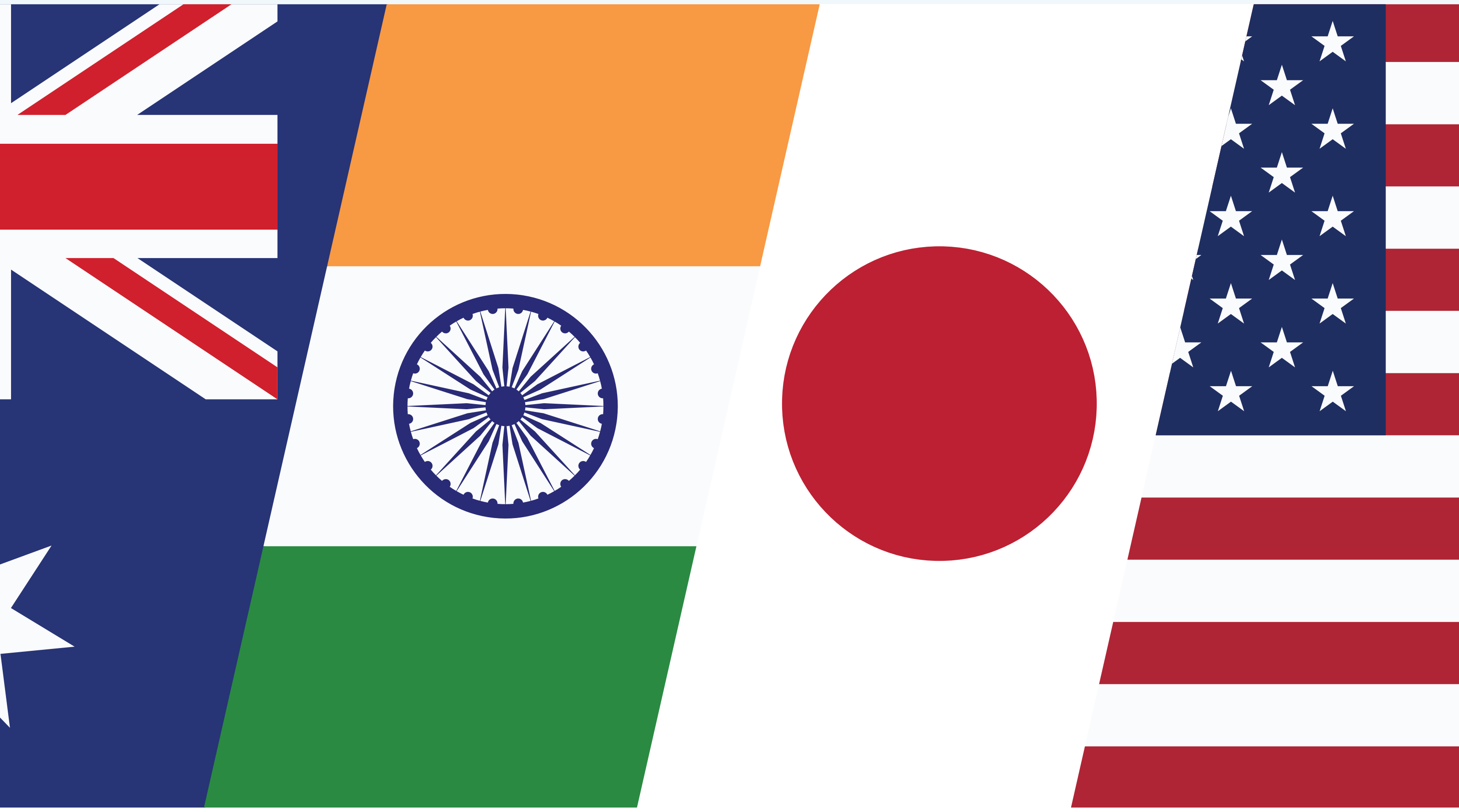
Quad Tech Network QTN Series

EMBRACING DIFFERENCE: GOVERNANCE OF CRITICAL TECHNOLOGIES IN THE INDO-PACIFIC

FEBRUARY 2021

Authors: Jolyon Ford and Damian Clifford

Series Editors: Katherine Mansted and Rory Medcalf



Australian National University

Center for a New American Security

GRIPS 政策研究大学院大学 National Graduate Institute for Policy Studies

ORF

About the Quad Tech Network Series

The Quad Tech Network (QTN) is an Australian Government initiative to promote regional Track 2 research and public dialogue on cyber and critical technology issues.

This paper is part of a series of papers by universities and think tanks in Australia (the National Security College at The Australian National University), India (the Observer Research Foundation), Japan (the National Graduate Institute for Policy Studies) and the United States (Center for a New American Security).

The QTN series offers analysis and recommendations on shared challenges facing Australia and Indo-Pacific partners across four themes:

- international peace and security
- connectivity and regional resilience
- human rights and ethics, and
- national security.

The QTN is managed by the National Security College at The Australian National University, with the support of the Australian Department of Foreign Affairs and Trade.

About the Series Editors

Rory Medcalf is Head of the National Security College at The Australian National University. Professor Medcalf's professional background spans diplomacy, journalism, think thanks and intelligence analysis, including as founding Director of the International Security Program at the Lowy Institute from 2007 to 2015. Professor Medcalf has been recognised as a thought leader internationally for his work on the Indo-Pacific concept of the Asian strategic environment, as articulated in his 2020 book *Contest for the Indo-Pacific* (released internationally as *Indo-Pacific Empire*).

Katherine Mansted is the Senior Adviser for Public Policy at the National Security College at The Australian National University, and a non-resident fellow at the Alliance for Securing Democracy at the German Marshall Fund of the United States. She regularly writes and presents to government and public audiences on technology and security policy. Ms Mansted holds a Master in Public Policy from the Harvard Kennedy School of Government, and a first-class degree in law and international relations.

Australian Government
Department of Foreign Affairs and Trade

Published by the National Security College, The Australian National University, Acton ACT
2601, Australia

Available to download for free at nsc.crawford.anu.edu.au

Cover design and layout by Black Bear Creative.

About the Authors

Jolyon Ford is Professor and the Associate Dean (International) at the Australian National University (ANU) College of Law. Before re-joining ANU in 2015, Dr Ford was an Associate Fellow of the Royal Institute for International Affairs, London (Chatham House), and a Research Associate of the Global Economic Governance Programme at the University of Oxford's Blavatnik School of Government. Before that, he held a senior role at Oxford Analytica. Dr Ford has worked in the federal public service, an intergovernmental organisation, academia, civil society and the private sector, and as a freelance consultant. He holds degrees from the University of KwaZulu-Natal (South Africa), Cambridge, and the ANU.

Damien Clifford is a Senior Lecturer at the Australian National University College of Law and an Associate Researcher at Information Law and Policy Centre at the Institute of Advanced Legal Studies (University of London). His research focuses predominantly on data protection, privacy and the regulation of technology. He has previously been a visiting lecturer at the Dickson Poon School of Law, King's College London, a sessional lecturer and honorary fellow at the Melbourne Law School, University of Melbourne, and a sessional lecturer at Swinburne University of Technology. Dr Clifford completed his PhD at the KU Leuven Centre for IT & IP Law where he was an FWO Aspirant Fellow funded by Fonds Wetenschappelijk Onderzoek – Vlaanderen.

Contents

Executive Summary

The Quadrilateral Security Dialogue (or 'Quad') aims to promote security and economic cooperation between the Indo-Pacific's four leading democracies: Australia, India, Japan and the United States. In this, the grouping is at once a mechanism to cooperate in relation to material interests, and a commitment to fundamental democratic values. Particularly in 2020, the Quad grouping has signalled an intention to increase engagement and agenda-shaping in relation to critical technologies. This is a complex undertaking: development, use and regulation of critical technologies cuts across multiple policy areas, including those outside (or at least adjacent to) the Quad grouping's traditional focus on security and economics. Further, critical technologies are also inherently social artefacts – they are shaped by, and shape, civil society and private-sector actors. This makes a purely state-led approach to their governance difficult, and arguably inappropriate.

This paper considers what an approach to human rights and ethical governance of critical technologies could entail for Quad members. Its focus is data-driven technologies (and associated data-sets). However, the paper's insights will be applicable across different categories of critical technologies. In a COVID-and-after world, this conceivably includes biotech and biometric contexts such as epidemiology, testing, vaccine and treatment technologies.

The key insight of the paper is that policymaking and diplomacy on critical technologies should proceed from a recognition that the uses and impacts of technology are heavily affected by social factors, including local culture, context and legal traditions.

Quad membership is often defined by distinguishing from autocratic/non-democratic powers. However, there are also considerable divergences within and between Quad members, and other partners, on what the responsible development, use and governance of technology (and related data) comprises.

There are also differences between and within like-minded countries about how technologies are perceived to either pose a risk to, or enhance, security, economic and social interests and values.

This techno-social context of critical technology raises important questions:

- Where is there scope to aim for common Quad-level approaches and standards?
- Where is difference inevitable (or even desirable), and how should it be managed?
- What is the role for ethics and human rights, and are these strategically the most appropriate and compelling frames for pursuing the governance of critical technologies? What other governance systems (or narratives) might assist in the socially responsible development and use of technology?
- How does the outsized role and impact of the private sector (especially transnational 'big tech') affect the viability of state-led approaches?

This paper grapples with each of these questions across five parts.

Part 1 examines the complexities of critical technology policymaking and diplomacy. First, critical technologies are not value-neutral; they therefore reflect and relate to local cultural and social factors. Second, it is difficult to apply 'universal' ethical principle and human rights frameworks to local contexts. There is a risk that frameworks based on high-level principles (such as 'sovereignty', 'fairness' and 'autonomy') become cooperation fig leaves: in-principle consensus between countries simply conceals significant divergences in how those principles are understood and applied. Third, governments are not always the most powerful or influential actors in shaping data-driven technologies, and related governance regimes. The private sector plays an outsized role, and governance is 'polycentric' – it occurs through and with multiple actors, institutions and systems.

Part 2 then asks what might be the most appropriate framing for approaching questions of the responsible development and use of critical technologies. So far, ethics-based frameworks have gained more traction than law-based and human rights ones. In part, this is because influential corporate players prefer the more voluntaristic, non-legalistic approach that this implies. 'Human rights' framings for critical technology are yet to gain significant traction in international or national-level governance debates. Regardless of framing, there is a risk that 'universal' frameworks paper over differences in countries' domestic contexts, legal traditions, and local culture and traditions. Accordingly, diplomacy is most likely to succeed where it comprises messages, assistance and engagement that speak to things that are useful to partner states, not just 'right'. This could involve a focus on themes of economic prosperity and community utility and safety – and on helping societies strike a balance between integration with global technology, on one hand, and autonomy over the terms of that integration, on the other hand.

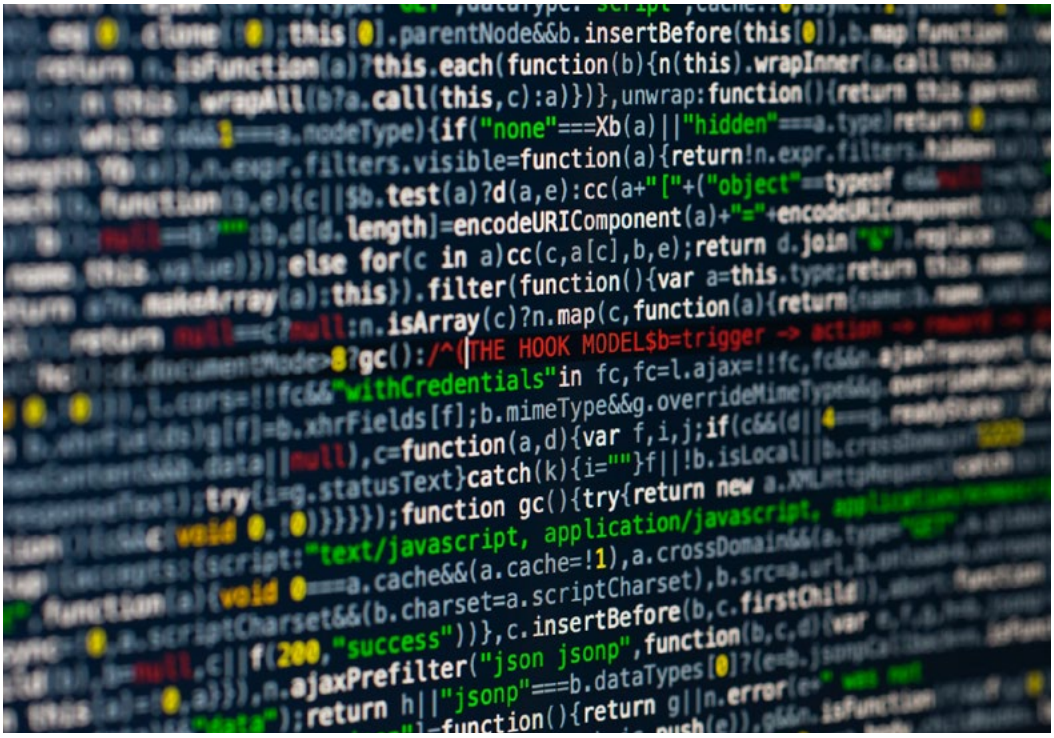
Part 3 then canvasses key issues at the intersection of human rights, ethics and security that Quad members – either alone or together – will need to bear in mind when promoting critical technology governance standards. This includes:

- ***Avoiding patterns of domination and exclusion:*** diplomacy on critical tech governance should avoid – in reality and perception – perpetuating patterns of domination and exclusion especially among tech-importing less-developed societies. This is a particularly charged concern in relation to data-driven technologies, given evidence that artificial intelligence (AI) systems can entrench inequality, and arguments that 'big tech' corporations have both extractive and monopolistic business models and tendencies. Accordingly, diplomacy should not just be about *leading* development of governance models (let alone imposing or exporting these), but including and supporting other societies in those debates and processes. Successful diplomacy may be less about 'selling' a vision of critical tech's role in society, and more about creating forums and platforms for dialogue and model-building. Further, diplomacy will need to strike a careful balance between both security *and* prosperity concerns – and be careful to not be seen as again asking lower income countries to trade their prosperity and autonomy away for other countries' security.

- ***Prioritising sovereignty and trust in local institutions:*** data-driven technologies create unprecedented scope for external forces to shape socio-political discourse and cultural themes in far-off societies. This may result from calculated sustained efforts, but may also be an incidental externality of the uptake by populations of certain global tech products and platforms. Local governance institutions are not necessarily influential in such contexts and may be by-passed or undercut as effective forums – which could have major impacts on social cohesion, and public trust in institutions. Thus, critical technology diplomacy should focus on capacity-building of local institutions – even if those institutions differ in practice, there is shared interest in standards and approaches that preserve and protect the 'local' in 'local institutions'.

Part 4 then narrows in on a key issue across a range of critical technologies: data governance and privacy regimes. It uses divergences between Quad countries' regulatory approaches in these areas as a case study of the tension between, on the one hand, strategic and economic incentives for harmonisation and, on the other hand, cultural, legal, political and security factors that drive difference. The part discusses some of the inherent characteristics of data and data-driven technologies that drive differences in approach between even like-minded countries – such as tensions between domestic private regimes for commercial uses of data, and public regimes using data for a range of national purposes, from government services to law enforcement and national security.

Part 5 offers insights for how Australia, especially via mini-lateral groupings such as the Quad, can engage in diplomacy at the nexus of critical technologies, human rights and ethics.



Data is the basic building block of many critical technologies. Picture: Marcus Spiske / Unsplash, https://bit.ly/3r1TM3p

Actors and Activities: Multiplicity and Divergence

Shared Values and 'Critical Technologies'

Some current and emerging technologies have the potential to significantly enhance or to threaten prosperity, social cohesion and security – and so impact countries' core national and foreign policy interests.[1] The salience of technology to foreign policy is evidenced in the inclusion of digital infrastructure and cyber security on the agenda for Quad ministerial dialogues in 2020, and the growth of bilateral agreements between Quad countries on issues of cyber and critical technologies.[2] Since its revival in 2017, Quad members have emphasised their 'like-mindedness' as the four leading democracies in the Indo-Pacific. Shared approaches to technology governance, building trusted supply chains and cyber security norms seems a natural progression. Certainly, Quad members express a shared interest in maintaining a rules-based global order and in balancing the influence of authoritarian powers (China and Russia) in the Indo-Pacific.

However, foreign policy approaches based on democratic or other shared values must navigate twin realities:

1. **Critical technologies are value-laden instruments.** The creation and reception of technology is shaped by culturally specific preferences and perspectives. This is heightened in the case of information-based and data-driven technologies (compared with, for example, nuclear technologies) as these are intimately and deeply connected with patterns of economic and social life. Moreover, critical technology policy issues are *techno-social* in nature since technologies necessarily interface with human-social factors.

2. **Even 'universal' values must be adapted for, and applied at, the local level.** Notionally universal ethical principles and human rights frameworks must be approached through an appreciation of the significance of cultural diversity and local contextual factors. Interpretations of ethical and human rights principles change with time and place.

Further, interpreting and applying values is not the exclusive purview of the state. Especially in a democracy, values are constantly interpreted and reinterpreted by cultural and social actors, a process that is particularly acute in the case of critical technologies. Multiple non-state actors have stakes in the development, use and regulation of critical technologies. In practical terms, governments are not always the most powerful or influential actors in shaping the use and impact of data-driven technologies or their governance.

Diplomacy and Standard-setting in the Context of Private and Plural Governance Systems

Analysis of the governance of critical technologies must account for multiplicity and diversity: in terms of *who* has power and influence, and *how* regulatory and governance frameworks are constituted.

Private Sector

There is significant diversity in terms of who constitutes a 'key stakeholder' in shaping how critical technologies are developed, used, perceived and governed. State action in this area – including Quad regional cooperation, diplomacy and standard-setting/norm-promotion – must account for the particular and outsize role that 'big tech' firms and other private sector actors play in respect of both *the governance of critical technologies* and, conversely, *the impact of critical technologies on governance.* The private sector's role and influence is crucial not just in relation to shaping the design and implementation of particular technology regulation regimes and governance architectures. It is also crucial in relation to how technology firms have the power, capacity, reach and resources to shape what we conceive as possible and appropriate approaches to tech governance more generally. This includes shaping societal meta-narratives about 'technologies and the public good' and about what constitutes responsible and appropriate development, use and regulation of technology.

What does this mean for Quad-level dialogue and diplomacy? Key technology firms (and their professional and industry associations and standardisation bodies, etc.) are not necessarily passive or cooperative vehicles for the attempted projection, by states, of national and foreign policy interests. Nor is the idea of government cooperation with big tech risk-free: explicit partnerships raise the risk of potentially negative public sentiment and distrust given the concentration of market and social power in some of these firms. Closer cooperation carries some risk of perceived – or real – corporate capture of state policymaking and regulation. Yet it is also true that Quad states (jointly and individually) have not yet fully explored how to advance national and foreign policy interests through strategic engagement with private sector actors – or with the civic and intellectual/academic networks that research and critique them – including in relation to ethical and human rights issues.

Pluralised Governance

Compared to a classic formal institutionalist approach, the governance of critical technologies is 'polycentric': it occurs from and through multiple sources and systems. Conceptions of governance along a statist national–international axis can be highly misleading, or at least do not fully account for the reality of multiple actors and governance systems. Even if state control is being reasserted in the COVID-and-after era, it is still axiomatic (and vital in conceiving Quad policymaking) to observe that authority and influence is dispersed across society. State-made laws and institutions, and conventional hierarchical structures, do not have a monopoly on influencing behaviours within industry sectors and societies. Non-state actors (e.g. transnational industry associations) define and administer standards over many areas, and 'regulate' formal regulatory bodies. State and non-state actors interact in governance ecosystems without structural pathways; for example, private transnational actors might engage directly with multilateral public authorities without state-level interlocutors being involved, and vice-versa. 'Jurisdictions' are not necessarily self-contained and territorially based, but are often functional and specific, overlapping and/or competing. Moreover, social ordering does not arise only from state sanction, coercion or threat: negotiation, compromise and cooperation due to interdependence and mutual benefit can define many governance relationships. Yet while global and other governance systems are not always planned, formally mandated or even mandatory, they can generate compliance as great as systems involving direct government intervention.

AI and other related emerging technologies may be new. But there is nothing particularly new about the fact that we are not just governed, day to day, by top-down state-made 'hard' (binding) laws and regulations; we are all also 'governed' by a very complex constellation of national, international and transnational frameworks and schemes.

These may be public or private, mandatory or voluntary, state-mandated or driven by industry groups, financiers, insurers and other key players. They may be intentional or inadvertent, in the sense that they arise from design or structure of widely used systems and infrastructure. Thus, with respect to human rights and ethics, it is important to bear in mind that not all the regulation that matters emanates from state-made national or treaty legal and other frameworks. Moreover, this has long been true. For example, marine safety standards now embedded and adopted in national laws originated 'bottom up', some centuries ago, from the self-regulatory practices of London marine cargo insurance brokers. The state's role came later, and was fundamentally shaped by existing industry practices and business imperatives. In many economic sectors, it is possible to say that non-state industry, professional and other standards (even where not mandatory) are more influential in shaping behaviour than statist ones. This does not negate the need for hard law in the responsible and democratic governance of critical technologies, but properly situates the debate within a more complex multi-actor regulatory ecosystem.

What does this mean for Quad-level dialogue, including about frameworks for governing critical technologies? The existence of pluralised sources of state and non-state, 'hard' and 'soft' governance is a salient reality in relation to frameworks for the governance of responsible technology development and use. Accepting the plurality of governance actors and systems does not mean that formal state institutions, rule-systems and standard-making have no role. But the existence and influence of multiple and often private systems of governance point to the difficulty of integration and coordination even within a single state. This is true even if one had a universal and stable set of values, an issue to which we now turn.

Framework Diplomacy: Ensuring Resonance and Credibility

Tech systems are contingent upon, and partly constituted by, social systems (including legal systems), that vary considerably even within supposedly like-minded democratic states. The 'technical' aspects of critical technologies are inevitably and intimately connected to their 'sociocultural' aspects. However, the fast-paced roll-out of technologies – and proliferation of schemes for their governance – may cause policymakers to lose sight of the reality of diversity and contestation over meaning between and within different cultures and societies. This important differentiation might be missed in contrasting between democratic and non-democratic powers, as Quad membership does, since democratic countries are themselves so diverse in how they imagine, engage with and regulate technologies and their impacts.

This part argues that critical technology diplomacy should be wary of assumptions about supposedly universal and culturally neutral values-based frameworks. Such assumptions can create analytical blind spots and policy approaches that overlook important patterns of diversity and divergence. The consequences of glossing over difference could range from relatively confined (e.g. failed traction for governance frameworks) to systems-wide (e.g. more generalised push-back against open markets and political systems).

Values in Technology

Data-based technologies such as AI and machine learning (ML, a subset of AI) are somewhat instrumental in nature. That is, they can be used in very different ways or with different political motives (for example, to enhance political freedoms, or to repress and distort these). Yet because of their reliance on particular data-sets and the nature of their design, such technologies are also not just neutral technical instruments. Instead, most technologies (and certainly AI/ML technologies) are both inherently and deeply value-laden. This is true in at least two ways.

1. **Application of technologies.** In a narrow sense, applications of data-driven technologies reflect values to the extent they reflect particular data-sets – and the cultural, social and historical reference points of system designers. These platforms or programs typically carry their own embedded preferences, the hallmarks of the cultural place (and time) of their design, along with certain in-built logics and assumptions that, typically, are specific to certain cultural or social viewpoints. A decision-assisting AI trained on Japanese societal data is likely to have very particular characteristics wherever in the world it is deployed.

2. **Design and adoption of technologies.** More broadly, there are close links between what any one society values or aspires to and the sorts of technologies that the society accordingly develops, prefers or reacts adversely to. Attempts to conceive and develop Quad-wide approaches should proceed from a recognition that there are close links between a society's collective cultural imagination and the technologies it uses and/or develops, and how it relates to (trusts or distrusts, etc.) any one kind of technology. For example, media effects scholars might argue that popular culture products such as the Terminator have influenced US collective societal approach to and imagination of 'robots' (fear, distrust), whereas Japanese attitudes to robots are very different due to influential cartoon characters. Meta-analyses of social science scholarship in this area have demonstrated how perceptions and understandings of AI or other technologies such as CCTV are very different around the world, and heavily shaped by local cultural and social context.

   For instance, the political viability of large-scale, tech-assisted social surveillance and control techniques is closely connected to cultural-political imaginations: it cannot be assumed that all societies will have roughly the same view of the ethics and social impacts of such technologies. Some societies (or sections of societies) may be far more comfortable with AI-enabled surveillance than others. Scholars argue, for example, that European countries' emphasis on privacy and digital rights is at least in part a response to the historical legacy of 20th-century totalitarianism and wide-spread social surveillance. There is still relatively little research on issues such as whether, and under what circumstances, people in different Asian countries might accept AI-assisted governmental decision-making. Yet it is clear that policymaking around data-based technologies must account for the fact that culturally specific considerations affect the operation of such technologies as well as how they are received and perceived.

Values in Technology's Governance

Likewise, the supposedly universal ethical and human rights precepts that are being put forward to govern AI technologies are, in reality, contingent on contextual and cultural factors. Considerable uncertainty remains around the governance of AI and other technologies, but the broad trend in recent years has been to promote ethics-based frameworks. There has been a huge proliferation of these principled frameworks,[3] promoted or adopted by governments, inter-governmental organisations such as the OECD, the world's largest technology companies, expert and professional groupings, and civic organisations.

This choice of ethics-based governance approaches is common, from the US and EU to China. Moreover, these frameworks and their overarching principles are superficially similar, as is evident from comparing the OECD's 2019 AI Principles[4] with Beijing's May 2019 principles.[5] Whether corporate or state-based in origin, all such frameworks express ostensibly universal values (e.g. 'safe', 'trustworthy', 'fair').

In the case of the Beijing AI Principles, many observers have appeared surprised that there was a willingness, within Chinese policy circles, to discuss such values-based issues so openly.

Yet this assumes that such lists of ethical principles relate to a universally agreed, stable and objective set of values. Instead, the deceptively simply ethical precepts such as 'fairness' or 'explainability' contained in such lists are – like concepts such as 'the rule of law' and 'sovereignty' – open to all manner of interpretation and operationalisation. They are also heavily contingent on cultural factors. These vary hugely across the region, even within democratic and Quad countries. The 'shared values' and 'like-minded' rhetoric around Quad membership can potentially obscure this fact.

Regional variations are something of a blind spot in the 'ethical AI' debate. Societies have particular conceptions of ethics, and apparently universal concepts such as 'fairness' or 'privacy' are deeply value-laden and contestable, and may have different meanings (and claims to significance/priority as values) in different societies, even if one is somehow able to arrive at perfect translations of such terms across all languages.

'Ethics' can be understood as a set of principled methodologies for resolving competing claims, but the principles' content only really takes on meaning in particular cultural contexts where those claims arise. This is why it is often said that the ethical 'rules' of any game may appear the same, but how people understand and play those games will likely differ by culture and indeed sub-culture.

The proliferation of broad ethics-based principles around the governance of AI and related technologies can obscure the existence of very different cultural conceptions and concerns, in different societies, about issues such as the proper relationship and distribution of power as between individuals, governments and corporations. This sort of insight has significant implications for the legitimacy and/or traction of foreign policy strategies to promote ethics-based or other value frameworks where these inevitably both contain particular conceptions of values, and are likely to be received or understood in diverse ways.

Unintended Consequences and Possible Implications of Different 'Frames' of Values-based Governance

What, then, is the most appropriate framing for approaching questions of the proper or responsible development and use of critical technologies? Is the appropriate framework an ethics-based one, or a human rights–based one, or are these not mutually exclusive? Is it best framed in terms of human rights, or other concepts such as 'freedom' or 'democratic values', and what are the implications – for cooperation and influence – of preferring and projecting different frames?

The proliferation of ethics-based AI frameworks deploying supposedly universal terms such as 'fairness' can obscure that the 'turn to ethics' in AI governance represents (or can be perceived to represent) a very particular choice in terms of the overall posture of regulation. In any sector – from corporate environmental issues to gender equality targets – ethical frameworks, at least as contrasted with law-based ones, are associated with voluntarism and self-regulation. In the context of the pervasive and increasing concentration of power in big tech (See Part 1 above), the decision to promote an ethics-based approach to the governance of responsible AI is itself a value-laden and essentially political decision. For instance, ethics-based approaches can be received by critical communities as unduly deferring to corporate interests, or as disconnecting AI governance issues from legal systems for the protection, review and remedy of rights.[6]

This is not to say that strategies to promote an overtly human rights–based approach to responsible tech governance is necessarily preferable to an ethics-based one, even if the former are at least more typically associated with formal rule-of-law frameworks. This is in part because 'rights' may not be any more culturally universal or neutral or content-certain than 'ethics'. Both sets of values (ethics and human rights) are attended by questions of cultural legitimacy and specificity, and the prospect of localised backlash against the perceived external imposition of values, as well as Western value-hypocrisy.

To the extent that 'ethics' and 'human rights' are competing framings for the governance of responsible technology, the ethics frame certainly appears to be dominant.

Human rights–based approaches to AI have gained far less traction, at least outside the EU. For example, the 2011 UN Guiding Principles on Business and Human Rights are largely invisible in debates over responsible AI.[7] Various explanations might exist for the relatively muted role of human rights in these debates globally. One is the more direct factor of corporate influence on these debates, where big tech prefers a non-legalistic 'ethics' framing. A more amorphous explanation is the longer-term secular decline of the human rights lexicon overall. This is the theory that as a result of things such as the backlash against globalisation, the perceived hypocrisy of Western rhetoric about the rule of law after the 2003 invasion of Iraq, and the perceived failure of the human rights project to deliver on socioeconomic terms, people in developed and developing countries are turning away from solutions or claims couched in universal human rights to more localised 'ordinary virtues'.[8] The UN Human Rights Council has not been driving an agenda on tech-related rights, perhaps as a function of populist disengagement by Western democracies from the multilateral human rights project, along with Beijing's incremental efforts to refocus UN-level human rights discourse on 'economic development' rather than civil and political rights.

What does this mean for Quad-level dialogue, including about frameworks for governing critical technologies? The promotion of value-based frameworks for AI governance is a site of geopolitical contestation for influence. It follows that Quad approaches to consensus-building on governance frameworks will require greater awareness of the socio-cultural issues associated with supposedly universal terms and norms. Quad countries will also need to assess the implications of choosing 'ethics', 'human rights', 'democratic freedoms' or other framings to promotes their goals. Backing an ethics-based approach might connote a corporate-led and voluntaristic framework disconnected from the 'rules-based order' rule-of-law rhetoric that accompanies other areas of foreign policy. On the other hand, backing a human rights–based approach is more difficult if democracies do not themselves engage with or agree on that approach, or have largely abdicated a lead in shaping the debate in international forums where such concepts might be advanced.

If both ethics and human rights carry 'baggage' in terms of cultural content or perceived external imposition, and do not necessarily connote a universal set of values that every society jointly identifies with, how would Quad member strategies around critical technologies such as AI both 'stay true' to their democracies' (varying) values, while also seeking to persuade others to prefer a broadly similar path?

A calculating approach might put human rights (and democracy) in the background and not lead with that frame. Instead, in 'pitching' or 'selling' a vision in the geopolitical competition over preferred political system type, the question might be 'what will resonate across diverse societies?' This may be about messages, assistance and engagement that speak to things that are useful to partner states, not just 'right'. In addition to greater responsiveness (rather than one-way projection of aims onto others), this might mean a focus on themes of economic prosperity and community utility and safety, helping societies strike a balance between integration with global technology trends, on the one hand – with some insulation from aspects of that exposure – and autonomy over the terms of it, on the other hand. Explicit human rights frameworks may be in the background or incidental.

Perhaps there are insights on how AI governance debates are often framed as 'responsible' or 'trustworthy' rather than 'human rights compliant'. Strategies and framings that promise and deliver technologies that are safe, beneficial, pro-social, transparent and trustworthy may gain more traction. Even in Australian government departments, for example, express use of 'human rights' terms can generate defensiveness, liability-thinking and resistance. Ultimately, regardless of the overarching framing, tech governance schemes will need to be embedded in national-level legal systems in order to offer credible systematic protection and remediation where there is demonstrable adverse impact on people or societies.

Human Rights and Ethics in Techno-social Systems: Implications for Values-based Diplomacy

This part explores two further implications of diversity and divergence for a values-led foreign policy for critical technologies. Importantly, critical technology diplomacy occurs in a broader context of geopolitical competition for influence and of concentrated private-sector power and influence. To gain traction with other partners in the region, conversations about critical technology governance will need to be seen to be responsive to other countries' needs – particularly less-developed countries. There is also a shared interest in ensuring local institutions have the capacity to adapt to critical technologies in ways that protect and enhance security, social cohesion and prosperity at the local level. Otherwise, there will be costs in terms of both human security and development goals, as well as wider regional stability and security.

Sore Points: The Risks of Reproducing Patterns of Domination and Exclusion

Quad policymaking ought to be alive to the risk of being seen to be perpetuating deeply resented patterns of domination, imposition and exclusion among societies that must import technologies and, often, the regulatory systems to govern them. This risk is particularly acute in the context of a broader geopolitical contest for influence in the Indo-Pacific, including in relation to technology and governance.

Inclusive, Not Imposed, Governance

If one of the perceived challenges for Quad democracies is to ask 'how do we sell our vision of a preferable political-economic order', the premise may already be off-target. This is because it continues the quasi-colonial approach of forming *our* vision (in this context, complete with 'our' technologies and 'our' cultural, etc., relationships with technologies) and seeking to take, project, export, sell, transplant it elsewhere. This is not partnership, really. A partner would ask countries – for example, in South-East Asia – 'what is *your* vision for the role of critical technologies such as AI in your societies, how can we help explore what is at stake? How can we plug you into debates about the governance of responsible innovation?' There is something counter-intuitive about promoting democratic values without participatory processes and approaches. Yet most countries are disconnected from processes and debates about the proper ways to govern data-intensive tech such as AI.

If technology is central to, and a central site of, regional competition or cooperation, then shaping the standards for responsible development and use of technology (and data) must matter equally. Unsurprisingly, a priority action of the new US National Strategy for Emerging and Critical Technologies is to 'lead the development of worldwide technology norms, standards and governance models that reflect democratic values and interests'.[9] This creates opportunities for inclusive leadership so that competition (and Quad cooperation) does not perpetuate historical patterns of neglect or marginalisation of non-dominant states. The articulation of existing ethical and other frameworks – such as the 2019 OECD one – around responsible development and use of critical technologies excludes voices of many affected states and groups within states. This is a digital divide not just in the familiar sense of access to technology, etc., but in terms of participation in dialogues about what societies want and need, and responsible ways to govern tech accordingly.

To engage effectively and with legitimacy in deliberations about appropriate tech governance and regulation, and to ensure an inclusive conversation about responsible or ethical AI, a far greater diversity of inputs is needed. Yet the vast majority of research on AI's social impact is EU- or US-based, and ethical frameworks such as the OECD one might be projected onto other societies in ways that obscure opportunities for inclusive dialogue about how governance should occur and by reference to what principles.

What does this mean for Quad-level dialogue and diplomacy? The foregoing opens up questions about the tone and audience for Quad-related dialogue on technology governance. Including tech-importing (and regulation-importing) societies into such conversations might hold considerable promise in terms of wider strategic alliance-building and consensus over the values at stake. After all, it is not obvious that all the tech innovations that matter will come from developed societies. Kenya's record of innovative 'mobile money' apps is a demonstration of how the developmental/poverty-reduction imperatives in some developing countries can yield tech-based solutions with far greater bearing on everyday lives. Likewise, it would be disrespectful (and so a poor way to 'sell' the preferable path of liberal societies) and not particularly democratic to presume that supposedly 'tech-poor' states have no interest or contribution to make to debates over what should comprise (to quote the US Emerging and Critical Technologies Strategy) 'worldwide technology norms, standards and governance models'.[10] It is not just about *leading* development of those models, but including and supporting other societies in those processes.

> **Quad countries may be less about 'selling' a vision of critical tech's role in society, and more about creating forums and platforms for dialogue and model-building, so demonstrating the very values of openness and transparency that Quad countries seek to persuade others to follow.**

Moderating the Amplification of Inequality

It is also imperative to recognise the links between new technologies such as AI/ML and entrenched patterns of inequality, discrimination and bias more generally. This is a function of the earlier point about technologies not being value neutral. There is ample evidence of how AI-based systems can amplify social inequality, bias and discrimination across and within societies. This connects the 'ethical AI' debate with the longer-standing 'digital divide' one (which also relates to skills differentiation, access issues, and so on). For one thing, many parts of the world have a very small digital footprint and are not represented in the data-sets used to train AI systems. Parts of communities may be excluded from participation in tech advancement even as this transforms their lives and livelihoods, further exacerbating and marginalising certain communities (except perhaps as consumers or subjects of technology). On one view, big tech is a form of extractive industry that is not simply providing a service but gathering data from users, in ways that might reinforce existing inequalities. AI-related systems that are very expensive to train at scale, reinforce monopolistic firms. Development-oriented policymaking has not adequately assessed what these patterns mean for efforts to advance the poverty-reduction and inequality agendas, for example. The benefits of AI may be very unevenly distributed both within and between societies.

What does this mean for Quad-level dialogue, including about frameworks for governing critical technologies? Critical technologies are prioritised in national and foreign policy because of their relationship with both security *and* prosperity. Diplomacy will need to strike a careful balance between both – and, particularly for lower-income countries, not be seen as trading prosperity away for the security of other countries. Moreover, the tech-related amplification of social exclusion, inequality and extraction may hold implications for social cohesion and stability in Indo-Pacific countries and for geopolitical alliance-making. If Quad members are concerned to persuade countries faced with a choice of strategic partners and a choice of political systems, what are Quad countries doing to integrate support for localised, country-specific critical tech initiatives into development assistance, market development and trade access initiatives for less-developed economies? The history of counter-terrorism cooperation, for example, suggests that Quad countries not ask 'what can partner countries do for our security, but what can we help do for theirs?' Likewise, there is a risk that the 'critical technologies' policy space becomes focused on what commitment powerful democracies can get from less-developed states, rather than what they can do to help those states imagine and engage with their own priorities. This would repeat the historic pattern of *extraction* from 'peripheral' societies, with associated backlash and resentment.

Red Flags: Sovereignty Over and Trust in Local Institutions Amid External Influence

A third dimension around the social impact of critical technologies such as AI is related to the 'external imposition of values' and 'digital divide' concerns in Part 2 ("Unintended Consequences") and Part 3 ("Sore points") above. How might Quad members – in their own societies and within trading and developmental partnerships – develop strategies for countering the negative impact that critical information-based technologies such as algorithmic social media and news recommendation platforms might have on social cohesion, perceived insecurity and trust in institutions at local levels?

Alongside the accelerating 'digital divide' within and between countries in terms of development and economic prosperity are other pervasive impacts of critical technologies. These may, on aggregate, be significant in terms of social cohesion and perceived insecurity, as well as the sovereignty and traction of localised institutions. It is one thing to note the risks (and related resentments) of cultural impositions or colonialism in terms of how some societies may feel excluded from dialogue about values-based frameworks for the governance of key technologies, and find these imposed upon them. A more subtle effect, however, is the existence of pathways for influencing, much more broadly and profoundly, national experiences of and visions for technology and its governance, and indeed for influencing overall social and political calibrations on certain values. This risk flows from the observation above that values are not fixed, but change and evolve through time.

Data-driven information technologies create unprecedented scope for external forces to shape far-off societies and polities in unprecedented ways. This may result from calculated sustained efforts, but may also be an externality of the uptake of certain global tech products and platforms.

If those products embed or reinforce particular values or viewpoints, this might generate backlash sentiments as people realise how their own cultural sovereignty is undermined or diluted or appropriated. This is a now familiar reaction: there is a strong argument that the rise of populism, and democratic backsliding, in the second decade of the 2020s is associated with resentment about rampant globalisation of the '90s and '00s.

In the face of pervasive and sometimes amorphous tech-enabled influence across borders and around institutions, this is ultimately a concern about the resilience and responsiveness of local institutions and local sovereignty over how these institutions operate or are designed in future. Development discourse has long focused on the need for resilient and responsive institutions in less-developed countries, and how local institutions both shape societies and are shaped by them. Yet now interconnectedness and newer technologies mean that societies (and sub-groups within them) are directly reached and influenced from abroad in ways that are not based on their own values or historic data patterns.

Whole groups may be unaware of how values embedded in or promoted by certain platforms are subtly, but at scale, changing the terms of their routine societal debates.

External actors with varying degrees of deliberate manipulative agenda – whether big tech platform monopolies, or techno-authoritarian states – might make choices or decisions that impact on overseas citizens' rights or significantly shape their sociopolitical experiences and debates, often in circumstances where 'detection' or recourse is difficult or impossible. Localised governance institutions are not necessarily influential in such contexts, and may be bypassed or undercut as effective forums, compounding the public's issues of engagement, trust and responsiveness with institutions.

This point relates to unconscious adoption or the subtle shaping of views and preferences from abroad. In conscious terms, there is some scope for fears and uncertainties about perceived undefined and misunderstood critical technologies 'from abroad' to feed into existing fault-lines in divided societies or to amplify distrust in general terms. The existing perception in many developing countries that amorphous but non-benign external forces are seeking to extract from or intervene in one's society is perhaps only heightened by algorithmic 'autonomous' social media or investment platforms and other technologies. The sense by people of being exposed to (and even 'tracked' by) external influences through technology might feed into feelings of insecurity and vulnerability that then discredit the discourse on rights and freedoms that supposedly makes democracy and open markets the preferable political-economic system. It is not obvious what such insights entail in terms of policy interventions, especially given the significant variation (even within 'like-minded' democracies) in terms of legal and ethical frameworks on issues such as data privacy.

Privacy Rights and Data Governance: A Case Study

Data is a key input into many critical technologies. The market for data is huge, expanding and global. But the ease with which data can be transferred across borders belies the differences that exist in national law for the processing and transfer of data. This part examines divergences in legal regimes relating to data. In doing so, it presents a case study of how countries are balancing the drive towards common standards, and the need to acknowledge and accommodate difference.

Local legal-cultural and constitutional traditions and, more recently, impulses by governments to localise laws, policy and supply chains exert a gravitation pull. This is even as there are compelling economic and strategic – and, perhaps, principled – arguments for more standardised data protection regimes, especially among otherwise like-minded democracies.

Data Governance: Sources of Difference and Plurality

Understanding several key qualities of data helps to explain the divergences in data governance regimes between countries. Specifically:

- Sensitive inferences can be drawn from relatively innocuous data. The Cambridge Analytica/Facebook scandal highlighted how data processing might have a significant impact on democratic institutions. That scandal also catalysed public support for, and government action towards, more robust privacy protection in legislation.
- Data is a 'non-excludable' good – there are multiple uses possible from the one data-set, alone or in combination with others, and its use in one context does not diminish its value in another.
- The boundaries between public and private uses of data are incredibly blurry. This was highlighted by recent controversy in Australia over the relationship between law enforcement agencies and US tech firm Clearview AI, which is said to have scraped some 3 billion online photos to build a facial recognition service.[11]
- Governments both regulate private data transfers – itself a balance of economic and social/political interests – and make policy for government access and use of data – for example, for national security purposes. Thus, the sites for data governance include both domestic and international private and public law.

Reflecting these qualities, the purposes of data governance regimes are manifold: they involve the protection of certain social and political values and rights (e.g. freedom of expression, freedom of information and freedom of assembly). But they also have an important instrumental purpose: controlling data's downstream applications – for economic, security or other purposes. Even within the one polity there are also multiple regimes and stakeholders in play – with often competing purposes and interests. Thus, in analysing a country's approach to data governance, there is a need to examine both data privacy/protection legislation and policing/national security–oriented legislation aimed at accessing private data. At the core of both protection *and* access regimes are local legal-cultural interpretations of the rule of law and political values, including human rights.

Trends in Diversity and Convergence

The European Union General Data Protection Regulation (GDPR)[12] has been positioned as the global high-water mark in terms of the protections it affords for personal data. Positioned as such, the GDPR, which was adopted in 2016 and came into force in 2018, has had an important influence on the reform of data privacy legislation in a range of jurisdictions. This influence has been mapped to several policy developments in Indo-Pacific jurisdictions including Quad countries. Despite the GDPR's influence, however, significant disparities between national approaches remain – even between like-minded democratic nations.

Constitutional and Definitional Differences

The disparities are reflected in, and arguably even stem from, the differences in the respective constitutional guarantees provided for in national law. For instance, although India, Japan and the US have a long history in relation to the discussion of a constitutionally guaranteed right to privacy, there is no right to privacy recognised in Australian law. This is despite Australia's commitments in international human rights frameworks, in particular the 1966 International Covenant on Civil and Political Rights, and state- and territory-level human rights charters, which recognise a right to privacy. That said, while Australia does not have a constitutionally protected right to privacy, its highest court has left the door open to recognising a privacy right at common law. Australia does not have a constitutional or statutory bill of rights. As Part 2 above notes, this points to the need to understand the legal-cultural history of a jurisdiction in order to appreciate the value it attaches to privacy, and its approach to policy and law.

Even where the right to privacy is constitutionally recognised, there are key differences as to how 'privacy' is understood and interpreted. Privacy is a notoriously amorphous and malleable term,[13] and its precise meaning varies according to time, place and context. For instance, privacy law in Japan has traditionally reflected a culture of respecting the public good at the expense of private interests.[14] While Europe has a long tradition of protecting the right to privacy, as enshrined in the 1953 European Convention of Human Rights[15], the European Court of Human Rights (ECHR) has allowed the right to serve many ends. Some cases equate privacy with 'seclusion' or 'intimacy', while others see it extending to protection for freedom of action, self-determination and autonomy. Further, in the EU, data protection and privacy are recognised as distinct rights in the Charter of Fundamental Rights of the EU, despite their overlapping bodies of jurisprudence. These rights are also informed by a complex interplay between national, EU and ECHR rights protection jurisprudence.

International Data Transfers as a Key Cooperation Issue and Metaphor for Wider Trends

Despite the national disparities underlying its interpretation, the GDPR has influenced law reform across Quad countries. For example, California's recently enacted *Consumer Privacy Act* is arguably a move towards a more 'European' approach. There is academic debate as to whether the Californian Act reflects an 'adoption' by the US state of a European model, or instead is a unique approach spurred by a regulatory 'race' on either side of the Atlantic. On either interpretation, the GDPR has proved agenda-setting.[16] This is also evident in India where the 2019 Personal Data Protection Bill, largely speaking, tracks the GDPR and is currently under debate with adoption likely in early 2021.

The GDPR's influence, however, is not just a function of it being seen as a legislative high-water mark. The Regulation applies extraterritorially. And the EU restricts transfer of data to countries that do not provide an equivalent level of protection. Other countries therefore have economic and trade stakes in looking to GDPR standards. Of note, Japan received a GDPR adequacy decision in 2019 from the European Commission, allowing for the free flow of personal data between the jurisdictions. Although distinct, this agreement is significant for the 2019 economic partnership agreement between the two jurisdictions.

Australia does not have an adequacy agreement, an important point considering the ongoing Australia–EU trade negotiations and where adequacy may be treated as distinct from trade. Australia's approach to data privacy has traditionally been much more business-friendly than the EU's human rights–centric approach. Although Australia has an omnibus regime – the *Privacy Act 1988* – this framework provides broad carve-outs that differentiate it even from the GDPR's predecessor,[17] let alone the protections provided for in the modernised Regulation. The *Privacy Act* also takes a narrow interpretation of 'personal information'[18] and provides a limited role for consent. Such substantive differences act as an impediment to the free flow of personal data between the EU and Australia. This has prompted calls for Australia to consider privacy reform – including from the Australian Competition and Consumer Commission (ACCC).[19]

The EU and the US also have a complex history on data transfer. In a 2015 case known as 'Schrems I', the EU Court of Justice invalidated the European Commission's adequacy decision that had underpinned the EU–US 'safe harbour' arrangement for data transfer between the two jurisdictions.[20] In 2020, the Court's Schrems II decision then invalidated the legal basis for the predecessor transfer arrangement – the US 'privacy shield'.[21] The Schrems II judgment will have a major impact on the validity of international data transfers going forward, with the implications of the Court's ruling extending far beyond its impact on the US–EU relationship and privacy shield scheme. The judgment clarifies that if there is no adequacy agreement between the EU and a third country, then those exporting personal data are expected to examine the circumstances surrounding *each* transfer and to assess whether the protections provided in the third country are essentially equivalent to those provided for in the EU.

As there is no EU–Australia adequacy agreement, the Schrems II ruling is of significant importance. Moreover, even significant reform to the *Privacy Act* may not bring Australia in line with GDPR standards. In Schrems II, the EU Court of Justice was particularly concerned with law enforcement access to data and individual redress against national security and intelligence services. Given Australia's membership of the 'Five Eyes' intelligence arrangement and the extensive powers afforded to law enforcement agencies under, for instance, the *Data Retention Act*[22] and the *Telecommunications Legislation and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA)*,[23] whether personal data can be transferred from the EU to Australia is in significant doubt.

What does this mean for Quad-level dialogue, including about frameworks for governing critical technologies? International data transfer regimes showcase the significant hurdles to cooperation, even amongst like-minded democratic nations. In this, they provide a strong metaphor for the wider challenges of siloed national responses to the development and use of technology. While this part has focused on data transfers between Quad countries and the EU, similar disparities are also an impediment between the Quad countries. For example, Australia's *Privacy Act* restricts the transfer of personal information internationally in some cases. Indeed, the future efforts of Quad countries to align themselves more with the GDPR might also deepen disparities in the region. This serves as a reminder that Quad members need to look both inwards and outwards – since critical technology supply chains are fairly global, and one of their fundamental inputs (data) is on one level largely borderless.

A number of other implications flow from this case study, of relevance to how Quad countries, alone or together, might approach rights- and values-based standards for critical technologies:

1. Historical and legal conceptions of privacy: Privacy concerns also extend beyond data transfer regimes. Privacy is a core concern animating debates about governance regimes for smart cities, facial recognition and biotech. But this case highlights the fundamental differences in how the right to privacy is interpreted and embedded in different national legal traditions (if at all). Significantly, privacy and data transfer schemes build on centuries-old legal traditions, and the constitutional underpinnings of different countries. However, how a country deals with privacy rights in relation to one application (e.g. data transfer) could affect its credibility in promoting rights-based approaches in relation to other, newer applications (e.g. facial recognition).

2. The tension between strategically useful standards among 'like-minded' and domestic sovereignty and security interests: When assessing differences – and prospects for greater harmonisation – both private and public law matter. Today's critical technologies involve inherently dual-use, if not multi-use, inputs and applications. This reality adds even further complexity to the trade-offs involved in how governments use and regulate critical technologies, as both public and private law are engaged. Quad countries may perceive they have a strategic, or even security, interest in advocating for common standards on data governance. But more harmonisation at an intergovernmental level has implications for domestic sovereignty and autonomy – and will require them to make deliberate trade-offs about how they use and access data domestically for national security and policing purposes.

3. The pull of sociocultural tradition: From a trade and economic perspective, it is clear that a more coordinated approach to data governance is needed at both the national and international level. However, disparities exist due to real sociocultural variations, and the way in which legal systems and institutions have evolved over time. The question thus becomes one of when – and how – we might learn to live with some difference while at the same time respecting certain key rights and values and the rule of law.

COVID-19 highlights the significance of critical data-driven technologies. Picture: Martin Sanchez / Unsplash, https://bit.ly/3cjd0h8

A Forward Agenda

Despite – and in some cases because of – the differences and divergences between Indo-Pacific countries' approaches to critical technologies, there is scope for further cooperation. The key challenge for critical technology diplomacy is determining where it is viable to aim for common standards – or shared understanding about the meaning of standards – and where it is better to accept difference. This final part sets out a forward agenda for how Australia, and other Quad members, can approach this dilemma, and identify and prioritise areas for cooperation. It argues that the guiding approach need not be explicitly based on democracy promotion, or 'techno-democratic statecraft',[24] since there are Indo-Pacific countries that are not electoral democracies, but with whom common ground can be found.

Indeed, Quad members jointly and in their own spheres will be best able to protect democratic values and human rights (broadly defined) through an inclusive and open approach to promoting technologies and the systems intended to govern these. The key insights of this part are that:

1. The ***process*** for dialogue about critical technology governance should be multi-stakeholder and inclusive – from the national level to mini-lateral efforts such as the Quad, to multilateral standards-setting efforts.

2. In ***substance***, critical technology standards and governance frameworks should reflect the interests and values of diverse groups, both within and across countries, be responsive to the risks of widening digital inequality, and empower local institutions to absorb the political and economic changes brought about by rapidly changing technology.

The recommendations that follow are all process orientated and designed to have an influence on substance as opposed to speaking to substance directly – thus, for example, not making any substantive recommendations as to harmonised legal frameworks. This reflects this paper's message of acknowledging difference within Quad countries. The Quad's focus ought to be on processes that are inclusive and might develop balanced substantive rules, etc., that respect diversity amongst the Quad and other countries, processes that are capable of exerting substantive influence in terms of promoting openness, democracy, the rule of law and human rights.

Starting Local: Australia's Role

DFAT: A Fulcrum for Overcoming Difference

A major challenge for critical technology diplomacy is the extreme difficulty *even just at the national level* of getting a cross-government 'grip' on the tech governance agenda. This is partly because of a lack of digital literacy even among developed country regulators, legislators and policymakers. It is also because national-level agencies have competing mandates and stakeholder interests. For example, the case study in Part 4 showed tensions between legal regimes focused on protection and restricting access, and those focused on opening access. Similarly, other papers in this series have highlighted divergences between Quad countries' approaches (for instance, on national identity, and law enforcement and government use of facial recognition in Australia), where deeper cooperation may necessitate trade-offs between domestic imperatives and foreign policy objectives. Regional consensus seems some way off where national strategies are still coming together. Further, the lack of domestic mechanisms for progressing the critical technology governance agenda arguably inhibits scaling up these conversations to the multinational level.

These challenges point to the opportunity for DFAT to play a convening role – indeed to act as a bridge between foreign policy and domestic policy on various aspects of the critical technology agenda.

This may be a non-traditional role for a foreign affairs department to play – looking both outward and inward. However, critical technology diplomacy faces something of a 'chicken/egg' dilemma: to

The technical aspects of critical technologies are intimately connected to their sociocultural aspects. Picture: Robert Bauernhansl / Ars Electronica, https://flic.kr/p/WMNtZC address divergences between even like-minded countries there is a need to simultaneously understand and address differences inside domestic systems.

In this, a foreign affairs department is well placed to understand the strategic context, and to engage with the wide set of state and non-state actors with power and influence over technology development, use and regulation. It is also best placed to communicate these back to domestic audiences, to build an understanding of whole-of-government objectives, and assess how aspects of domestic policy advantage or curtail opportunities for diplomacy.

Quad-level Dialogue: Inclusive, Informed and Informative

Modelling Inclusivity

Given the pluralistic nature of tech governance, the power and influence of tech companies, and the inherently socio-technical nature of critical technologies, there is a need for a more multi-stakeholder dialogue on these issues. In particular, there is an opportunity to extend Quad dialogue well beyond ministerial and official meetings. More track 2 and multi-stakeholder networks involving civil society, business and university perspectives on technology governance, rights and values could then feed into ministerial-level Quad dialogue. This could be done, for example, via:

- **Educational exchange:** scholarships and short courses for emerging or key officials in relation to the governance of responsible technologies, between different Quad countries.
- **Private sector engagement:** brokering links, dialogue and opportunities for partnerships between leading technology developers (and users) on a bi-, tri- and quadri-lateral basis, and scoping possibilities for public–private partnerships.

The Quad may be a convenient 'starting point' for these non-state networks. However, there is significant scope to use these as platforms for wider engagement. For example, university-level partnerships could be scaled to include non-democratic states, especially on 'applied' issues such as building consensus on responsible AI applications, and on sharing insights into different societies' experiences and approaches.[25]

Sub-regional Feeder Dialogues

Partner countries need to be, and feel, involved in this process. In creating opportunities for dialogue outside of the Quad construct, members can demonstrate the key concepts of participation, inclusion, procedural fairness and respect, allowing partner states a role in shaping tech governance values (rather than projecting 'our' values or trying to tout or sell these pre-made). This might involve helping to convene sub-regional dialogue on responsible governance of principled AI and other data-based technologies, where the emphasis is on inclusivity and diversity of perspectives (rather than 'pushing and persuading' on the adoption of certain values or frameworks).

Influencing the Regional Critical Technology Agenda through Consensus Statements

Quad countries can help shape the regional critical technology agenda, and inform domestic-level policy debates on values and critical technology, including by crafting joint statements, sharing vulnerability assessments and information on best-practice security practices, building a shared picture of supply chain vulnerabilities, etc. Where the Quad can develop consensus views, this could bring credibility – indeed because of the four countries' differences, rather than because of their shared democratic heritage – and could help other countries in the region make informed decisions.

Action Outwards

A growing number of fora for conversations about critical technology governance makes choosing where to prioritise effort important. There is significant utility in Quad partners maintaining and deepening dialogue, at the same time as Quad participants – acting together or alone – participating in other dialogues and engagements, including with 'non-like-minded' and non-regional partners. Quad members should prioritise:

- **Reigniting human rights frames at the UN level, but leading with practical frames at the local level:** Quad members should consider the benefits of more deliberate engagement with 'technology and human rights' debates and processes in the UN-based multilateral human rights system. High-level principles and rights alone are insufficient to prompt real action at the state level, but are an important step. However, as Part 2 discusses, there is a risk of no-traction or reactance to overt rights-based strategies. While maintaining a constructive human rights dialogue at the international level is an important long-term objective, in the short- to medium-term diplomacy at the regional may be best placed to background human rights and ethics concerns, and to focus on issues of concern to partner countries. Particularly as these countries recover economically in the post-COVID world, there is an opportunity to explore critical tech governance through frames of economic development, prosperity, sovereign autonomy and supply chain diversity (through vectors such as competition regulation and consumer protection).
- **Focusing on applied standards:** A key challenge for critical technology diplomacy is giving practical effect to broad values in ways that do not simply extend divergent approaches under the fig leaf of joint approaches. For example, APEC's four digital principles ('awareness', 'responsibility', 'cooperation' and 'privacy') do not necessarily point in any distinct policy direction, and are broad enough to mean almost anything. Likewise, the seven 'implementation strategies' to give effect to these principles.[26] There is a clear need to move beyond words to action. One way to address this is to focus on industry/professional standard-setting for near-term applications of critical technologies – to create 'worked

examples' of governance in applied contexts, rather than high-level principles for technologies in general. What greater support, investment and time could Quad members be giving to efforts in the near term (2020–2022) at principled professional standardisation around critical technologies (notably, the ISO process via its Working Groups on Trustworthy AI standards[27])? Standards-setting can also help move the needle on *domestic* debates too since they are transnational/co-regulatory.

- **Practical assistance across the 'digital divide':** Quad members can support developing standards by 'doing'. For example, via public–private partnerships with less-developed countries, Quad countries might engage in scaling-up digital development assistance methodologies in Indo-Pacific least-developed countries (LDCs), with a focus on principled and trustworthy governance of critical data-based technologies. This might include:
    - o Assistance to less-developed countries in the Indo-Pacific with technology and data-related consumer protection and competition and media freedom legal frameworks, including in the context of trade partnership agreements.[28]
    - o Assistance to LDCs with methodologies for assessing the social and institutional impacts of AI and related technologies, including in relation to integrity of electoral systems.
    - o More explicit consideration of the digital dimensions to development policy, including around human rights and ethical uses (e.g. DFID/FCO approach),[29] and promotion of inclusivity frameworks with appropriate rights protections (e.g. WEF scheme).[30] This includes targeted demonstrations of the developmental and humanitarian applications of data-driven technologies so as to reinforce the advantages of approaches that are explicitly pro-social and grounded in principle.
    - o Schemes to help increase the awareness, literacy and confidence of less-developed partner officials in relation to AI and other technologies (and data) and of the governance of these, in keeping with the theme of inclusive partnership.
- **Prioritising data protection and governance frameworks:** Data is the basic building block of so many critical technologies – from AI to emerging biotechnology applications. However, data governance remains characterised by divergence and difference. Quad members should support platforms and working groups pursuing legal harmonisation on issues of data governance in the context of human rights. While Japan has an adequacy agreement with the EU, without such an equivalent Australia and to a lesser extent India might struggle to find a role in diplomatic approaches that might increase EU–US convergence on data privacy/protection post-Schrems II.

We are governed by both state-made laws and a complex constellation of national, international and transnational frameworks and schemes. Picture: Christopher Sonnleitner / Ars Electronica, https://flic.kr/p/T2qSmk

Conclusion: 2021 – A Window of Opportunity?

COVID-19 has opened a real, if fragile, window of opportunity for progress on reconciling divergence and difference in critical technology governance at both the domestic and multilateral levels.

COVID-19 has heightened attention on the significance of critical data-driven technologies. AI, big data modelling and tracking apps have all played high-profile roles in the pandemic response. The working-from-home trend has revealed the importance of a high-quality national internet infrastructure backbone. The rollout of biotechnologies (especially various vaccines) could present an opportunity to shape a much broader narrative around benevolent technology, and trust in the institutions promoting and regulating it. It could also open opportunities for inclusive dialogue and capacity-building on how different societies wish to set their technology governance calibrations consistent with their own preferences.

But there is a need to be realistic about what is achievable. Coming on top of rising US–China tensions, COVID-19 has also exacerbated conditions unsuitable to harmonisation and cooperation: the quest for digital autonomy and sovereign capability, public distrust of government and corporate tech platforms, and the use of public health motifs to curtail political and civic space online and in the physical world.[31] These countervailing trends will need to be managed to ensure enhanced cooperation on critical technologies is both successful and sustainable.

In a COVID-and-after world, critical technology includes biotech and biometric contexts such as epidemiology, testing, vaccine and treatment technologies. Picture: CDC / Unsplash, https://bit.ly/3pkKKyd

Endnotes

1. Adapted from Australian Government Department of HomeAffairs. (2020). *Australia's Cyber Security Strategy 2020.* https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
2. See, for example, Australian Foreign Minister Marise Payne. (4 June 2020). 'Australia and India agree new partnership on cyber and critical technology.' Media release. https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-and-india-agree-new-partnership-cyber-and-critical-technology
3. For one diagrammatic representation, see Jessica Fjeld and Adam Nagy, Berkman Klein Center for Internet and Society. (15 January 2020). 'Principled Artificial Intelligence: A Map of Ethical and Rights-Based Approaches to Principles for AI (graphic).' Berkman Klein Center for Internet and Society. Harvard University. Fabric of Digital Life. https://fabricofdigitallife.com/Detail/objects/4740
4. Organisation for Economic Co-operation and Development. (2019). 'OECD Principles on AI.' https://www.oecd.org/going-digital/ai/principles/
5. Beijing Academy of Artificial Intelligence (BAAI). (2019). 'Beijing AI Principles.' https://www.baai.ac.cn/news/beijing-ai-principles-en.html
6. Meanwhile, in Australia and elsewhere, a two-track ethical debate has developed around civilian vs military usages of AI. For example, military contexts were explicitly excluded from the federal government's Data61/CSIRO 'Australian Ethical Framework on AI' process 2018–19. See https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/
7. Human Rights Council resolution 17/4, *Human rights and transnational corporations and other business enterprises.* A/HRC/17/31 (16 June 2011). Access via https://daccess-ods.un.org/TMP/4127027.98843384.html
8. See Michael Ignatieff. (2017). *The Ordinary Virtues: Moral Order in a Divided World.* Harvard University Press. In Europe, however, there is if anything an increasing focus on approaching the governance of data and data-based technologies through a human rights framework (e.g. the new Committee on Artificial Intelligence (CAHAI) set up by the Council of Europe).
9. U.S. Federal Government White House. (October 2020). 'National Strategy for Critical and Emerging Technologies.' 7. https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf
10. 'National Strategy for Critical and Emerging Technologies.' (October 2020). 7.
11. Ariel Bogle. (13 July 2020). 'Documents reveal AFP's use of controversial facial recognition technology Clearview AI.' ABC News. https://www.abc.net.au/news/2020-07-13/afp-use-of-facial-recocognition-sofware-clearview-ai-revealed/12451554
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 1–88.
13. See, for example, Daniel Solove. (2006). 'A Taxonomy of Privacy.' *University of Pennsylvania Law Review* 154(477).
14. See Hiroshi Miyashita. (2011). 'The Evolving Concept of Data Privacy in Japanese Law.' International Data Privacy Law, 4(1), 229.
15. Article 8(1) provides that 'Everyone has the right to respect for his private and family life, his home and his correspondence'.
16. See Paul Schwartz. (2019). 'Global Data Privacy: The EU Way.' *New York University Law Review*, 94(4); Anupam Chander, Margot E. Kaminski and William McGeveran. (Forthcoming). 'Catalyzing Privacy Law.' *Minnesota Law Review* (last revised 24 April 2020). http://dx.doi.org/10.2139/ssrn.3433922.
17. The Data Protection Directive (Directive 95/46/EC).
18. Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4.
19. In its 2019 Digital Platforms Inquiry, the ACCC questioned 'whether the Privacy Act should be revised such that it could be considered by the European Commission to offer "an adequate level of data protection" to facilitate the flow of information to and from overseas jurisdictions such as the EU': see recommendation 17(6).
20. Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650 14.
21. Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems,* ECLI:EU:C:2020:559.
22. The Telecommunications (Interception and Access) Act *1979* (Cth) (TIA), updated by the Telecommunications (Interception and Access) Amendment (Data Retention) Act *2015* (Cth) (Data Retention Act).
23. The Telecommunications Act *1997* (Cth), updated by the Telecommunications Legislation and Other Legislation Amendment (Assistance and Access) Act *2018* (TOLA).

24. Martijn Rasser (Center for a New American Security). (January 2021). ‘Networked: Techno-Democratic Statecraft for Australia and the Quad.’ Edited by Katherine Mansted and Rory Medcalf, Quad Tech Network Series: National Security College, Australian National University, 2021.

25. An existing example that includes elite Chinese institutions is Microsoft Asia’s ‘Dialogue on AI Governance’ academic network 2019–2021 (Peking University, Tsinghua University, Tokyo University, Seoul National University, National Law School Delhi, Singapore Management University, Australian National University).

26. APEC Telecommunications and Information Working Group. (November 2019). ‘APEC Framework for Securing the Digital Economy.’ https://www.apec.org/Publications/2019/11/APEC-Framework-for-Securing-the-Digital-Economy

27. See ISO/IEC JTC1/SC 42 Artificial Intelligence. (2017). https://www.iso.org/committee/6794475.html

28. For example, New Zealand Ministry of Foreign Affairs and Trade. (2020). ‘Digital Economy Partnership Agreement (DEPA).’ https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement/

29. UK Department for International Development. (23 January 2018). ‘DFID Digital Strategy 2018 to 2020: Doing Development in a Digital World.’ https://www.gov.uk/government/publications/dfid-digital-strategy-2018-to-2020-doing-development-in-a-digital-world/dfid-digital-strategy-2018-to-2020-doing-development-in-a-digital-world; see also Principles for Digital Development. https://digitalprinciples.org/

30. World Economic Forum. (12 May 2016). ‘Internet for All: A Framework for Accelerating Internet Access and Adoption.’ https://www.weforum.org/reports/internet-for-all-a-framework-for-accelerating-internet-access-and-adoption

31. See Trish Ray, Arjun Jayakumar, Sangeet Jain and Anurag Reddy (Observer Research Foundation). ‘The Digital Indo-Pacific: Regional Connectivity and Resilience.’ (January 2021). Edited by Katherine Mansted and Rory Medcalf, Quad Tech Network Series: National Security College, Australian National University, 2021. This paper forecasts increased regionalism and localisation in relation to digital economies.

About the National Security College

The National Security College (NSC) is a joint initiative of The Australian National University and Commonwealth Government. The NSC offers specialist graduate studies, professional and executive education, futures analysis, and a national platform for trusted and independent policy dialogue.

T +61 2 6125 1219

E national.security.college@anu.edu.au

W nsc.anu.edu.au

@NSC_ANU

National Security College

CRICOS Provider #00120C