, for the most part, corporate profiteering through the mining of data and training of machine learning models. Rather they articulate a set of coordinates through which corporate actors especially are expected to navigate. Nor do nation states simply imprint standards; as the otherwise widely diverse circumstances of Chinese and US government oversight and interrogation of technology firms like Alibaba, Tencent, Facebook, Google, Apple, and Microsoft show, such coordinates are capable of being multiplied, repositioned or re-emphasised, as the calculations of what we identify as the tripartite risk-ethics-value equation between regulatory and corporate actors are seen to diverge.

Roxana Radu[[32]](#footnote-32) notes that ‘[t]he countries hosting technology industry giants have taken the lead, with the ambition to dominate AI development at the global level in the next decade.’ The ambition to claim leadership in the AI market through regulation is paradoxical and conflicting, and reveals the uneasy interdependencies between national government and multinational tech giants. It is not always clear what local initiatives with global ambitions, especially in the field of developing trustworthy, fair, responsible, or ethical AI, aim to achieve: market regulation, government oversight, or geoeconomic dominance through technocratic means. Nor can domestic agitation, including criticisms of technology overreach, which in the US has been voiced on both left and right side of politics, be ignored, even when the results of such agitation may appear to constrain nationalistic ambitions. A further paradox of calls to regulation has been the guarded support of those corporations most likely to be affected. CEO of Facebook, Mark Zuckerberg, has for example endorsed greater government oversight of his company’s operations, no doubt aware that the costs of regulatory compliance are much easier borne by market incumbents and can be controlled both through investment in standards bodies and political lobbying. The roundabout logic of this endorsement inverts the public–private logic of the early Internet described by Birnhack and Elkin-Koren,[[33]](#footnote-33) where states mobilized private firms registered within their jurisdictions for regulation and governance of the then-emerging cyberspace. Facebook’s call for regulation asks for a reciprocal form of protection, in a situation where risks of non-compliance (such as fines) are relatively easily borne, and can be offset by an assumed greater public trust, once appropriate legislation is enacted. As scholars have argued, the support of Big Tech for ethics guidelines and norms suggests that ethics had become instrumentalized as a means to avoid—or just as likely, to steer—government oversight and regulation.[[34]](#footnote-34)

The European Union General Data Protection Regulation (GDPR) has already proved the cross-border impact of legislative instruments and standardisation attempts that are focused on data and digital technologies.[[35]](#footnote-35) GDPR’s repercussions for companies around the world is enabled through the specific scope of the EU legislation—it applies to data of EU citizens—and the difficulties, especially for smaller organizations, to enforce differential rules for each individual user of platforms and web services that are global in their reach and use. The GDPR model has shown that local initiatives for the regulation of digital technologies and innovation can shape the global geopolitical and geoeconomic landscape for the data industries, establishing a national or supranational state actor as a leader—not just in a symbolic sense but also by having real impact on the digital economy. As Metzinger argues[[36]](#footnote-36) from ‘inside the tent’ of AI ethics guideline development, the ambivalence of single nation-states like the US and China – regulating but also complicit in backing corporations with strong national affiliations – actually mean it is incumbent upon supranational or federated groups to build such guidelines for the rest of the world to follow.

At the same time, the example of GDPR and its effect on digital innovation complicates the notion of what geopolitics is in the current environment. The EU legislation has had some contradictory consequences in terms of reconfiguring political and economic power. On one hand, it is largely seen as establishing the influence of the EU and what is termed ‘European values’ on the future development of data-based innovation.[[37]](#footnote-37) On the other hand, and as a concrete case of the paradoxical effects of regulation we note above, GDPR has had the unanticipated consequence of consolidating corporate power and monopolies in the digital space by forcing some of the small actors out of competition, due to the added weight of monitoring for privacy compliance.[[38]](#footnote-38) Johnson, Shiver, and Goldberg note that the introduction of GDPR, shortly after its adoption, led to a drop in the number of web partners of tech giants like Google and Facebook and to an increase of the market share of these big corporations.[[39]](#footnote-39) This example of (perhaps) unintended market consolidation caused by the GDPR underscores the complexities of a multitude of actors involved in the development of data regulation and impacted by national, regional and transnational initiatives.

There is a comparable ambiguity in the role of geopolitical actors in the case of China. Chinese initiatives for regulating artificial intelligence and the ethics of data use and machine learning are often interpreted through the notion of a monolithic one-party state. However, the constellation of actors is more varied. The Chinese strategy for AI development entails coordination between central and local government, as well as select ‘national champion’ companies like Alibaba, Baidu, and Huawei.[[40]](#footnote-40) Notably, the *Ethical Norms for the New Generation Artificial Intelligence* published by the Chinese government in late 2021[[41]](#footnote-41) incorporate the rules of market competition as part of the ethical production and supply of AI—rules that can be interpreted in various ways but indicating regardless mixed political and economic agendas that underpin the understanding of what ethics is. While the effects of this and other Chinese state actions has led to a withering away of the market capitalization of firms like Alibaba,[[42]](#footnote-42) they seem directed as much to the alignment of corporate with state interests—in for example the ‘self-sufficiency’ of China’s semiconductor supply, an area in which Alibaba has made recent surprising in-roads[[43]](#footnote-43)—as to the establishment of greater competition or the pursuit of ‘common prosperity.’[[44]](#footnote-44)

The varied cases of regulation seek to enshrine equally varied ideas of ethical data governance. Indeed, Luciano Floridi[[45]](#footnote-45) suggests that we need two notions of ethics when analyzing data and AI ethics: hard (or normative) ethics and soft (or post-compliance) ethics. Soft ethics operates within the parameters of existing legislation and the feasibility of adhering to legal and moral norms of action. It entails calculation and compromise, and is openly motivated and constrained by existing political and economic realities. While Floridi links soft ethics to an evolutionary development of governance systems and places EU at the helm of political entities where soft ethics can be applied without compromising human rights, his distinction between ethics as moral philosophy and ethics in the context of legislative and technocratic norms of compliance and regulation reveals one important aspect of data ethics and AI ethics that we draw upon. Ethics in the field of digital technology and AI is increasingly reshaped and defined by initiatives for regulation and self-regulation of the industry. This development points to the contested political terrain within which a notion of the ethical is constructed; one that has also shaped the normative concepts of western moral philosophy that are often seen as universal and remain unquestioned. Indeed, Floridi’s high regard for GDPR can be seen to further the perception of a deceptively universalist morality at the expense of a disregard for the emergence of locally informed and politically grounded principles of data ethics such as Indigenous data sovereignty. The Eurocentricity of moral philosophy has been criticised from multiple standpoints with authors like Rosi Braidotti, Nikita Dhawan and Homi Bhabha[[46]](#footnote-46) questioning the assumptions of universal applicability from the perspective of feminist, posthumanist, and postcolonial studies. Paradoxically, the emergence of industry-led notion of data ethics serves as yet another reminder of the inherently political work of establishing a field of ethical practice and the categories that define it. In the case of ISO 31000, we see a notion of ethics construed in relation to two other key concepts of political and economic governance: risk and value.

## Conclusion

The operationalization of risk and ethics in the socio-technical infrastructures of standard-making and legislative documents suggests that states, companies and supranational organisations navigate and construct a new geopolitical framework of what ethics, risks and their mediation, through devices of control and management, entail. We argue that value stands in a kind of paradoxical relationship to these other terms. On the one hand, it works to destablise any geopolitical sureties underpinned by standards, producing new vectors of risk operation and putting into question the possibility of universal ethical principles. On the other, value in its various determinations—economic for corporations, geopolitical for states, and, at least within a literature devoted to the benefits of AI, epistemic for those whose data might, in the hands of medical, legal, or consumer institutions, be wrangled into more accurate predictions—also prepares the ground upon which risks can be taken and ethical principles prepared. Together, these three concepts and their shifting configurations help organize the marketplace of data exchange and algorithmic production.

In the context of AI regulation, this interrelationship operates through two distinct conceptualizations of risk. First, in algorithms and tools of risk management, preemptive control, and profiling, AI is articulated as a technology to eliminate risks.[[47]](#footnote-47) Second, through the notion of ‘risk appetite’, AI enters into ambiguous relations of tolerable levels of risks to individuals, communities, and nation-states, which are justified as part of the striving for leadership and innovation in the field of machine learning and AI. As productive agents in this new economy, risks of harms generated by data-supported decisions and systems motivate the capitalization of risk itself, a move that, though different in practice, is consistent with the operationalization of risk in finance.[[48]](#footnote-48) This operationalization appears to be part of the framework of financial and social behaviour of organisations in handling big data, and to that extent, every case of data breach or data harm helps to make new markets for that operationalization. Strategies for dealing with contingency are increasingly modelled through ‘risk appetite’ statements[[49]](#footnote-49) which in the context of data economies prioritize sharing and interoperability in order to unlock the value potential of datasets, but also factor in the costs inherent in managing risk.

The complex composition of the value of big data reiterates the dependency described by Simmel between trust and risk in the social relations of the new economy. Rather than functioning as an abstract moral category or code that sits outside and presides over such relations, ethics here supplies the frameworks of sociality and trust within which the value of big data can be produced and circulated. The case of Standards Australia and their global ambitions for AI leadership through standardization show that the socialization of risk is becoming a central part of the data economy, not just in the sphere of production and use, but also in the domain of regulation. This leads to a paradoxical relationship between risk and ethics: the development of AI and data ethics regulations provides the framework within which data-produced risks can be contained, even while ethics itself becomes a vehicle for the socialization of new forms of risk through experimental hubs and laboratory practices that can be scaled up to the level of a whole nation-state. This claim does not diminish the importance of social pressure and reputational stakes in the push for adopting ethical practices for exploiting big data,[[50]](#footnote-50) but rather accentuates it, stressing that managing trust and ethics are now integral to the extraction of economic value from highly socialized resources such as the mass aggregates of social data we now collectively produce.

## Funding disclosure

Work on this article was conducted as part of the project The Geopolitics of Automation (ID: GA64648) funded under the Discovery funding scheme of the Australian Research Council.

## References

Akhigbe, A., Martin, A.D., and Whyte, A.M. ‘Dodd–Frank and Risk in the Financial Services Industry’, *Review of Quantitative Finance and Accounting*, 47(2) (2016): 395–415.

Amoore, L. ‘Data Derivatives: On the Emergence of a Security Risk Calculus for our Times’, *Theory, Culture & Society*, 28(6), (2011): 24–43.

——. ‘Security and the Incalculable’, *Security Dialogue*, 45(5), (2014): 423–39.

——. ‘Doubt and the Algorithm: On the Partial Accounts of Machine Learning’, *Theory, Culture & Society*, 36(6), (2019): 147–69.

——. *Cloud Ethics*. Durham: Duke University Press, 2020.

Aradau, C. and Blanke, T. ‘The (Big) Data-security assemblage: Knowledge and critique’, *Big Data & Society*, issue 2(2) (2015): 1–12.

——. ‘Politics of Prediction: Security and the Time/Space of Governmentality in the Age of Big Data’, *European Journal of Social Theory*, 20(3), (2017): 373–91.

Barry, A. ‘Technological Zones’, *European Journal of Social Theory*, 9(2), (2006): 239–53.

Beck, U. *Risk Society: Towards a New Modernity*,trans. Ritter, M., Newbury Park, CA: SAGE Publications, 1992.

Bhabha, H.K. ‘Culture’s In-between’, in Hall, S. & du Gay, P. (eds) *Questions of Cultural Identity*, [place: publisher], 1996, pp. 53–60.

Birnhack, M. and Elkin-Koren, N. ‘The Invisible Handshake: The Reemergence of the State in the Digital Environment’, *SSRN Electronic Journal* 8(6), (2003): 1-57.

Brouwer, M.T. ‘Weber, Schumpeter and Knight on Entrepreneurship and Economic Development’, *Journal of Evolutionary Economics*, 12(1), (2002): 83–105.

Braidotti, R. *Transpositions: On Nomadic Ethics*. Cambridge: Polity, 2006.

Clarke, R. ‘Big Data, Big Risks’, *Information Systems Journal*, 26(1), (2016): 77–90.

Cooper, M. ‘Experimental Labour—Offshoring Clinical Trials to China’, *East Asian Science, Technology and Society: An International Journal*, 2(1), (2008): 73–92.

Cooper, M.E. *Life as Surplus: Biotechnology and Capitalism in the Neoliberal Era*. Seattle: University of Washington Press, 2011.

Daly, A. ‘Neo-liberal Business-as-Usual or Post-Surveillance Capitalism with European Characteristics? The EU’s General Data Protection Regulation in a Multi-Polar Internet’, in Hoyng, R. & Pak Lei Chong, G. (eds), *Critiquing Communication Innovation New Media in a Multipolar World. US–China Relations in the Age of Globalization*,Michigan State University Press, 2022, pp. 29–54.

Deloitte. ‘Risk Appetite Frameworks: How to Spot the Genuine Article’, available at https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-appetite-frameworks-financial-services-0614.pdf, 2014.

Dhawan, N. ‘Can Non‐Europeans Philosophize? Transnational Literacy and Planetary Ethics in a Global Age’, *Hypatia*, 32(3), (2017): 488–505.

Easterling, K. *Extrastatecraft: The Power of Infrastructure Space*. London: Verso Books, 2014.

The National New Generation Artificial Intelligence Governance Specialist Committee. ‘Ethical Norms for New Generation Artificial Intelligence’, 2021, English translation available at: https://cset.georgetown.edu/wp-content/uploads/t0400\_AI\_ethical\_norms\_EN.pdf

Eubanks, V. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York: St. Martin’s Press, 2018.

European Commission. ‘Regulatory Framework Proposal on Artificial Intelligence’,2022, available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#:~:text=The%20proposed%20AI%20regulation%20ensures,address%20to%20avoid%20undesirable%20outcomes.

Galloway, A. *Protocol: How Control Exists after Decentralization*, Cambridge, Massachusetts: MIT Press, 2004.

Goddard, M. ‘The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact’, *International Journal of Market Research* 59 (6, 2017): 703–5.

Gstrein, O.J. and Zwitter, A.J. ‘Extraterritorial Application of the GDPR: Promoting European Values or Power?’, *Internet Policy Review* [online] 10(3) (2021), available at: https://policyreview.info/articles/analysis/extraterritorial-application-gdpr-promoting-european-values-or-power.

Günther, W.A., Mehrizi, M.H.R., Huysman, M. and Feldberg, F. ‘Debating Big Data: A Literature Review on Realizing Value from Big Data’, *The Journal of Strategic Information Systems*, 26(3), (2017): 191–209.

Floridi, L. ‘Soft Ethics and the Governance of the Digital’, *Philosophy & Technology*, 31(1), (2018): 1–8.

Foucault, M. *Security, Territory, Population: Lectures at the Collège De France 1977–1978*, trans. G. Burchell. New York: Picador, 2007.

Hoelzl, I. and Marie, R. *Softimage: Towards a New Theory of the Digital Image*, Bristol, UK: Intellect Books, 2015.

Hristova, T. *Data Infrastructures and Digital Labour: The Case of Teleradiology*, PhD diss., Western Sydney University, Sydney, 2020.

Hristova, T., Neilson, B. and Rossiter, N. ‘Digital Infrastructure, Liminality, and World-Making Via Asia| On the Block Train: Rethinking Block Technologies on the YuXinOu Express’, *International Journal of Communication* 15 (2021): 2613–2630.

International Research Center for AI Ethics and Governance. *The Ethical Norms for the New Generation Artificial Intelligence, China*, 2021, available at: https://ai-ethics-and-governance.institute/2021/09/27/the-ethical-norms-for-the-new-generation-artificial-intelligence-china/.

ISO/IEC. 2022. International standard ISO/IEC DIS 23894. Information technology—Artificial intelligence—Risk management. International Organization for Standardization/International Electrotechnical Commission, (draft), Available at: https://www.iso.org/standard/77304.html

ISO/IEC 27001. Information security management. International Organization for Standardization/International Electrotechnical Commission, 2013, https://www.iso.org/standard/54534.html

ISO Guide 73:2009. Risk management—Vocabulary, International Organization for Standardization, 2009, https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en.

ISO 31000: 2018 Risk management—Guidelines, International Organization for Standardization, 2018, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

Johnson, G., Shriver, S. and Goldberg, S. ‘Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR’, 2021, https://dx.doi.org/10.2139/ssrn.3477686.

Kitchin, R. ‘Thinking Critically About and Researching Algorithms’, *Information, Communication & Society*, 20(1), (2017): 14–29.

LeCun, Y. ‘Deep Learning Hardware: Past, Present, and Future’, *IEEE International Solid-State Circuits Conference-(ISSCC)* 2019: 12–19.

Metzinger, T. ‘Ethics Washing Made in Europe’, *Der Tagspiegel*, 8 April 2019, https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html.

Munn, L., Hristova, T., & Magee, L. ‘Clouded Data: Privacy and the Promise of Encryption’, *Big Data & Society*, 6(1), (2019): 1–16.

Murphy, C.N. and Yates, J. *The International Organization for Standardization (ISO): Global Governance through Voluntary Consensus*. Milton Park: Routledge, 2009.

Naden, C. ‘It’s All About Trust’, 2019, https://www.iso.org/news/ref2452.html.

National Institute for Standards and Technology. ‘U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools Prepared in Response to Executive Order 13859’, 9 August 2019, https://www.nist.gov/system/files/documents/2019/08/10/ai\_standards\_fedengagement\_plan\_9aug2019.pdf.

Niebel, C. ‘The Impact of the General Data Protection Regulation on Innovation and the Global Political Economy’, *Computer Law & Security Review*, 40, (2021) 105523: p. 1–15.

Power, M. ‘The Risk Management of Everything’, *The Journal of Risk Finance*, 5(3), (2004): 58–65.

Productivity Commission. ‘Data Availability and Use: Productivity Commission Inquiry Report’, 2017. Available at: https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf.

Radu, R. ‘Steering the Governance of Artificial Intelligence: National Strategies in Perspective’, *Policy and Society* 40(2), (2021): 178–93.

Roberts, H., Cowls, J., Morley, J. et al. ‘The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation’, *AI & Soc* 36, (2021): 59–77.

Silverpond. ‘The Role of Ethics in AI Development, Implementation and Governance’, 2021, https://silverpond.com.au/ai-community/australian-ai-ecosystem-survey/aurelie-jacquet-2020-2021-australian-ai-ecosystem-survey/.

Simmel, G. *The Philosophy of Money*, Milton Park: Routledge, 2004.

Standards Australia. *An Artificial Intelligence Standards Roadmap: Making Australia’s Voice Heard. Final Report*, 2020, https://www.standards.org.au/getmedia/ede81912-55a2-4d8e-849f-9844993c3b9d/1515-An-Artificial-Intelligence-Standards-Roadmap12-02-2020.pdf.aspx.

Veracini, L. ‘Understanding Colonialism and Settler Colonialism as Distinct Formations’, *Interventions*, 16(5), (2014): 615–33.

Wagner, B. ‘Ethics as an Escape from Regulation. From “Ethics-washing” to Ethics-shopping?’ in Bayamlioglu, E., Baraliuc, I., Janssens, L.A.W., Hildebrandt, M. (eds) *Being Profiled*, Amsterdam: Amsterdam University Press, 2018, 84–9.

Wilkinson, M., Dumontier, M., Aalbersberg, I. et al. ‘The FAIR Guiding Principles for Scientific Data Management and Stewardship’, *Sci Data* 3, 160018, (2016): 1–9

Yahoo Finance. Alibaba Group Holding Limited (BABA), 2022, https://finance.yahoo.com/quote/BABA/.

1. M. Wilkinson, M. Dumontier, I. Aalbersberg, et al., ‘The FAIR Guiding Principles for Scientific Data Management and Stewardship’, *Sci Data* 3, 160018, (2016). [↑](#footnote-ref-1)
2. C.N. Murphy, and J. Yates, *The International Organization for Standardization (ISO): Global Governance through Voluntary Consensus*. Milton Park: Routledge, 2009. [↑](#footnote-ref-2)
3. ISO/IEC, ‘Draft international standard ISO/IEC DIS 23894’, Information technology—Artificial intelligence—Risk management, 2022. [↑](#footnote-ref-3)
4. Keller Easterling, K. *Extrastatecraft: The Power of Infrastructure Space*. London: Verso Books, 2014. [↑](#footnote-ref-4)
5. Andrew Barry, ‘Technological Zones’, *European Journal of Social Theory*, 9(2), (2006): 239–53. [↑](#footnote-ref-5)
6. C. Aradau and T. Blanke, ‘The (Big) Data-security assemblage: Knowledge and critique’, *Big Data & Society*, 2(2) (2015): 1–12; R. Kitchin, ‘Thinking Critically About and Researching Algorithms’, *Information, Communication & Society*, 20(1), (2017): 14–29. [↑](#footnote-ref-6)
7. Alexander Galloway. *Protocol: How control exists after decentralization*. MIT Press. 2004. [↑](#footnote-ref-7)
8. I. Hoelzl and R. Marie, *Softimage: Towards a New Theory of the Digital Image*, Bristol, UK: Intellect Books, 2015. [↑](#footnote-ref-8)
9. T. Hristova, *Data Infrastructures and Digital Labour: The Case of Teleradiology*, PhD diss., Western Sydney University, Sydney, 2020. [↑](#footnote-ref-9)
10. Easterling, *Extrastatescraft.* [↑](#footnote-ref-10)
11. L. Amoore, ‘Data Derivatives: On the Emergence of a Security Risk Calculus for our Times’, *Theory, Culture & Society*, 28(6), (2011):24–43; Amoore, ‘Security and the Incalculable’, *Security Dialogue*, 45(5), (2014): 423–39; Amoore, *Cloud Ethics*. Durham: Duke University Press, 2020; C. Aradau and T. Blanke, ‘The (Big) Data-security assemblage: Knowledge and critique’, *Big Data & Society*, issue 2(2) (2015): 1–12; V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York: St. Martin's Press, 2018, among many. [↑](#footnote-ref-11)
12. Hristova, *Data Infrastructures and Digital Labour*; T. Hristova, B. Neilson, and N. Rossiter, ‘Digital Infrastructure, Liminality, and World-Making Via Asia On the Block Train: Rethinking Block Technologies on the YuXinOu Express’, *International Journal of Communication* 15 (2021). [↑](#footnote-ref-12)
13. IPCC, ‘2—Determinants of Risk: Exposure and Vulnerability—IPCC’, https://www.ipcc.ch/pdf/special-reports/srex/SREX-Chap2\_FINAL.pdf. [↑](#footnote-ref-13)
14. G. Simmel, *The Philosophy of Money*, Milton Park: Routledge, 2004, 177–8. [↑](#footnote-ref-14)
15. U. Beck, *Risk Society: Towards a New Modernity*,trans. Ritter, M., Newbury Park, CA: SAGE Publications, 1992. [↑](#footnote-ref-15)
16. (ISO 31000: 2018), 3.1. [↑](#footnote-ref-16)
17. (ISO Guide 73:2009), 3.7.1.2. [↑](#footnote-ref-17)
18. Deloitte, ‘Risk Appetite Frameworks: How to Spot the Genuine Article’, available at https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-appetite-frameworks-financial-services-0614.pdf, 2014. [↑](#footnote-ref-18)
19. Y. LeCun, ‘Deep Learning Hardware: Past, Present, and Future’, *IEEE International Solid-State Circuits Conference-(ISSCC)* 2019: 12–19. [↑](#footnote-ref-19)
20. M. Power, ‘The Risk Management of Everything’, *The Journal of Risk Finance*, 5(3), (2004): 58–65. [↑](#footnote-ref-20)
21. L. Munn, T. Hristova, and L. Magee, ‘Clouded Data: Privacy and the Promise of Encryption’, *Big Data & Society*, 6(1), (2019): 1–16. [↑](#footnote-ref-21)
22. Amoore, ‘Doubt and the Algorithm: On the Partial Accounts of Machine Learning’, *Theory, Culture & Society*, 36(6), (2019): 147–69. [↑](#footnote-ref-22)
23. M.T. Brouwer, ‘Weber, Schumpeter and Knight on Entrepreneurship and Economic Development’, *Journal of Evolutionary Economics*, 12(1), (2002): 83–105. [↑](#footnote-ref-23)
24. C. Naden, ‘It’s All About Trust’, 2019, https://www.iso.org/news/ref2452.html. [↑](#footnote-ref-24)
25. Silverpond, ‘The Role of Ethics in AI Development, Implementation and Governance’, 2021, https://silverpond.com.au/ai-community/australian-ai-ecosystem-survey/aurelie-jacquet-2020-2021-australian-ai-ecosystem-survey/. [↑](#footnote-ref-25)
26. Standards Australia, *An Artificial Intelligence Standards Roadmap: Making Australia’s Voice Heard. Final Report*, 2020, 35–36, https://www.standards.org.au/getmedia/ede81912-55a2-4d8e-849f-9844993c3b9d/1515-An-Artificial-Intelligence-Standards-Roadmap12-02-2020.pdf.aspxhttps://www.standards.org.au/getmedia/ede81912-55a2-4d8e-849f-9844993c3b9d/1515-An-Artificial-Intelligence-Standards-Roadmap12-02-2020.pdf.aspx. [↑](#footnote-ref-26)
27. M. Cooper, ‘Experimental Labour—Offshoring Clinical Trials to China’, *East Asian Science, Technology and Society: An International Journal*, 2(1), (2008): 73–92; Cooper, M.E. *Life as Surplus: Biotechnology and Capitalism in the Neoliberal Era*. Seattle: University of Washington Press, 2011. [↑](#footnote-ref-27)
28. L. Veracini, ‘Understanding Colonialism and Settler Colonialism as Distinct Formations’, *Interventions*, 16(5), (2014): 615–33. [↑](#footnote-ref-28)
29. National Institute for Standards and Technology, ‘U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools Prepared in Response to Executive Order 13859’, 9 August 2019, https://www.nist.gov/system/files/documents/2019/08/10/ai\_standards\_fedengagement\_plan\_9aug2019.pdf. [↑](#footnote-ref-29)
30. European Commission, ‘Regulatory Framework Proposal on Artificial Intelligence’, 2022, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai#:~:text=The%20proposed%20AI%20regulation%20ensures,address%20to%20avoid%20undesirable%20outcomes. [↑](#footnote-ref-30)
31. H. Roberts, J., Cowls, J. Morley, J. et al. ‘The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation’, *AI & Soc* 36, (2021): 59–77. [↑](#footnote-ref-31)
32. R. Radu, ‘Steering the Governance of Artificial Intelligence: National Strategies in Perspective’, *Policy and Society* 40(2), (2021): 182. [↑](#footnote-ref-32)
33. M. Birnhack and N. Elkin-Koren, ‘The Invisible Handshake: The Reemergence of the State in the Digital Environment’, *SSRN Electronic Journal* 8(6), 2003: 1–57 [↑](#footnote-ref-33)
34. T. Metzinger, ‘Ethics Washing Made in Europe’, *Der Tagspiegel*, 8 April 2019, https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html; B. Wagner, ‘Ethics as an Escape from Regulation. From “Ethics-washing” to Ethics-shopping?’ in (eds) Bayamlioglu, E., Baraliuc, I., Janssens, L.A.W., Hildebrandt, M., Amsterdam (eds) *Being Profiled*, Amsterdam University Press, 2018, 84–9. [↑](#footnote-ref-34)
35. M. Goddard, ‘The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact’, *International Journal of Market Research*, 59(6),(2017): 703–5; C. Niebel, ‘The Impact of the General Data Protection Regulation on Innovation and the Global Political Economy’, *Computer Law & Security Review*, 40, (2021): p.105523. [↑](#footnote-ref-35)
36. Metzinger, ‘Ethics Washing Made in Europe’. [↑](#footnote-ref-36)
37. A. Daly, ‘Neo-liberal Business-as-Usual or Post-Surveillance Capitalism with European Characteristics? The EU’s General Data Protection Regulation in a Multi-Polar Internet’, in *Communication Innovation and Infrastructure: A Critique of the New in a Multipolar World*,East Lansing: Michigan State University Press, (forthcoming, 2021) pp.66–95; O.J. Gstrein. and A.J. Zwitter, ‘Extraterritorial Application of the GDPR: Promoting European Values or Power?’, *Internet Policy Review* [online] 10(3) (2021), available at: https://policyreview.info/articles/analysis/extraterritorial-application-gdpr-promoting-european-values-or-power. [↑](#footnote-ref-37)
38. G. Johnson, G., S. Shriver, and S. Goldberg, ‘Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR’, 2021. *3477686*. [↑](#footnote-ref-38)
39. Johnson, Shriver, and Goldberg, ‘Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR’, 15. [↑](#footnote-ref-39)
40. H. Roberts, J., Cowls, J. Morley, J. et al., ‘The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation’. [↑](#footnote-ref-40)
41. International Research Center for AI Ethics and Governance, 2021. [↑](#footnote-ref-41)
42. From its highpoint of $304.69 USD on October 1 2020, Alibaba’s US-listed holding company has declined by 69 percent at time of writing (June 4) (Yahoo Finance. Alibaba Group Holding Limited (BABA), 2022, https://finance.yahoo.com/quote/BABA/). [↑](#footnote-ref-42)
43. Dashveenjit Kaur, ‘China’s most advanced chip may soon come from Alibaba’, *Techwire Asia*, 21 October 2021. https://techwireasia.com/2021/10/the-new-chip-by-alibaba-may-be-one-of-the-most-advanced-in-china/. [↑](#footnote-ref-43)
44. Brian Liu and Raquel Leslie, ‘China’s Tech Crackdown: A Year-In-Review’, *Lawfare*, 7 January 2022. https://web.archive.org/web/20220506205610/https:/www.lawfareblog.com/chinas-tech-crackdown-year-review. [↑](#footnote-ref-44)
45. L. Floridi, ‘Soft Ethics and the Governance of the Digital’, *Philosophy & Technology*, 31(1), (2018): 1–8. [↑](#footnote-ref-45)
46. R. Braidotti, *Transpositions: On Nomadic Ethics*. Cambridge: Polity, 2006; N. Dhawan, ‘Can Non‐Europeans Philosophize? Transnational Literacy and Planetary Ethics in a Global Age’, *Hypatia*, 32(3), (2017): 488–505; H. Bhabha, ‘Culture’s In-between’, in S. Hall, and P. du Gay (eds) *Questions of Cultural Identity*, London: SAGE, 1996, pp. 53–60. [↑](#footnote-ref-46)
47. L. Amoore, ‘Data Derivatives: On the Emergence of a Security Risk Calculus for our Times’; Amoore, ‘Security and the Incalculable’; Amoore, *Cloud Ethics*; 2020, Aradau and Blanke, ‘The (Big) Data-security assemblage: Knowledge and critique’ Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, among many. [↑](#footnote-ref-47)
48. Cooper, ‘Experimental Labour—Offshoring Clinical Trials to China’, A. Akhigbe, A.D. Martin, and A.M. Whyte, ‘Dodd–Frank and Risk in the Financial Services Industry’, *Review of Quantitative Finance and Accounting*, 47(2) (2016): 395–415. [↑](#footnote-ref-48)
49. Productivity Commission, 2017; PricewaterhouseCoopers, 2012. [↑](#footnote-ref-49)
50. W.A. Günther, M.H.R. Mehrizi, M. Huysman, and F. Feldberg, ‘Debating Big Data: A Literature Review on Realizing Value from Big Data’, *The Journal of Strategic Information Systems*, 26(3), (2017): 191–209; R. Clarke, ‘Big Data, Big Risks’, *Information Systems Journal*, 26(1), (2016): 77–90. [↑](#footnote-ref-50)