Australian National University

TECH POLICY DESIGN CENTRE

MAY 2022

Tending the Tech-Ecosystem

who should be the tech-regulator(s)?

01

About the Tech Policy Design Centre

The Tech Policy Design Centre (TPDC) is a nonpartisan, independent research organisation at the Australian National University. TPDC's mission is to develop fit-for-purpose tech policy frameworks to shape technology for the long-term benefit of humanity. We are working to mature the tech-governance ecosystem, in collaboration with industry, government, civil society, and academia.

About the Authors

Johanna Weaver is the Director of the Tech Policy Design Centre
Sarah O'Connor is a Research Assistant at the Tech Policy Design Centre
With invaluable support from: Harry Rolf, Claire Irvine, Mitchell Henson, Tanvi Nair, and Ben Gowdie.

Independence Statement

Our work is made possible by the generous support of external funders from government, industry, and civil society. In all instances, TPDC retains full independence over our research and complete editorial discretion with respect to outputs, reports, and recommendations. If you would like to know more or support our work, please contact us at techpolicydesign@anu.edu.au

Acknowledgements

The TPDC acknowledge the Ngunnawal and Ngambri people, who are the Traditional Owners of the land upon which this report was prepared. We pay our respects to their elders, past, present and emerging.

This report was prepared by TPDC, with thanks to generous sponsorship from Microsoft.

TPDC thanks the 32 heads and senior representatives of Australian regulators, the Australian Government, industry, and civil society for generously giving their time to be interviewed.

TPDC would also like to thank Amit Singh and Jensen Sass for their case studies, as well as the contributing authors of the 13 jurisdiction overviews, for producing such high-quality summaries in compressed timelines: Rogier Creemers, Kadri Kaska, Elsa Neeme, Patryk Pawlak, Cherie Lagakali, Lola Attenberger, Jhalak M. Kakkar, Shashank Mohan, Bilal Mohamed, Mira Swaminathan, Hiroki Habuka, Mark Williams, Matthew G. O'Neill, Caitríona Heinl, Yong Lim, Sangchul Park, Haksoo Ko, Jonggu Jeong, Eunjung Cho, Haesun Lee, Benjamin Ang, Sithuraj Ponraij, Jose Tomas Llanos, Diana Bowman, Nicholas Davis, and Walter G. Johnson.

Finally, TPDC thanks all who peer reviewed this work and provided considered and insightful feedback, including anonymous reviewers and Jolyon Ford, Ellen Broad, Will Bateman, Jensen Sass, Belinda Dennett, and Amy Denmeade.

This research was conducted in accordance with the National Statement on Ethical Conduct in Human Research and was approved by the Australian National University's Research Human Ethics Committee (Human Ethics Protocol 2022/105).

The report's cover was illustrated by the Australian artist Bill Hope, The Jacky Winter Group, and the report's layout designed by the team at Black Bear Creative.

Contact

Tech Policy Design Centre
Level 3, Birch Building
The Australian National University Canberra ACT 2601, Australia
techpolicydesign@anu.edu.au

CRICOS Provider: 00120C

This report was sponsored by:

Table of Contents

****

Imagine a community garden, with no fences or barriers to define its boundaries, but with an order nonetheless - as though it was intended to be that way. A variety of flowers and plants can be seen growing harmoniously together, many of which would not normally interact in the wild. Some are edible, many bright and beautiful, others exotic and a few potentially harmful to the uninitiated.

A closer look reveals a system, characterised by many symbiotic relationships. The native flowers draw pollinators to the veggie patch. The shadow of a sapling shelters violets at its base, which in turn keeps weeds at bay. Gardeners move freely among the flowers and plants with the skill and care of experience. A plant that has grown too wild is pruned. A mature tree is carefully monitored to ensure its spreading canopy does not block nourishing sunlight needed below. The branch of a shrub bending under the weight of a beehive is supported by twine taken from the gardener's toolkit. In a sheltered corner, a community member nurtures a new varietal into splendour.

****

****

This vision of a well-tended, thriving garden is a metaphor for the role of effective regulators in cultivating the digital technology ecosystem; the gardeners are synonymous with regulators.

Like gardeners, effective regulators cultivate innovation and growth. They also weed out harmful practices and products that threaten to outcompete or overrun the ecosystem. But, if regulators exert excessive control, they risk curating a staid formal garden with little innovation or new life. At the opposite end of the spectrum: an uncontrolled jungle. In the middle: the community garden depicted above.

Community gardeners don't operate in isolation; they use tools given to them and work within the boundaries set by landscape architects (politicians and policymakers to the regulators). Mirroring disruption in the tech sector, gardens can be subject to unforeseen shocks, like drought and flood.

Importantly, a flourishing garden is not simply attributable to the interventions of the gardeners. It is the interaction between all the systems within the garden that fosters life and growth (i.e., a gardener plants flowers, that attract bees, that pollinate other plants, and then go on to produce honey). The best gardeners have a deep understanding of, and respect for, these interdependencies. They work to counteract power imbalances between systems (i.e., between mature and emerging plants) and nurture symbiotic relationships that minimise the need for intervention at all.

Just as a thriving garden requires tending by an effective gardener (that is, a gardener with skills, knowledge, and resources), the tech-ecosystem will flourish when it is tended by well-resourced and skilful regulators that understand the interests and interdependencies of each constituent part of the ecosystem. In this way, the role of the regulator is not to 'control' the tech sector, but to create the space and conditions for the tech-ecosystem as a whole to thrive.

In doing so, regulators – working with all stakeholders in the tech-ecosystem (government, industry, civil society, and consumers) – shape an environment from which the full potential of digital technologies can be harvested.[1]

****

Executive Summary

For many years the prevailing view – at least in western liberal democracies – was that governments could not, and should not, regulate digital technologies.

The origins of this philosophy lie in part in the ethos of the early internet, which was developed as a free and open global communication network. The fear was – and at an international level still is[2] – that the internet's potential would be limited if it was beholden to governance by any one country. This philosophy was widely endorsed by democratic governments, industry, and civil society alike.

However, as internet penetration grew exponentially, and business models and digital technologies evolved, tension emerged between the underlying philosophy of the early internet, a growing demand for governments and industry to do more to safeguard citizens and consumers from the harms of digital technologies, and a continuing near insatiable thirst for innovation.

Skim the news anywhere in the world today and you will find articles imploring governments to step in and regulate 'Big Tech'. Articles extolling the transformative virtues of digital technologies. And articles condemning the misuse of digital technologies by autocratic *and* democratic governments.

While these headlines may appear contradictory, each has merit and necessitates action. To be effective, tech regulation must embrace and operate within this complexity.

An important first step is acknowledging that the tech sector is much broader than 'Big Tech' (generally synonymous with global social media and online search platforms).

For the purposes of this report, the tech sector includes companies and individuals whose core business is to develop digital technologies, including infrastructure, hardware, software, products, platforms, and services (or, as is increasingly the case, a combination of some or all these elements).

The tech-ecosystem is defined more broadly; it includes the tech sector, its employees, and its financiers. But it also includes manufacturers, retailers, installers, repairers, and end users of digital technologies, as well as entities (other than those for whom it is a core business) that develop digital technologies, study the impact of digital technologies, support the tech sector's talent pipeline, or that design and implement tech regulation.

Given this breadth, calls for tech regulation are more usefully characterised as calls to regulate the *use* of digital technologies, or *behaviour* within the tech-ecosystem, rather than calls to regulate specific technologies or actors. This report focuses on regulation by government, future work will expand this scope.

Looking beyond news headlines, the necessity of tech regulation is now acknowledged by politicians, policymakers, regulators, civil society and by many – but not all – in the tech industry. That said, views continue to differ significantly on the nature and urgency of regulation.

Echoing the philosophy of the early internet, for some the tech-ecosystem remains a valued natural habitat that needs to be protected from (at best) misinformed or (at worst) malign intervention by government. At the other end of the spectrum, the tech-ecosystem is perceived as an uncontrolled jungle, which requires heavy earth-moving machinery to impose order. And then there are those who see it is a garden that has grown organically and is now in need of pruning.

This research has two foundational propositions:

- tech regulation is needed, but
- this imperative does not justify bad regulatory design.

It is possible to reward innovation, drive economic growth, strengthen democracy, enhance national security, *and* shape an environment (online and offline) in which individuals and communities can thrive. These objectives are not mutually exclusive – but to achieve each concurrently requires nuanced regulatory responses, which are currently rarely evident.

Nuanced and effective regulatory interventions are carefully calibrated to alleviate the harms associated with the use of digital technologies, without unnecessarily limiting (present and future) opportunities, while also considering the impact of the interventions on the entirety of the tech-ecosystem.

Despite the polarised nature of recent debates, the incentives for government and industry can be aligned. Well-designed and effectively implemented tech regulation reflects positively on politicians, policymakers and regulators (fulfilling their social contract with citizens) *and* delivers certainty for industry (generating investment and growth).

The maturity of the entire tech-ecosystem needs to be uplifted (this includes politicians, policymakers, regulators, industry, civil society, and consumers). This research focuses on the role of regulators, but its recommendations span all actors in the tech-ecosystem.

Just as tech policy is fast becoming "everything policy"[3], *tech regulation* can increasingly be equated with *everything regulation*; one need not strain their imagination to consider *tech regulators* becoming *everything regulators*.

The question of who the regulator(s) of the tech-ecosystem should be warrants closer attention.

Is a new stand-alone super tech regulator required? Should existing regulators be upskilled? Or a hybrid of both? Is there a new model that has not yet been considered? And what are the attributes (skills, knowledge, and expertise) of an effective tech regulator?

In Phase One of this project the Tech Policy Design Centre (TPDC) put these questions to 32 heads and senior representatives of Australian regulators, the Australian Government, industry, and civil society.

While it is a current subject of discussion[4], and may still evolve over time, of note, no interviewee argued for a new centralised super tech regulator. All advocated for upskilling and improving coordination among existing regulators. Many underscored the need for better coordination among and between regulators and policymakers. The knowledge asymmetry between industry and regulators was also a common theme.

As a point of comparison, the TPDC also commissioned overviews of tech regulators in 14 jurisdictions globally. No jurisdiction has established a centralised super tech regulator; universally, current practice is to upskill existing regulators. With the notable exception of China, formal coordination mechanisms among tech regulators and policymakers are in their infancy across all jurisdictions.

Informed by the expert interviews and current global practice, the TPDC developed a proposed Tech Policy and Regulation Coordination (TPRC) Model. Phase Two of this project tests the proposed TPRC Model with broad groups of stakeholders in Australia and abroad.

Institutional structures and bureaucratic processes are often dismissed as boring details. But these processes and structures provide the foundation for our societies and economies to function.[5]

The pervasiveness of digital technologies, combined with nascent tech policy and regulatory mechanisms, are producing lacklustre regulatory outcomes to the detriment of Australia and Australians. We are not getting the most out of digital technologies, and the use of some digital technologies are causing harm. It is a pattern that is repeated globally.

The good news is that many actors in the tech-ecosystem have an appetite to do better, and the imperative to do so becomes clearer every day. The proposed TPRC Model aims to funnel that appetite towards coordinated and effective regulatory outcomes.

It is in the interests of government, industry, civil society, and citizens to get this right. Good tech regulation will help shape digital technologies for the long-term benefit of humanity.

1. For an exploration of similar metaphors in a different context, see: Roberts, A and St John, T 2021, 'Complex Designers and Emergent Design: Reforming the Investment Treaty System', *American Journal of International Law*, 116(1):96-149, https://doi.org/10.1017/ajil.2021.57.
2. The White House 2022, *Fact Sheet: United States and 60 Global Partners Launch Declaration for the Future of the Internet*, statement, accessed 29 April 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/.
3. Davis, N 2021, 'Face-off: The Worldwide Battle with Big', in P Lewis & J Guiao (eds), *The Public Square Project: Reimagining Our Digital Future*, Carlton, Melbourne University Press, 68–81.
4. Smith, B 2022, *International Association of Privacy Professionals (IAPP) Summit 2022: Closing Session with Brad Smith, Neil Richards, Julia Angwin and Cecilia Kang*, online video, 13 April, viewed 21 April 2022, https://www.youtube.com/watch?v=QMho_jCYpYo.
5. Freiberg, A 2017, *Regulation in Australia*, The Federation Press, 42.

Key findings

The Key Findings in this report are drawn from 32 interviews (summarised in Sections One and Two of this Report) and a review of overviews of tech regulators in 14 jurisdictions globally (detailed in Section Three). The interviews and reviews were representative, but not exhaustive. Phase Two of the Project tests these findings with broad groups of stakeholders in Australia and abroad.

What are the attributes (skills, knowledge, and expertise) of an effective tech regulator?

1.1 All interviewees concurred that effective tech regulators required deep knowledge of the business models and incentives that drive the technology companies; there was strong support for the establishment of non-adversarial fora to facilitate ongoing, non-transactional exchanges to build and mature knowledge sharing among government and industry.

1.2 There were differing views as to the level of *in-house* technology-specific expertise tech regulators needed, but *access* to independent technical expertise was considered a minimum requirement by all (to enable meaningful engagement by regulators and secure effective regulatory outcomes).

1.3 The need for tech regulators to cultivate a diversity of multidisciplinary skills was unanimously endorsed, acknowledging that the skills, knowledge, and expertise required will differ depending on the specific regulatory context.

1.4 An outcomes-focused regulatory toolkit received strong support; no interviewee spoke in favour of prescriptive regulation. Many spoke about the tension between identifying when an outcome set by government was not technically feasible, as distinct from when it was something industry didn't want to do; cultivating independent expertise and repairing trust between government and industry were commonly proffered antidotes.

1.5 Interviewees were all bound by a strong sense of purpose, which many observed could be better harnessed to drive more effective regulatory outcomes. Many interviewees also expressed frustration and/or disappointment at the current adversarial state of relationships between industry and government and the underrepresented voice of civil society.

Is a new centralised super tech regulator required? Or should existing regulators be upskilled? Or a hybrid of both? Is there a new model that has not yet been considered?

2.1 No interviewee (regulator, public servant, industry executive, or civil society representative) supported the establishment of a single, centralised 'super tech regulator'.

2.2 Upskilling existing regulators was the preferred base model, supported by increased funding and enhanced transparency and accountability.

2.3 All interviewees conceded that emerging and maturing technologies may give rise to the need for new regulatory powers. However, they were divided as to if those new powers required new domain specific tech regulators or should be subsumed into existing regulators.

2.4 Calls for consistent political leadership and improved coordination between and among regulators and policy agencies, and with industry and civil society were common themes.

2.5 All agreed that an effective regulator needs access to information and independent expertise; various suggestions were made to facilitate this, some of which are reflected in the proposed Tech Policy and Regulation Coordination (TPRC) Model (Figure 1).

How are other jurisdictions organising themselves?

3.1 No jurisdiction has established a single, centralised 'super tech regulator.'

3.2 Australia[6], China[7], Estonia[8], Fiji[9], India[10], Republic of Korea[11], and Singapore[12] have established domain specific tech regulators with responsibility for at least one element of tech regulation.

3.3 All jurisdictions are expanding the mandates of existing regulators to encompass enforcement of tech regulation, with varying degrees of internal coordination and coherence; competition regulators across jurisdictions are particularly active.

3.4 Australia[13], China[14], Japan[15], and the United Kingdom[16] are the only jurisdictions with formal coordination mechanisms among some tech regulators; China[17], Japan[18], and Republic of Korea[19] are the only jurisdictions with a formal mechanism for coordination among tech regulators *and* tech policy departments and agencies. The relative maturity of these coordination mechanisms is assessed in Table 5.

3.5 Despite the increasing prominence of cyber security, only half of the jurisdictions surveyed have a cyber security regulatory body with enforcement powers (as distinct from policy or operational responsibilities): Australia[20], China[21], Estonia[22], Germany[23], India[24], Republic of Korea[25], and Singapore.[26]

6. Office of the eSafety Commissioner and Office of the National Data Commissioner.
7. Cyberspace Administration of China.
8. Estonian Information System Authority.
9. Fijian Online Safety Commission.
10. Indian Ministry of Electronics and Information Technology.
11. Korean Game Rating and Administration Committee and Korea Internet and Security Agency.
12. Cyber Security Agency of Singapore and Singaporean Protection from Online Falsehoods and Manipulation Act Office.
13. Australian Digital Platforms Regulators Forum.
14. Central Commission for Cybersecurity and Informatization and Cyberspace Administration of China.
15. Japanese Headquarters for Digital Market Competition.
16. United Kingdom Digital Regulation Cooperation Forum.
17. Cyberspace Administration of China.
18. Japanese Headquarters for Digital Market Competition.
19. Korean Presidential Committee on the Fourth Industrial Revolution.
20. Australian Department of Home Affairs, Cyber and Infrastructure Security Centre.
21. Cyberspace Administration of China.
22. Estonian Information System Authority.
23. German Federal Office for Information Security.
24. Indian National Critical Information Infrastructure Protection Centre.
25. Korea Internet and Security Agency.
26. Cyber Security Agency of Singapore.

Proposed Tech Policy and Regulation Coordination (TPRC) Model

> There is a key role for something – let's call it a government technology authority – that undertakes especially the stewardship function...Any new model must confront the reality of entrenched bureaucratic politics, a limited talent pool, a misaligned funding system, an extractive consulting sector, and impatient ministers...It would need independence, its own legislative or Cabinet remit, adequate funding guarantees, clarity of strategic purpose, and bi-partisan support.
>
> **– Professor Lesley Seebeck[27]**

> While there is now a plethora of internal government policy coordination committees...and a series of ad hoc, bilateral engagement forums between regulators, it is clear that these processes are not preventing the emergence of duplicative and inconsistent policy development...Labor Members recommend that the Government consider the establishment of a Council of Technology Regulators, modelled on the Council of Financial Regulators, to coordinate and align technology policy-making.
>
> **– House of Representatives Select Committee on Social Media and Online Safety[28]**

> The most important question for us to think about is this, what would a Digital Regulatory Commission look like? What would its scope be? How would it work? Would we be better served to place in the hands of people, pursuant to the rule of law, the ability to learn and master the facts for an industry and craft carefully, very thoughtful rules? Is that a better future than asking your congress or a legislature or a parliament to go on a piecemeal basis and change each and every law, separately, and with less coordination?
>
> **– Brad Smith[29]**

Informed by the Key Findings of this Report, the TPDC developed the following proposed Tech Policy and Regulation Coordination (TPRC) Model (Figure 1).

Phase Two of this project tests the proposed TPRC Model with a broad group of stakeholders in Australia and abroad. Report Two provides final recommendations.

While the TPRC Model is tailored to the specific conventions of the Australian Government, the principles and overall structure of the Model is transferable to other jurisdictions.

The TPRC Model takes an ecosystem wide approach. It builds on several sound proposals already in the public domain, as well as the suggestions of interviewees and current global practice.

It responds to calls for political leadership, strengthened coordination, increased transparency, access to independent technical expertise, and regularised, meaningful input by industry and civil society.

Most significantly, the proposed TPRC Model does not alter the independent mandates of existing policy owners or regulators. Except for the *Tech Policy and Regulation Coordination Cabinet Committee*[30], each TPRC body has an advisory and coordination role.

The distinct roles of politicians, policymakers and regulators (in the design and implementation of regulation) provides an important check and balance on power. This is particularly so for regulators, whose independence from the government of the day is generally enshrined in statute. The TPRC Model enhances coordination, improves transparency and democratic oversight of all actors in the tech-ecosystem, while respecting and preserving the independence of regulators.

Responsibilities and regulatory actions continue to be undertaken by individual departments, agencies and regulators in accordance with their existing legislated powers and obligations. However, the judgements formed by constituent members of the TPRC Model are informed by their participation in TPRC processes, improving the overall effectiveness of regulation of the tech-ecosystem.

The TPRC Model does not assume a clean slate. It adopts a pragmatic approach.

The TPRC Model is designed for immediate implementation and iterative revision. If enhanced coordination does not produce improved regulatory outcomes, it leaves open the possibility for the TPRC Model to evolve from one of 'regulatory coordination' to 'regulatory consolidation' over time.

Figure 1: Proposed Tech Policy and Regulation Coordination (TPRC) Model

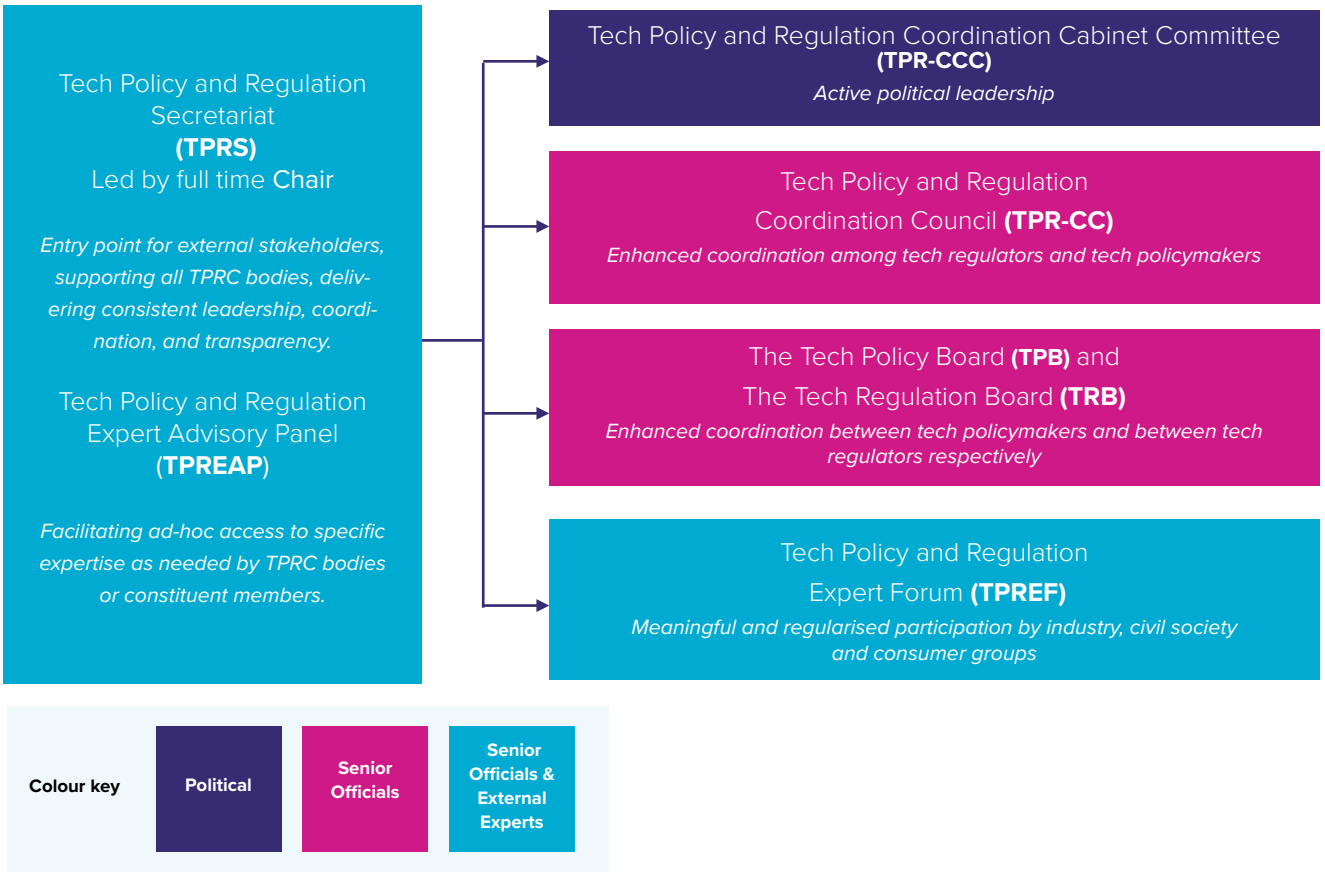


Table 1: Proposed Tech Policy and Regulation Coordination Model

Objective	Body	Meetings
1. Active political leadership, to: set tech policy priorities; coordinate and action new tech regulation proposals; and receive tech regulation enforcement updates (as appropriate, noting regulator independence).	***Tech Policy and Regulation Coordination Cabinet Committee (TPR-CCC)***, led by the Prime Minister, informed by the *Tech Policy and Regulation Coordination Council*, supported by the *Tech Policy and Regulation Secretariat*.	Quarterly meetings[31] of all relevant Ministers, including the Prime Minister, Attorney-General, Treasurer and the Ministers for Communications, Cyber Security, Defence, Digital (super or otherwise)[32], Education, Foreign Affairs, Home Affairs, Industry, Trade and others active in tech policy and regulation.
2. Enhanced coordination among tech regulators and tech policymakers, to: facilitate collaboration to advance a coherent and coordinated approach to the design and implementation of tech policy and regulation (respectful of independent mandates); exchange information and views; and assist with coordination where members' responsibilities overlap.	***Tech Policy and Regulation Coordination Council (TPR-CC)***, led by full-time independent Chair (or 'Chief Technologist')[33], informed by the *Tech Policy Board* and the *Tech Regulation Board*, supported by the *Tech Policy and Regulation Secretariat*.	Quarterly meetings at the Secretary/Agency/Regulator Head level. This Council is analogous to the Australian Council of Financial Regulators (CFR).[34] However, its mandate is broader, with membership by policy owners *and* regulators as well as a full-time Chair[35] and Secretariat[36] mandated to coordinate and support each element of the TPRC Model. A snapshot comparison of TPR-CC and CFR is at Table 2.
3. Enhanced coordination between tech regulators, and enhanced coordination between policymakers, to strengthen coordination, capacity, and stewardship among tech policy owners, and separately among tech regulators (preserving their distinct roles and independence).	***The Tech Policy Board (TPB)*** *and* ***the Tech Regulation Board (TRB)***, led by Chair of the Council, informed by respective independent mandates of constituent members and the *Tech Policy and Regulation Expert Forum,* supported by the *Tech Policy and Regulation Secretariat*.	Monthly Meetings, at the Deputy Secretary/Agency/Regulator Head level. The *Tech Policy Board* could amalgamate, or supplement, existing Secretaries' Boards, and the *Tech Regulation Board* could expand membership of the Digital Platforms Regulators Forum (DP-Reg), established in March 2022. Unlike the Council, regulators and policy owners meet separately (preserving the independent functions, while also enhancing coordination).
4. Meaningful participation by industry, civil society, and consumers, to ensure diverse perspectives inform the deliberations of the Boards, Council and Committee.	***Tech Policy and Regulation Expert Forum (TPREF)***, led by Chair of the Council, comprising 25 core industry, civil society and consumer representatives appointed for 2-year terms, supported by the *Tech Policy and Regulation Secretariat.*[37] To inform deliberation on specific issues, the core members could be supplemented on an ad-hoc basis with agreement of the Chair and all members.	Monthly meeting (two weeks before/after Board meetings). Members are experts (not exclusively CEO/C-Suite) and receive prioritised Australian Government Security Clearances. Appointment is via an open call for nominations, assessed by a selection panel (comprising the Council Chair and an industry and a civil society representative, both appointed by the Chair).
5. Informed by expert advice, to address the information asymmetry between government and industry.	*Standing* ***Tech Policy and Regulation Expert Advisory Panel (TPREAP)***, a database of Australian and international experts, maintained by the *Tech Policy and Regulation Secretariat.*	Experts would be called upon to provide advice to the Committee, Council, Boards, or individual regulators and policy owners on a case by case/as needed basis. Experts could be drawn from industry, academia, or civil society, but would serve in an independent personal capacity, in accordance with standard terms.
6. Cognisant of international developments, to ensure interoperability and harness economic opportunities.	Tech regulators and policy owners establish ***bilateral relationships with respective counterparts*** in key jurisdictions.	'Significant International Developments' is a standing agenda item on Forum, Board, Council, and Committee meetings. All participants are encouraged to raise new and emerging best practice.
7. Consistently coordinated.	***Tech Policy and Regulation Secretariat (TPRS),*** led by full-time permanent Chair of the Council[38], supported by small staff of directly engaged Australian Public Service (APS) Officers and supplemented by long-term APS secondments from constituent members of the Council. Secondments from industry, academia and civil society could also be considered, with appropriate confidentiality protections.	In addition to supporting and attending the Committee, Council, Boards, Forum and Panel, the Secretariat would: be the main contact/entry point to government for industry, maintain a public register of proposed and adopted Australian tech policy and regulation[39], conduct horizon scanning[40], and, could be tasked on an ad-hoc basis (with supplementary funding) by the Committee, Council or Boards to produce reports on specific issues[41], drawing as appropriate on each of the bodies above.

27. Seebeck, L 2022, 'Government tech is hard. If not the DTA, then what?', *InnovationAus.com*, 11 April, accessed 21 April 2022, https://www.innovationaus.com/govt-tech-is-hard-if-not-the-dta-then-what/. Note: in this article Seebeck was specifically commenting that digital transformation of government requires more than creation of a "single, under-resourced and under-powered agency". The authors of this report suggest that Seebeck's observations are equally transferable to regulation of the tech-ecosystem.
28. House of Representatives Select Committee on Social Media and Online Safety 2022, *Social Media and Online Safety*, The Parliament of the Commonwealth of Australia, accessed 14 April 2022, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024877/toc_pdf/SocialMediaandOnlineSafety.pdf;fileType=application%2Fpdf. See: Section Three for a full overview of Australian Regulators.
29. Smith, B 2022, International Association of Privacy Professionals (IAPP) Summit 2022: Closing Session with *Brad Smith, Neil Richards, Julia Angwin and Cecilia Kang*, online video, 13 April, viewed 21 April 2022, https://www.youtube.com/watch?v=QMho_jCYpYo.
30. *Tech Policy and Regulation Coordination Cabinet Committee* will have decision making authority, in line with Cabinet Committee Conventions.
31. Additional ad-hoc meetings of each body could be called on an as needed priority basis, however, ad hoc meetings should be kept to a minimum to regularise the development of tech policy and regulation; which, in and of itself, would represent maturity in the tech eco-system.
32. The Australian Information Industry Association advocates for establishment of a "Digital Super Minister"; Riley, J 2022, 'AIIA calls for Cabinet-level digital super-Minister', *InnovationAus.com*, accessed 12 April 2022, www.innovationaus.com/aiia-calls-for-cabinet-level-digital-super-minister/#:~:text=The%20Australian%20Information%20Industry%20Association,%2C%20Cabinet%2Dlevel%20ministerial%20position. While not directly analogous, no experts interviewed for this research supported creation of a 'super tech regulator'; given the breadth of tech regulation, the universal preference was to upskill existing regulators. In a similar vein, the "Digital Super Minister" as envisaged by AIIA would encompass only some elements of Tech Policy and Regulation (as broadly defined in this report). Therefore, if a Digital Super Minister portfolio were established that Minister would be an important constituent member of, but not replace, the proposed *Tech Policy and Regulation Coordination Cabinet Committee*.
33. The full-time independent Chair (or Chief Technologist) borrows and builds on a proposal by *Committee for Economic Development of Australia (CEDA): Committee for Economic Development of Australia* (CEDA) 2021, *Technology and trust: Priorities for a reimagined economy led by technology*, accessed 12 April 2022, https://cedakenticomedia.blob.core.windows.net/cedamediacontainer/kentico/media/general/publication/pdfs/technology-and-trust-may2021.pdf.
34. The concept of a body analogous to *Council of Financial Regulators* has been proposed in several fora, including: Watts, T & Claydon, S 2022, *Labor members' additional comments, Inquiry into Social Media and Online Safety,* The Parliament of the Commonwealth of Australia, accessed 12 April 2022, www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Media_and_Online_Safety/SocialMediaandSafety/Report/section?id=committees%2Freportrep%2F024877%2F79437.; Smith, P 2022, 'Directors and industry at risk from 'knee-jerk' tech policies', *Financial Review*, 14 March, accessed 12 April 2022, www.afr.com/technology/directors-and-industry-at-risk-from-knee-jerk-tech-policies-20220306-p5a27i.
35. See: Note 4, above.
36. See: Item 6, below "Consistent and coordinated": *Tech Policy and Regulator Secretariat.*
37. While it would sitting within a different structure, this idea draws on the General Services Administration's (GSA) Federal Advisory Committee Act (FACA) Database n.d., *All Agency Accounts*, United States government, accessed 12 April 2022, www.facadatabase.gov/FACA/FACAPublicAgencyNavigation.
38. See: Note 4, above.
39. While the proposed model would be broader. See: IP Australia 2021, *Policy Register*, accessed 12 April 2022, www.ipaustralia.gov.au/policy-register.
40. See: *Regulatory Horizons Council* (RHC) n.d., *GOV.UK*, accessed 12 April 2022, www.gov.uk/government/groups/regulatory-horizons-council-rhc.
41. In this way the *Tech Policy and Regulator Secretariat* is more closely analogous to the Australia Law Commission than the Australian Council of Financial Regulators. This concept draws from and builds upon the concept of Law Reform and Tech Assessment as discussed in: Bennett Moses, L 2013, 'Bridging Distances in Approach: Sharing Ideas about Technology Regulation', in R Leenes & E Kosta (eds), *Bridging Distances in Technology and Regulation*, Wolf Legal, 37-51. See also: The Parliamentary Office of Science and Technology (POST) 2022, *Bridging research and policy*, UK Parliament, accessed 12 April 2022, https://post.parliament.uk/. Analogies have also been made to the Productivity Commission and the Australian National Audit Office: Seebeck, L 2022, 'Government tech is hard. If not the DTA, then what?', *InnovationAus.com*, 11 April, accessed 21 April 2022, https://www.innovationaus.com/govt-tech-is-hard-if-not-the-dta-then-what/.

Table 2: Snapshot Comparison of the Australian Digital Platforms Regulators Forum (DP-REG), the United Kingdom's Digital Regulation Cooperation Forum (DRCF), the Australian Council of Financial Regulators (CFR), and the proposed Tech Policy and Regulation Coordination Council (TPR-CC).

Name	The Australian Digital Platforms Regulators Forum	UK Digital Regulation Cooperation Forum	The Australian Council of Financial Regulators	Proposed Tech Policy and Regulation Coordination Council
Leadership	Rotating Chair and Secretariat (6-month rotations).	The first DRCF CEO took office in November 2021. The CEO leads a Secretariat formed by each DRCF member. DRCF's CEO works closely with the heads of each DRCF member.	Chair (Reserve Bank of Australia (RBA)) and part-time Secretariat (RBA).	Full-time independent Chair (or 'Chief Technologist')[42], supported by the Tech Policy and Regulation Secretariat.
Institutional form	The DP-REG is an advisory body and has no bearing on members' existing regulatory powers, legislative functions, or responsibilities.	The DRCF is a non-statutory voluntary network. It is an advisory body and does not provide formal advice or directions to members.	The CFR is an advisory body focused on coordination and cooperation. The CFR and its activities are not established by statute, and it has no formal regulatory or policy decision-making powers.	TPR-CC would be an advisory and coordination body. Policy responsibilities and regulatory actions would continue to be undertaken by members in accordance with their legislated powers and obligations. However, decision would be informed by their participation in TPR-CC.
Membership	Regulators only: • Australian Competition and Consumer Commission • Office of the Australian Information Commissioner • Australian Communications and Media Authority • Office of the eSafety Commissioner	Regulators only: • Competition and Markets Authority • Information Commissioner's Office • Office of Communications • Financial Conduct Authority {originally an observer member, full member as of April 2021}	Regulators only: • Australian Prudential Regulation Authority • Australian Securities and Investments Commission • Reserve Bank of Australia • Treasury	Regulators *and* Policymakers. Specific membership to be discussed.
Participation by non-members (government)	By agreement among all existing members, other relevant Australian *regulatory agencies* may be invited to join the DP-REG or attend meetings on an ad hoc basis.	The DRCF workplan recognises that there is a wide range of regulatory agencies with remits covering the tech sector/ emerging and maturing technologies, and it might be appropriate for the DRCF membership to expand further. The DRCF has stated publicly that it intends to work closely with the Advertising Standards Authority, Prudential Regulation Authority, Payment Systems Regulator, Intellectual Property Office, Gambling Commission, and other agencies as appropriate.	The CFR draws on the expertise of other non-member government and international agencies where appropriate for its agenda. It meets jointly with the following agencies at least annually to discuss broader financial sector policy: • Australian Competition and Consumer Commission • Australian Transaction Reports and Analysis Centre • Australian Taxation Office The CFR also has crisis resolution and planning arrangements in place with New Zealand through the Trans-Tasman Council on Banking Supervision.	TPR-CC would comprise a core membership of policy owners and regulators that deal with tech policy and regulation issues daily. Other government bodies could attend on an ad hoc basis, as and when tech policy and regulator issues become a priority within their respective portfolios.
Participation by industry/ civil society	No formal mechanism.	No formal mechanism.	No formal mechanism.	*Tech Policy and Regulation Expert Forum* and *Standing Tech Policy and Regulation Expert Advisory Panel*.[43]

Name	The Australian Digital Platforms Regulators Forum	UK Digital Regulation Cooperation Forum	The Australian Council of Financial Regulators	Proposed Tech Policy and Regulation Coordination Council
Mandate	The Digital Platform Regulators Forum (DP-REG) is an avenue for Australian regulators to share information about, and collaborate on, cross-cutting issues and activities relating to the regulation of *digital platforms*. For the purposes of DP-REG, a 'digital platform' includes, but is not limited to, search engines, digital content aggregators, social media services, private messaging services, media referral services, and electronic marketplaces. Issues relating to cyber security or cybercrime are outside of the DP-REG's remit. Collaboration between DP-REG members includes: • compiling and maintenance of a contact list • information and data sharing • enhancing regulatory capabilities • collaboration opportunities.	The DRCF supports cooperation and coordination among its members on *online regulatory matters*, and enables coherent, informed, and responsive regulation of the United Kingdom's digital economy. This digital economy serves citizens and consumers, and enhances the global impact and position of the United Kingdom. The DRCF was the first national regulatory network supporting cooperation across the breadth of its responsibilities for regulating *'digital services.'* Together these include promoting competition, regulating communication services and broadcasting, protecting people's data rights, regulating harmful online content, and the regulation of financial services. The DRCF has the following objectives: • collaborate to advance a coherent regulatory approach • inform regulatory policymaking • enhance regulatory capabilities • anticipate future developments (horizon scanning) • promote innovation • strengthen international engagement.	The CFR facilitates cooperation and collaboration between member agencies, with the ultimate objectives of *promoting stability of the Australian financial system* and supporting effective and efficient regulation by Australia's financial regulatory agencies. As per its Charter, the CFR provides a forum for: • identifying important issues and trends in the financial system • exchanging information and views and assisting with coordination where members' responsibilities overlap • harmonising regulatory and reporting requirements, paying close attention to regulatory costs • ensuring coordination among the agencies in planning for and responding to instances of financial instability • coordinating engagement with the work of international institutions, forums, and regulators. A MOU between all members sets out the CFR's role in coordinating responses to financial distress (including crisis coordination). In between quarterly meetings, the work of the CFR is facilitated through various working groups. These groups progress work on specific topics or policy reforms. They develop papers for discussion that may include working group-level advice on whether the CFR should support a particular position. The working groups are established either on an ongoing or temporary basis. CFR agencies conduct regular crisis exercises and simulations to ensure they are adequately prepared to resolve failures and near-failures in an orderly manner. Simulations are sometimes also carried out under the auspices of the Trans-Tasman Council on Banking Supervision.	TPR-CC would facilitate cooperation and collaboration among members to promote effective design and implementation of tech policy and regulation. Specific mandate could include: • collaboration to advance a coherent and coordinated approach to the design and implementation of tech policy and regulation (respectful of independent mandates) • exchanging information and views and assisting with coordination where members' responsibilities overlap • enhancing tech policy capabilities and strengthening stewardship among tech regulators • harmonising regulatory and reporting requirements, paying close attention to regulatory costs • identifying important issues and trends in tech policy and regulation • coordinating engagement with the work of international institutions, forums, and regulators. The TPR-CC Secretariat would support each body in the Tech Policy and Regulation Coordination Model, including: *Tech Policy and Regulation Coordination Cabinet Committee*, the *Tech Policy Board* and *Tech Regulation Board,* the *Tech Policy and Regulation Expert Forum*, and the *Standing Tech Policy and Regulation Expert Advisory Panel.*[44] The TPR-CC Secretariat would also: maintain a public register of proposed and adopted Australian tech policy and regulation[45], conduct horizon scanning[46], and be tasked on an ad-hoc basis (with supplementary funding) by the TPR-CCC or TPR-CC to produce reports on specific issues[47], drawing on the expertise of the constituent bodies in the TPRC Model as appropriate.

Name	The Australian Digital Platforms Regulators Forum	UK Digital Regulation Cooperation Forum	The Australian Council of Financial Regulators	Proposed Tech Policy and Regulation Coordination Council
Budget	Each member bears its own costs in relation to the DP-REG.	Chair: not publicly disclosed. Secretariat: composed of staff from constituent members.	The RBA bears all costs related to the Chair and Secretariat. Each member bears its own costs of participation.	Central funding for full-time permanent Chair. Secretariat would comprise a small number of centrally funded core staff (Australian Public Service (APS) Officers) and supplemented by long-term APS secondments from constituent members. Secondments from industry, academia, and civil society could also be considered, with appropriate confidentiality protections.
Meetings	Every two months, at deputy head level. Ad hoc meetings can be convened by the Chair as necessary.	Not publicly disclosed.	Meeting quarterly at a minimum with two representatives – the agency head and another senior representative – from each of the four member agencies. Additional meetings as needed.	TPR-CC would meet quarterly at the Secretary/Agency/Regulator Head level. TPR-CC Chair would attend, and the Secretariat would support, all meetings of the other consistent bodies in the proposed TPRC Model.[48]
Key documents	DP-REG Terms of Reference (2022).[49] Bilateral MOUs between members.	DRCF: Plan of work for 2021 to 2022.[50] Letter from Secretary DCMS to DRCF (2022).[51] DRCF: Establishing Document (2022).[52]	The CFR Charter (updated in 2019).[53] Memorandum of Understanding on Financial Distress Management with CFR Members (2008).[54] Terms of reference for the Trans-Tasman Council on Banking Supervision.[55] Bilateral MOUs between members.[56]	Not applicable.

42. The full-time independent Chair (or Chief Technologist) borrows and builds on a proposal by *Committee for Economic Development of Australia* (CEDA): Committee for Economic Development of Australia (CEDA) 2021, *Technology and trust: Priorities for a reimagined economy led by technology*, accessed 12 April 2022, https://cedakenticomedia.blob.core.windows.net/cedamediacontainer/kentico/media/general/publication/pdfs/technology-and-trust-may2021.pdf.
43. For details of these bodies, see: Table 1: Proposed Tech Policy and Regulators Coordination Model.
44. For details of these bodies, see: Table 1: Proposed Tech Policy and Regulators Coordination Model.
45. While the proposed model would be broader. See. P Australia 2021, Policy Register, accerssed 12 April 2022. www.ipaustralia.gov.au/policy-register.
46. See: Regulatory Horizons Council (RHC) n.d., *GOV.UK*, accessed 12 April 2022, www.gov.uk/government/groups/regulatory-horizons-council-rhc.
47. In this way the *Tech Policy and Regulator Secretariat* is more closely analogous to the Australia Law Commission than the Australian Council of Financial regulators. This concept draws from and builds upon concept of Law Reform and Tech Assessment is discussed in: Bennett Moses, L 2013, 'Bridging Distances in Approach: Sharing Ideas about Technology Regulation', in R Leenes & E Kosta (eds), *Bridging Distances in Technology and Regulation*, Wolf Legal, 37-51.
48. See also: The Parliamentary Office of Science and Technology (POST) 2022, *Bridging research and policy*, UK Parliament, accessed 12 April 2022, https://post.parliament.uk/.
49. Australian Communications and Media Authority 2022, *Digital Platform Regulators Forum (DP-REG) Terms of Reference*, accessed 14 April 2022, www.acma.gov.au/sites/default/files/2022-03/DP-REG%20Terms%20of%20Reference%20.pdf.
50. Digital Regulation Cooperation Forum 2021, *Digital Regulation Cooperation Forum: Plan of Work for 2021 to 2022*, accessed 14 April 2022, www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022#annex-1-the-drcf-objectives-and-operation.
51. Dorries MP, Rt Hon Nadine 2022, *Letter from DCMS Secretary of State to the Digital Regulation Cooperation Forum,* Department for Digital, Culture, Media & Sport, accessed 14 April 2022, www.gov.uk/government/publications/letter-from-dcms-secretary-of-state-to-the-digital-regulation-cooperation-forum/letter-from-dcms-secretary-of-state-to-the-digital-regulation-cooperation-forum-html.
52. Competition and Markets Authority, Information Commissioner's Office, and Office of Communications n.d., *Digital Regulation Cooperation Forum*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896827/Digital_Regulation_Cooperation_Forum.pdf.
53. Council of Financial Regulators 2019, *Charter*, Reserve Bank of Australia, accessed 14 April 2022, www.cfr.gov.au/about/charter.html.
54. Council of Financial Regulators 2008, *Memorandum of Understanding (MOU) between the Members of the Council of Financial Regulators (Council),* Reserve Bank of Australia, accessed 14 April 2022, www.cfr.gov.au/financial-institutions/crisis-management-arrangements/pdf/mou-financial-distress-management.pdf.
55. Council of Financial Regulators 2017, *Terms of Reference for the Trans-Tasman Council on Banking Supervision*, Reserve Bank of Australia, accessed 14 April 2022, www.cfr.gov.au/about/trans-tasman-council-on-banking-supervision/terms-of-reference.html.
56. Council of Financial Regulators 2022, *Memoranda of Understanding*, accessed 14 April 2022, www.cfr.gov.au/about/memoranda-of-understanding.html.

Definitions

There are no universally accepted definitions for many of the foundational terms used in this report. The definitions adopted for the purposes of this report are set out below. Establishing a common lexicon is a first step to fostering a mature conversation.

> **Once when talking about tech, we all visualised people parked behind computer screens writing code, in languages mere mortals didn't understand. However, today I struggle to think of a single business or job in our vibrant and diverse economy that is not in some way touched by technology. Today's technologists might be found sitting on a tractor, mapping out new digital farming strategies, in a warehouse building an e-commerce solution or a high-school student designing new software for sharing education resources. We are now all technologists, and our businesses are all technology businesses.**
>
> **– Robyn Denholm[1]**

Table 3: Definition of terms

Regulation	"An intentional form of intervention…in the economic and social activities of a target population with the aim of achieving a public policy objective or set of objectives. The intervention can be direct and/or indirect, the activities can be economic and/or non-economic, and the regulatee may be a public or private-sector actor."[2]
Regulators	"Government officials, departmental units and independent statutory authorities that are empowered by legislation to administer and enforce regulation, or more specifically to: grant approvals (including registration and licensing); monitor compliance; and enforce laws."[3]
Tech Sector	includes: • companies and individuals whose core business is to develop digital technologies, including infrastructure, hardware, software, products, platforms, and services (or a combination of some or all of those elements); and • companies and individuals whose core business is to develop digital technologies to deliver previously analogue products and services (for example: FinTech, MiningTech, and AgriTech companies).
Tech-Ecosystem	is broadly defined to include: • the tech sector, its employees, and financiers • manufacturers, retailers, installers, and repairers of digital technologies • end users of digital technologies (government, enterprises, or individuals) • entities (other than companies and individuals for whom it is a core business) that develop digital technologies, study the impact of digital technologies, or support the tech sector's talent pipeline • entities (public or private) that design and implement tech regulation, and • tech regulators.
Tech Regulation	An intentional form of intervention in the tech-ecosystem with the aim of achieving a public policy objective or set of objectives. The intervention can be direct and/or indirect, the activities can be economic and/or non-economic, and the regulatee may be a public or private-sector actor.
Tech Regulators	Government officials, departmental units and independent statutory authorities that are empowered to administer and enforce tech regulation, or more specifically to: grant approvals (including registration and licensing); monitor compliance; and enforce the regulations.

1. Denholm, R 2022, 'Australia's Next Five Unicorns Will Come from Five Areas', *Australian Financial Review*, 11 March, accessed 14 April 2022, www.afr.com/business-summit/australia-s-next-unicorns-will-come-from-five-areas-20220311-p5a3t1#:~:text=The%20research%20identifies%20five%20tech,distributed%20ledger%20and%20diversified%20fintech.
2. Freiberg, A 2017, *Regulation in Australia*, The Federation Press, xxxviii.
3. Productivity Commission 2013, *Regulator Engagement with Small Business*, p. 34, accessed 14 April 2022, www.pc.gov.au/inquiries/completed/small-business/report/small-business.pdf.

Abbreviations and Acronyms

AI	Artificial Intelligence
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ADHA	Australian Digital Health Agency
AGD	Attorney-General's Department
AHRC	Australian Human Rights Commission
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investment Commission
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CFR	Council of Financial Regulators
CIGI	Centre for International Governance Innovation
CMA	Competition and Markets Authority (UK)
CISC	Cyber and Infrastructure Security Centre
DPRF	Digital Platforms Regulators Forum
DRCF	Digital Regulation Cooperation Forum (UK)
eSafety	Office of the eSafety Commissioner
EU	European Union
FCA	Financial Conduct Authority (UK)
FIRB	Foreign Investment Review Board
GDPR	General Data Protection Regulation (European Union)
GFC	Global Financial Crisis
DHA	Department of Home Affairs
ICO	Information Commissioner’s Office (UK)
IPO	Intellectual Property Office (UK)
MOU	Memorandum of Understanding
Ofcom	Office of Communications
OAIC	Office of the Australian Information Commissioner
ONDC	Office of the National Data Commissioner
PMC	Department of Prime Minister and Cabinet
PRA	Prudential Regulation Authority (UK)
PSR	Payment Systems Regulator
RBA	Reserve Bank of Australia
UK	United Kingdom
US	United States

Interview Methodology

In March 2022, the Tech Policy Design Centre (TPDC) interviewed 32 heads and senior representatives of Australian regulators, the Australian Government, industry, and civil society.

Sections One and Two of this Report summarise the responses received using thematic analysis. **Text Box 1** and **2** provide a key to the quantitative and qualitative terms used in the summaries respectively.

All interviews were conducted on a non-attribution basis to encourage frank responses. Interviews lasted for about an hour and were conducted in person or online.

A list of the organisations represented by the interviewees and the set of questions posed during the interviews are provided for in Annex A and B respectively.

The interviews and reviews were representative, but not exhaustive. Phase Two of the Project tests the Key Findings from the interviews with broader groups of stakeholders in Australia and abroad.

This research was conducted in accordance with the National Statement on Ethical Conduct in Human Research[1], and was approved by the Australian National University's Research Human Ethics Committee (Human Ethics Protocol 2022/105).

Text Box 1: Key to quantitative terms used in interview summaries

All – everyone interviewed expressed this sentiment

Most – all bar one or two outliers expressed this sentiment

A majority – more than 70% expressed this sentiment

Many – between 30-70% expressed this sentiment

A minority – less than 30% expressed this sentiment

Several – three to six interviewees expressed this sentiment

Few – two or less interviewees expressed this sentiment

Text Box 2: Key to qualitative terms used in interview summaries

Industry Executive – Senior Executive from Industry

Leading Regulator – Head of an Australian Regulatory Body

Senior Regulator – Senior Executive from an Australian Regulatory Body

Senior Public Servant – Senior Executive from the Australian Public Service

Thought Leader – Senior Leader from Civil Society, Think Tanks, or Academia

If the category of interviewee (leading regulator, industry executive, senior public servant, thought leader, etc.) is not specified, it was sentiment expressed equally across the spectrum of interviewees.

1 Section One: Skills, Knowledge, and Expertise

This Section offers insights into the attributes (skills, knowledge, and expertise) of an effective tech regulator, as articulated by the participants of the regulator research interviews. These ideas and suggestions, along with those in Sections Two and Three of this report, informed the development of the proposed Tech Policy and Regulation Coordination (TPRC) Model.

The specific question put to the interviewees is shown below in **Text Box 3**. A key to the qualitative and quantitative terms used in the following summaries is above at **Text Box 1** and **2**.

When asked to provide examples of an effective regulator in action, several interviewees cited the Australia Security and Investment Commission (ASIC) during the Global Financial Crisis (GFC). **Case Study A** demonstrates how ASIC's skills, knowledge, and expertise and a principles-based approach helped Australian corporations get through the GFC.

Text Box 3: Interview Question

What skills, expertise, and tools would tech regulator(s) need to be effective?

Summary of Key Findings

1.1 All interviewees concurred that effective tech regulators required deep knowledge of the business models and incentives that drive the technology companies; there was strong support for the establishment of non-adversarial fora to facilitate ongoing, non-transactional exchanges to build and mature knowledge sharing among government and industry.

1.2 There were differing views as to the level of in-house technology-specific expertise that tech regulators needed, but access to independent technical expertise was considered a minimum requirement by all (to enable meaningful engagement by regulators and secure effective regulatory outcomes).

1.3 The need for tech regulators to cultivate a diversity of multidisciplinary skills was unanimously endorsed, acknowledging that the skills, knowledge, and expertise required will differ depending on the context.

1.4 An outcomes-focused regulatory toolkit received strong support; no interviewee spoke in favour of prescriptive regulation. Many from regulators and industry spoke about the tension between identifying when an outcome set by government was not technically feasible, as distinct from when it was something industry didn't want to do; cultivating independent expertise and repairing trust between government and industry were commonly proffered antidotes.

1.5 Interviewees were all bound by a strong sense of purpose, many observed that it could be better harnessed to drive more effective regulatory outcomes. Many interviewees also expressed frustration and/or disappointment at the current adversarial state of relationships between industry and government and the underrepresented voice of civil society.

1.1 Deep knowledge of the business models and incentives that drive the tech sector was considered a core requirement by all

> Regulators need to have deep knowledge of how the tech sector operates. This has many different dimensions; how we build the technology, not just in the technical sense, but also having an awareness of business models and how this drives the choices that tech companies make. You must really understand all those dimensions to have a good understanding of where the levers might be – to try and change behaviours.
> **– Industry Executive**

> It is not so much, do you have to have direct experience working in a specific tech company, it's more how much proximity do you have to the tech sector. Proximity to the industry is key, provided you are not captured by it.
> **– Thought Leader**

> If you do not have deep domain expertise, there is no way to understand how the tech industry thinks, what their true limitations are, or how they could do it/ things differently.
> **– Leading Regulator**

> Regulators need to know the incentives in the system. Is our problem the technology? Or is it the use of the technology, which is influenced by the business model and the incentives that drive the business?
> **– Thought Leader**

> We benefit from having people who know the industry. We'll hire them if we can, otherwise, we will go and talk to a lot of people. You can go along way taking staff who are fascinated by the topic and can feed their curiosity and ask others for help.
> **– Leading Regulator**

- Several Industry Leaders underscored the plurality of business models; suggesting that a nuanced appreciation of the diversity would foster more effective regulatory interventions.
- Obtaining, and then maintaining, the currency of knowledge about business models and incentives was highlighted by most interviewees as a significant hurdle; many industry representatives also underscored that, even if you could incentivise it, taking people from industry and putting them in-regulator would have limited utility given the pace of innovation.
- A minority of interviewees (predominately, but not exclusively from industry) were of the view that regulators needed prior hands-on experience in the tech sector, but most interviewees did not consider it a prerequisite, and several across the spectrum of interviewees outright dismissed it: *"That is just nonsense. That is rot"* said one Leading Regulator.
- There was strong support for the establishment of non-adversarial fora to facilitate ongoing, non-transactional exchanges to build and share knowledge among regulators and industry.

1.2 There were differing views as to the level of in-house technology-specific expertise tech regulators needed, but access to independent technical expertise was considered a minimum requirement by all (to enable meaningful engagement by regulators and secure effective regulatory outcomes)

> The notion of the need for the regulator to have deep technological expertise in a particular technology area is often impractical (for example due to technology salaries) and can serve as a distraction. The regulator needs to have an understanding of the benefits and risks associated with the technology and how characteristics of the technology and its use influence those, and the focus should be on how the technology is operated and the effects that its use has.
>
> **– Thought Leader, with deep technical experience**

> You need diverse expertise. It is important to agree on what experts need to be at the table. 75% of people in government come from the humanities. They tend to unconsciously champion the disciplines they know.
>
> **– Senior Industry Leader**

> For a starting point, there is no such thing as a tech business model, and it changes and adapts so quickly. There is a lack of understanding and technical expertise, but that goes both ways as sometimes the expertise is held up as a way of keeping people out.
>
> **– Leading Regulator**

- Understanding the limits of what the technology can and cannot do was highlighted by many in industry as a deficiency in regulators (as well as in politicians and policymakers).
- A minority of interviewees felt that deep in-house technology-specific expertise was needed. Several others acknowledged it would be desirable, particularly during confidential investigations, but difficult to secure given these skills were in-demand globally.
- Many from industry also underscored that technology-specific expertise quickly becomes dated when people leave the private sector.
- Many interviewees suggested that recruiting *some* staff with Science, Technology, Engineering and Mathematics (STEM) backgrounds provided sufficient technical foundations for regulators to frame questions to extract the right information from the regulated population; one Senior Regulator described this as "*knowing enough to ask the right questions, and to identify when an answer hides an important truth*".
- There was strong support for cultivating a base level of digital literacy among all staff, in addition to, and as distinct from, nurturing deep technical and/or STEM expertise.
- There was unanimous recognition that tech regulators would require access to deep technical expertise from time to time; the challenge of sourcing that independent expertise was likewise universally acknowledged.

1.3 The need for regulators to cultivate a diversity of multidisciplinary skills was unanimously endorsed

> No one particular discipline has all the answers.
> **– Thought Leader**

> You need as many people trained in the humanities as you do with deep technical chops to be able to properly regulate a system. You need a multidisciplinary set of skills to accurately assess potential harms to society and do something about them. You need deep knowledge of the technology and how the choices and business models impact tech companies' behaviour. This in turn is overlaid with the technology that is quickly and constantly developing and changing.
> **– Industry Executive**

> Regulators need knowledge of regulatory policy, knowledge of enforcement mechanisms, and knowledge of the sector. It helps to know when you are speaking different languages; it is about the diversity of the people, you need all of the skillsets and experience.
> **– Senior Public Servant**

> The notion that we need to push students into STEM for them to be useful is false. They need critical thinking. How to attract staff to a tech regulator? Don't over-emphasis the hard skills. People can learn on-the-job the technical skills and knowledge they need.
> **– Thought Leader**

> Best practice regulators in all areas actively build staff capability. They ensure staff have relevant knowledge of regulatory craft and the industry they regulate. They also have the capacity and are empowered to identify and implement improved practices. The specific skills, expertise, and tools required by a technology regulator will depend on the subject matter of the regulations to be administered.
> **– Leading Regulator**

- Most interviewees emphasised that the skills, knowledge, and expertise required differed depending on the domain (compare, for example: FinTech, dual-use export controls, and competition).
- In a notable departure from standard public service strictures, many regulators expressed an openness to on-the-job training; a comment echoed by several from industry.
- Technologists were important – but investigators, economists, public policy specialists, business analysists, and those with "regulatory oversight experience" were equally sought-after.
- Analytical thinking, pragmatism, constant curiosity, and a willingness to challenge assumptions were particularly valued traits; although, as one Leading Regulator acknowledged, this sometimes represented a "*challenge of cultural fit*" within the public service.
- In a similar vein, many prioritised research skills, with one Industry Leader acknowledging that "*tech will raise problems that people haven't seen before; we need to understand the problems.*"
- Legal skills and the capacity to take enforcement action was identified by several interviewees as key characteristic of an 'effective regulator.'
- Many regulators and several from industry also underscored the importance of staff with experience operating across jurisdictions, and the need for international dialogue and engagement; industry, in particular, underscored a desire for regulatory harmonisation.
- Several interviewees observed that staff with excellent stakeholder and communication skills were invaluable to facilitate translation between the disciplines (internally and externally).

1.4 A regulatory toolkit that was outcomes-focused received strong support

> Regulators in this space should regulate by the outcomes that they do or don't want, rather than the details of how you get there. This will require less technical expertise, as they just need to focus on a defining outcome. But even in an outcome focused regime, you still need people who understand technology and what is technically feasible.
> **– Industry Executive**

> The target of regulation can...shift rapidly, requiring continuous regulator improvement, awareness of technological changes, and development of technology-neutral approaches focused on the harm to be addressed where possible.
> **– Leading Regulator**

> Regulators should not be too quick to be negative. Many new technologies are disrupting – often biggest disruptions are where there is consumer need. We need to consider if it is a need that should be met or not. And then consider the regulatory implications.
> **– Senior Public Servant**

> Tech is unique because of the pace at which it moves. It requires looking further ahead at the breadth of possibilities and what you are prepared to accept in terms of risk. Based on what could happen rather than what is happening. There is often a disconnect between perceived risk and genuine risk.
> **– Thought Leader**

> The challenge is defining the problem. What is the end goal? Sometimes the goalposts get shifted and that creates frustration. There are quite a few areas (i.e., artificial intelligence, online safety, competition) we have not reached the point where we are communicating the same harms and concerns.
> **– Industry Executive**

- A majority of interviewees raised the need to prioritise outcomes-based regulation, rather than prescriptive black letter law (the remainder did not speak against the concept, it was rather just not something they raised).
- In a similar vein, many spoke of the dangers of regulators getting 'bogged down' at the technical level, suggesting regulators should focus on the outputs of technology (the novel harms and risks, the unintended and unforeseen consequences) and on creating a 'bounding box' for behaviour; if regulators defined the box, regulatees could then innovate within the bounds of that box.
- Plainly defining the purpose of the regulatory intervention and clearly articulating the end goal (or the bounds of the box) was identified by many as an area requiring urgent improvement.
- One Senior Regulator noted that an outcomes-based approach was preferable because of the level of maturity of regulation; as regulators build expertise, it may become more feasible to take a more prescriptive approach.
- Many industry representatives and regulators spoke of the tension between identifying when an outcome set by government was technically not feasible, as distinct from when it was just something industry didn't want to do; cultivating independent expertise and repairing trust between government and industry were commonly proffered antidotes.

1.5 Interviewees were bound by a strong sense of purpose – many were of the view that this could be better harnessed to drive more effective regulatory outcomes

> We need to move beyond the binary view that tech companies are bad, and government is good, and government must teach industry a lesson. Our objective is not to make democratic tech toothless – it should be collaboration to make tech work for our society and for democratic business interests.
> **– Thought Leader**

> There is a complexity. Walking into these discussions you feel you are behind the eight ball. But it goes both ways, and those from the tech industry don't understand the complexity of the legal and regulatory system. We need a practical meeting of minds.
> **– Leading Regulator**

> Most people that work in these industries are committed to the purpose of their work. We should play to that. The most important cost of Cambridge Analytica to Facebook was that recruitment from top tier schools dropped by 30-50 per cent that year.
> **– Industry Executive**

> The regulator's conundrum: sharing knowledge and expertise of the industry, but also maintaining separation between the gamekeeper and the poacher.
> **– Senior Public Servant**

> A lot of people go into technology to change the world, salaries aren't the only factor. My experience, particularly from living in Silicon Valley, is that people are drawn to technology careers to solve problems through technology.
> **– Industry Executive**

- All interviewees expressed a strong sense of purpose in their own roles and recognised this to varying degrees in others.
- Several spoke persuasively of the benefits that would flow if a tech regulator nurtured a purpose driven culture in terms of recruitment and retention, but also regulatory outcomes.
- Many underscored the need to repair and rebuild relationships, citing trust and accountability as an essential foundation on which to build an effective regulator.
- There was forthright acknowledgement by most interviewees that every dimension of the tech regulation ecosystem lacked maturity; at least behind closed doors, each of the interviewees refreshingly accepted this as truth for their own domain, as much as for others.
- Most spoke of a willingness for more collaboration and consultation.
- Many interviewees were frustrated and disappointed at the current adversarial state of relationships between industry and government and the underrepresented voice of civil society.

Case Study A: ASIC during the Global Financial Crisis

AMIT SINGH, ACCENTURE

This case study demonstrates how an empowered corporate regulator (ASIC) and a principles-based approach helped Australian corporations get through the GFC. Lessons may be drawn from this case study when considering what skills, knowledge, and tools an effective tech regulator would need, and what institutional structures would best support this.

During the GFC, financial markets regulators across the globe grappled with how to balance consumer protection with a return to growth. Australia's financial markets supervisory architecture, underpinned by principles-based regulation and empowered and responsive regulators, helped to create an authorising environment that supported investment and financial innovation, enabled recapitalisations, and lessened the long-term impact of the crisis within Australia.

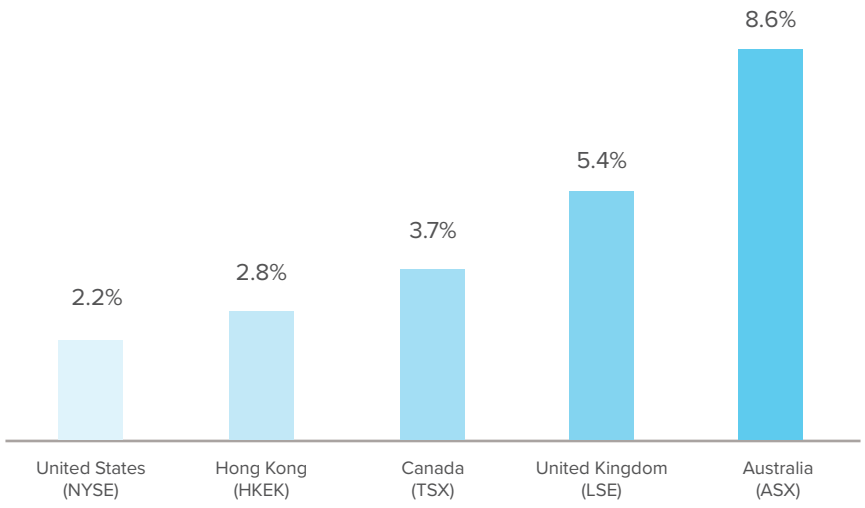
At a critical time for corporations and the economy, regulators need to make timely and considered judgements that achieve the right balance between maintaining confidence within markets and responding to potential or immediate issues. An example of ASIC's good judgement at that time related to capital raising.

As the crisis unfolded, Australian companies were severely impacted. After peaking in November 2007, the All-Ordinaries Index fell by 55 per cent to a low in March 2009.[1] Major corporate collapses, or near collapses (e.g., ABC Learning, Allco Finance, and Babcock and Brown), totalled around A$66 billion during that period, representing a slightly greater proportion of Australian GDP than the A$20 billion lost during the turmoil of the late 1980s.[2]

Australian companies aimed to raise capital to strengthen their balance sheets both quickly and at low cost. Over the 2008–2009 financial year, Australian listed companies' secondary raisings totalled A$88 billion - among the highest rates in the world.

Secondary capital raisings as a proportion of average monthly total market capitalisation in 2009

(Source: ASX, World Federation of Exchanges, exchange websites, Accenture analysis)



This record equity capital raising allowed companies to repay debt and undoubtedly helped to forestall foreclosures and promote credit growth through the Australian banking sector. These capital raisings were enabled by Australia's financial markets supervisory architecture, where ASIC operates within the context of an articulated set of principles (Eggleston principles)*, with the regulator empowered to approve (quickly and with discretion) innovative deal structures. This includes circumstances that are outside the scope of what was initially articulated within the *Corporations Act*.[3] Applying these principles generally, ASIC encouraged corporate decision-makers to determine how best to pursue these principles — enabling innovation — while putting up and enforcing guardrails to ensure equal opportunity for shareholders.†

Innovative capital raising structures

During the GFC, this regulatory environment enabled Australian companies to adopt non-traditional rights issues that facilitated a better balance between efficiency and equal opportunity. Companies were able to quickly access capital from institutional investors (who are expected to have the expertise and resources to decide with short notice) and provide retail investors with the opportunity to evaluate their participation (and avoid share dilution) in a matter of weeks. To improve fairness, ASIC also intervened, adapting the law to reduce the administrative costs to companies of including retail investors in raises. This was alongside pursuing over 323 investigations of wrongdoing in the aftermath of the GFC.[4]

As the Chair of ASIC at the time, Tony DeAloisio, summarised in a speech following the GFC: "[W]e monitored retail investor impact but, on balance, felt that it was acceptable, and the impact did not outweigh the benefits of these raisings."[5] ASIC played an important role in both recovery and prevention.

Compared to the United States and the United Kingdom, Australia's rules for secondary raises emphasised principles and allowed more flexibility, increasing the amount of capital raising in circumstances where it was urgently needed. A similar principles-based, flexible approach could likewise be well-suited to regulation of the dynamic tech sector and fast evolving digital technologies.

* The Eggleston principles are a set of principles created by the Company Law Advisory Committee in 1969. For more information, see: The Treasury of the Commonwealth of Australia 2019, *Takeovers Issues – Treasury Scoping Paper,* accessed 14 April 2022, https://treasury.gov.au/sites/default/files/2019-03/Taskeovers-issues-TSY-scoping-paper.pdf.

† Reform context: Australian financial regulators had been empowered almost a decade prior to the GFC in the aftermath of the 1997 Wallis Inquiry.

1. Christie, J 2021, 'Stock Market Crashes in Australia: A Brief Technical Note,' *Australasian Accounting, Business and Finance Journal*, vol. 15, no. 4, pp. 175–78. https://doi.org/10.14453/aabfj.v15i4.10.
2. D'Aloisio, T 2010, 'Responding to the Global Financial Crisis: The ASIC Story', transcript, *Australian Securities & Investments Commission*, 30 November 2010, https://download.asic.gov.au/media/1347350/speech-responding-global-crisis-nov-2011.pdf
3. *Corporations Act 2001*
4. D'Aloisio, T 2010, 'Responding to the Global Financial Crisis: The ASIC Story', transcript, *Australian Securities & Investments Commission*, 30 November 2010, https://download.asic.gov.au/media/1347350/speech-responding-global-crisis-nov-2011.pdf.
5. D'Aloisio, T 2010, 'Responding to the Global Financial Crisis: The ASIC Story', transcript, *Australian Securities & Investments Commission*, 30 November 2010, https://download.asic.gov.au/media/1347350/speech-responding-global-crisis-nov-2011.pdf.

2 Section Two: Institutional Models

This Section offers insights into institutional models to best support an effective tech regulator, as articulated by the participants of the regulator research interviews. These ideas and suggestions, along with those in Sections One and Three of this Report, informed the development of the proposed Tech Policy and Regulation Coordination (TPRC) Model.

The specific question put to the interviewees is shown below in **Text Box 4**. A key to the qualitative and quantitative terms used in the following summaries is above at **Text Box 1** and **2.**

While it is not always possible to draw direct comparisons, several experts suggested that the evolution of biotechnology regulatory models could inform current tech regulation debates. **Case Study B** provides an overview of the key structural developments around biotechnology regulation in the United States and their eventual global repercussions.

Text Box 4: Interview Question 5

Three tech regulator models are popularly posited:

1. establishment of a standalone tech regulator
2. assimilation of tech-specific responsibilities into the mandates of existing regulators, or
3. a hybrid of one and two.

What are the merits and pitfalls of each, and is there an alternative model that should be considered?

Summary of Key Findings

2.1 No interviewee (regulator, public servant, industry representative or civil society representative) supported the establishment of a single, centralised 'super tech regulator.'

2.2 Upskilling existing regulators was the preferred base model, supported by increased funding, and enhanced transparency and accountability.

2.3 All interviewees conceded that emerging and maturing technologies may give rise to the need for new regulatory powers but were divided as to if those new powers required new domain specific regulatory institutions or should be subsumed into existing institutions.

2.4 Calls for consistent political leadership and improved coordination between and among regulators and policy agencies, and with industry and civil society were common themes.

2.5 All agreed that an effective regulator needs access to information and independent expertise; various suggestions were made to facilitate this, many of which are reflected in the proposed Tech Policy and Regulation Coordination (TPRC) Model.

2.1 No interviewee (regulator, public servant, industry or civil society representative) supported the establishment of a single, centralised 'super tech regulator'

> I object to the concept of a 'tech regulator', as opposed to 'regulators who regulate tech.' What is the problem we are trying to solve? Tech is not often the problem. Although the solutions can look different online and offline.
>
> **– Thought Leader**

> The ACCC reached the view that it was not appropriate to recommend the establishment of a new regulator or agency. A new regulator or agency would take considerable time to build the skills already possessed by existing regulators and, being so targeted, would run a clear risk of regulatory capture. Rather, more effective and targeted oversight would be provided by supplementing the functions of existing enforcement and regulatory agencies including the ACCC, the ACMA and the OAIC, which are already working very well together.
>
> **– ACCC Digital Platforms Final Report[1]**

> Regulators need to be well versed in tech but also recognise how behaviours manifesting on digital platforms reflect broader social issues, which highlights a risk with regulators that solely have an online remit. This has been one of the concerns from day one of the eSafety Commissioner. We know that upwards of 95% of bullying online is an extension of bullying taking place in the physical world. You need to consider the broader context. We can't solve for bullying at a societal level by just regulating the digital manifestations.
>
> **– Industry Executive**

- Interviewees were unanimous in expressing concern that the establishment of a single, centralised 'super tech regulator' risked creating an unwieldly 'everything regulator.'
- While, in theory, such a 'super tech regulator' would centralise tech expertise, there was considerable trepidation that it would do so at the detriment of other specialist expertise needed by a regulator (competition lawyers, privacy specialists etc.).
- Likewise, while a 'super tech regulator' might reduce silos across tech-specific regulation, most interviewees suggested it would likely increase silos between tech-regulation and existing domain regulation. In effect it would be transferring the coordination burden from:
  - enforcement of diverged tech regulation by and in coordination with concurrent regulators with specific domains (including tech), to
  - enforcement of converged tech regulation by a single tech regulator in coordination with existing concurrent regulators (excluding tech).
- At a practical level, most interviewees questioned how the scope of a 'super tech regulator' would be determined, what would remain in the mandates of existing regulators, and how such a 'super tech regulator' would prioritise actions.

2.2 Upskilling existing regulators was the preferred base model, supported by increased funding, and enhanced transparency and accountability

> My overarching view is we don't need a new or hybrid tech regulator. We just need the existing regulators to do their jobs effectively.
> **– Thought Leader**

> Ministers have a high bar for establishing new regulators. We already have a lot of regulatory overlap. They would need to be convinced why the businesses should be treated differently. You often hear that tech is different or special but, when you break it down, they have similar functions and regulatory challenges to many other industries. I would need to be convinced that digital is different; it's not as different as it might seem on the surface.
> **– Senior Public Servant**

> Build on what you are. Don't have a group off to the side that can't communicate to the rest of the organisation.
> **– Leading Regulator**

> Add the expertise into existing regulators. Upskill the existing regulators. A siloed approach would make everything fall over. Having regulators is one thing, but robust oversight of government activities is another. Significant regulatory powers have been given to ministers and regulators and there needs to be clearer oversight of that and transparency around those powers and the impact.
> **– Industry Executive**

- While supported by all, the challenge of upskilling existing regulators was equally recognised by all interviewees (see point 2.4 on coordination and 2.5 on independent expertise).
- The need to mainstream regulatory capacity across the existing regulators, rather than creating specialist tech regulation divisions in existing regulators, was emphasised by many.
- Most underscored the need for a clear demarcation of the new domains of tech regulatory responsibility, and the importance of protecting against mission creep; from regulators and public servants this comment was often accompanied by a wry reference to turf wars.
- While supportive of existing regulators taking on new responsibilities, a few within industry were wary of directly transposing all existing regulatory powers, proposing a considered process to look at the limits of existing authorities and whether that current authority usefully translates into new tech domains.
- Several highlighted the need for existing regulators to be funded adequately and appropriately resourced to take on these new regulatory responsibilities.
- One Industry Executive highlighted the need for regulators to be proportionately resourced; citing as an example the 'uniquely Australian' funding disparity between OAIC and the comparatively well-funded eSafety.
- Surprisingly, the need for good governance was only mentioned by one regulator. However, many across the spectrum of interviewees emphasised the need for regulators to develop a culture of regulatory stewardship; in this regard industry tended to prioritise trust and mutual respect, whereas regulators emphasised the need for impartiality and independence.

2.3 All interviewees conceded that emerging and maturing technologies may give rise to the need for new regulatory powers, but were divided as to if those new powers required new domain specific regulatory institutions, or should be subsumed into existing institutions

> Upskill existing regulators, whose core role will continue, to take on related tech oversight roles that they must embrace. If it is a natural fit to combine some of this in existing regulators, we should. But there will also be new roles that aren't a natural fit (i.e., digital identity). We need to think carefully about the new roles and where to put them.
>
> **– Leading Regulator**

> There are a lot of areas of tech policy that will always reside in other departments. National security policy will always be done by Defence and Home Affairs, and financial policy will be done by the ATO and Treasury. It is not practical to aspire to house everything in one regulator. However, there are areas that have never had a natural home (i.e., data policy) and for these issues there is value in creating a single [specific] regulator.
>
> **– Industry Executive**

> In some circumstances, introducing cross-sector regulation will need to be accompanied by a regulator with a specific remit. This is seen in Australia's *Online Safety Act 2021 (Cth)*, administered by the eSafety Commissioner, which is dedicated to the broader theme of keeping people safe online. When attached to a technology-neutral cross-sector regulatory remit, staff with technical expertise and resources, and support from across the system of government, this can be a highly effective model for addressing specific risks flowing from the technology sector.
>
> **– Leading Regulator**

- Several interviewees argued that specific technologies warranted new regulatory powers; particular uses of artificial intelligence or autonomous vehicles were given as examples.
- Several felt that regulating the 'impact' of technologies was better suited to existing regulators, while regulating the 'design' of technologies may warrant new specialist tech regulators. Most, however, rejected this distinction.
- Most interviewees argued that any new regulatory powers should be focused on the new or novel types of outcomes created by the technologies rather than on the specific technologies themselves. One Industry Executive suggested that 'sensitive use' or 'consequential outcomes' would be a more useful criterion; arguing that just because something is new or novel doesn't mean it needs regulation.
- Data Governance, eSafety or Digital Safety, and Cyber Security were the three domains most cited as requiring powers beyond those traditionally held by existing regulators.[2]
- Interviewees were divided on whether new regulatory powers required new regulatory bodies or could be subsumed into existing bodies with a commensurate increase in resources; most felt it would depend on the subject of the new powers and if they had a 'natural fit' within existing regulators.
- Several emphasised that, if new domain specific regulators are established, structures need to be in place to facilitate cooperation with existing regulators (on issues like privacy, cyber security, human rights, for example).
- The importance of culture and leadership was underscored by many.

2.4 Calls for political leadership and improved coordination among regulators, between regulators and policy agencies, and with industry and civil society were common themes

> There can be a problem [with regulators] saying they are independent and how that's interpreted – yes, you're independent but that doesn't mean you operate independent of government expectation. Being independent doesn't mean you can't talk to the regulated community. This view enforces the fortress mentality. Regulators should have empathy for the regulated population. They should know the impacts of what they've done and why they're doing it.
>
> **– Senior Public Servant**

> I often get frustrated spending a lot of time building relationships and developing a knowledge base with individuals in particular [government] departments to then have them leave. There needs to be a more sustainable way for industry to help policymakers and regulators develop the experience...furthermore regulators appear ashamed to admit that they work closely with industry. There is a perception that being close to industry is a bad thing. This is indicative of a lack of maturity in the relationship between regulators and tech companies and the public conversation about this relationship.
>
> **– Industry Executive**

> Regulators shouldn't be making policy outside of democratic processes. It is important for them to understand "what is policy." Regulators may have useful insight to share with politicians and policy-makers. And regulators need flexibility to respond to crises. But if regulators are creating policy, it will inevitably veer of track from society's expectation and fracture important governance processes. Society's trust in regulators is very vital.
>
> **– Senior Public Servant**

> We need to coordinate and deconflict. It's the mission creep that is the most problematic. If we had clear lines of delineation, especially with the policy departments that design much of the regulation that we enforce, it would help to prevent bad design from the outset and avoid regulators having to retrofit solutions.
>
> **– Leading Regulator**

- Confusion, conflation and duplication, contrasted with gaps, were examples given by many interviewees to highlight the need for better coordination among regulators and, just as importantly, between regulators and policy agencies (who develop much of the regulation).[3]
- Several interviewees also underscored the importance of citizens knowing that help was available to address specific harms and where to go to get that help.
- Many (particularly, but not exclusively, from industry) expressed exasperation at the politicisation of tech policy issues eroding good regulatory design.
- The DP-REG[4] was welcomed, but most saw it as a first step in a larger process given the narrow scope, small membership, and absence of policy agencies, budget and standing secretariat. The DRCF and CFR were two models that many suggested could be usefully built upon. See **Table 2** for a comparison of these two bodies.

2.5 An effective regulator needs access to information and independent expertise; various suggestions were made to facilitate this, many of which are reflected in the proposed Tech Policy and Regulation Coordination (TPRC) Model

> **What's needed is an independent conduit. A professional that says no matter what this is, we can deal with it. Whatever institutional form this takes it needs to have a high-level of visibility, be independent, and provide objective advice. It should be the consistent entry or a door into the conversation, that can then go off in different directions.**
>
> **– Thought Leader**

> **The concept of an independent expert advising government has value and merit, but the execution to date has not been ideal. We've seen examples of this – but the concept falls down in two areas: (1) the people appointed to these bodies are appointed for optical reasons rather than actually bringing value and expertise to the table (e.g., CEOs are appointed because that looks like the government is engaging with senior people); and (2) these groups produce recommendations or reports and the government doesn't do anything with the outputs, it doesn't inform their thinking or policy-making.**
>
> **– Industry Executive**

> **A lot of this work is human-centred design. Perhaps what government needs is almost like a policy sandbox (to test their ideas), rather than an advisory committee which often seems transactional.**
>
> **– Thought Leader**

- All interviewees agreed that regulators will need access to independent expertise, both technical and with respect to the different business models within the tech sector.
- Many interviewees also suggested that regulators needed better access to information, or the ability to use more readily their information compulsion powers.
- Separate to the question of new regulatory institutions, many interviewees endorsed the establishment of expert bodies to inform the work of regulators, policymakers, and legislators. A number of specific suggestions were proposed and are listed in no particular order:
  - Establish a Tech Policy and Regulation Clearing House or sandbox.
  - Appoint an Australian Chief Technology Officer (and supporting office).[5]
  - Combine Law Reform and Technology Assessment traditions to establish specific project-based teams of experts, with a standing secretariat to coordinate.[6]
  - Establish a Standing Expert Panel, with experts (from Australia and overseas) appointed in their personal capacity, with agreed renumeration structure (emphasizing 'service to the public'), to be accessed on an as needed basis.
  - Establish advisory committees; the *United States Federal Advisory Committee Act (FACA)* model could be instructive.[7]
  - Create consultative committees that meet on a regular non-transactional basis (particularly useful to build understanding of business models and incentives).

- Develop tailored training (formal and informal, tertiary, and executive education).
- Encourage secondments, and greater mobility between industry and government and between policy agencies and regulators (with appropriate confidentiality and capture safeguards).
- Increase funding for foundational research (to incentivise and build independent expertise in academia that could be drawn upon as needed by government).
- Consider a model like the United States National Institute of Standards and Technology (NIST).[8]
- Establish a Parliament Office for Digital Technology (modelled in part on United Kingdom's Parliamentary Office for Science and Technology[9], and in part on the Australian Parliamentary Budget Office).[10]
- Create a Civil Society Advisory Board and a Youth Representative Forum.
- IP Australia's Policy Register was put forward as a potential model that could be replicated and evolved to foster improved communication and collaboration between regulators, policymakers, industry, and civil society.[11]

• Sustainability, recruitment, and retention of the required expertise, and avoiding capture, were consistently acknowledged as challenges to most of the above models.

1. Australian Competition and Consumer Commission 2019, *Digital platforms inquiry,* p. 33, accessed 30 March 2022, www.accc.gov.au/publications/digital-platforms-inquiry-final-report.
2. Note: In Australia, the Office of the National Data Commissioner (ONDC) has been incorporated into Department of Prime Minister and Cabinet (PMC), cyber security regulatory powers into the Department of Home Affairs (Home Affairs), and the Office of the eSafety Commissioner (eSafety) has been established as an independent statutory office holder, supported by the Australian Communications and Media Authority (ACMA).
3. For example: *Australia's eSafety Act (2021)* (overseen by the eSafety Commissioner); *Social Media (Anti-Trolling) Bill (2021)* and defamation reform (to be overseen by Attorney General's Department) and proposed increased powers to counter misinformation and disinformation (to be overseen by Australian Communications Media Authority) were regularly cited as case in point.
4. The Digital Platforms Regulators Forum was foreshadowed in several interviews with regulators and announced on 11 March 2022 when approximately two thirds of the Phase One interviews were complete.
5. See also: Committee for Economic Development of Australia 2021, *Technology and trust: Priorities for a reimagined economy led by technology*, accessed 12 April 2022, https://cedakenticomedia.blob.core.windows.net/cedamediacontainer/kentico/media/general/publication/pdfs/technology-and-trust-may2021.pdf.
6. Bennett Moses, L 2013, 'Bridging Distances in Approach: Sharing Ideas about Technology Regulation', in R Leenes & E Kosta (eds), *Bridging Distances in Technology and Regulation*, Wolf Legal, Oisterwijk, pp. 37–51.
7. General Services Administration's Federal Advisory Committee Act Database n.d., *All Agency Accounts*, United States government, accessed 12 April 2022, www.facadatabase.gov/FACA/FACAPublicAgencyNavigation.
8. The National Institute of Standards and Technology (NIST) 2022, *About NIST*, accessed 14 April 2022, www.nist.gov/about-nist.
9. The Parliamentary Office of Science and Technology (POST) 2022, *Bridging research and policy*, UK Parliament, accessed 12 April 2022, https://post.parliament.uk/.
10. The Parliament of the Commonwealth of Australia n.d., *Parliamentary Budget Office*, accessed 14 April 2022, www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Budget_Office. See also: Senate Standing Committees on Legal and Constitutional Affairs 2020, *List of Recommendations: Recommendation 14*, The Parliament of the Commonwealth of Australia, accessed 14 April 2022, www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Nationhood/Report/section?id=committees%2freportsen%2f024372%2f76059.
11. IP Australia 2021, *Policy Register*, accessed 14 April 2022, www.ipaustralia.gov.au/policy-register.

Case Study B: The Regulation of Biotechnology

DR JENSEN SASS, AUSTRALIAN NATIONAL UNIVERSITY

The emergence and evolution of regulation around modern biotechnology bears striking similarities and important differences with contemporary debates concerning the regulation of digital technologies. As modern biotechnology crossed the threshold from being a disparate set of laboratory practices to front-page news, its significance was interpreted in divergent ways. Modern biotechnology at once represented a national competitiveness imperative, a promise of rapid advances in medicine and agriculture, and a source of unprecedented human health, ecological and moral dangers.

As the transformative yet ambiguous character of biotechnology rose to attention in policy circles and public life in the mid-1970s, the imperative to regulate became clear. What follows is a highly condensed periodisation capturing key structural developments around biotechnology regulation in the United States and the eventual global repercussions.

Period 1

Modern biotechnology coincides with the development of recombinant DNA techniques. These techniques allowed the intermingling of organisms across species boundaries, something thought impossible. The scientific community saw immense potential for transgenesis to hasten scientific progress but also risk in its catastrophic misuse.

Remarkably, the first regulatory push on biotechnology emerged from the scientific community itself. Immediately following the first demonstration of recombinant DNA technology, leading scientists called for a moratorium on a subset of these techniques and requested that the United States National Institutes of Health (NIH) develop guidelines for its use. The NIH obliged and, in 1975, announced the establishment of biosafety committees that would monitor compliance across all institutions receiving NIH funding.

The proactive stance taken by the scientific community assuaged public concern around biotechnology, helping to ensure that regulations were not imposed reactively under politicised conditions. However, additional regulation was inevitable; the guidelines only concerned a limited set of scientific practices, only applied to institutions receiving NIH funding, and there existed no mechanism for their enforcement.

Period 2

By the late 1970s, discussions around biotechnology proliferated across United States federal agencies and industries using recombinant DNA techniques. In the first instance, government officials faced two overriding regulatory questions: whether regulatory authority should rest at the federal or state level, and whether regulation could be developed and enforced by existing agencies, or whether a new biotechnology 'super regulator' was necessary. Industry associations uniformly backed a federal product-based system such that the risks associated with biotechnology applications would be assessed by existing federal agencies in light of existing principles of risk and hazard management.

A draft of the Coordinated Framework for the Regulation of Biotechnology (Framework) was published in the Federal Register in December 1984. It positioned the Food and Drug Administration (FDA) as the lead regulatory agency for biotechnology and saw the creation of an overarching science advisory body (to guide regulatory rulemaking in a rapidly evolving scientific context). In addition, regulatory committees would be established within each of the five agencies involved in regulating biotechnology applications (FDA, Environmental Protection Agency, U. S. Department of Agriculture, NIH, and Occupational Safety and Health Administration). Overseeing these committees was a coordinating committee that would facilitate communication across the agencies and handle jurisdictional conflicts.

The draft Framework was intended to guide agency practice until it was revised and formally enacted. In the intervening period, however, regulatees found that agencies were applying its guidelines inconsistently and they discovered regulatory paths of least resistance. This led to conflict between the agencies and sparked public concern as applications proscribed by one agency were subsequently approved by another. The draft Framework was formally enacted in 1986, having been revised such that a lead agency would be nominated where a product spanned agency jurisdiction.

Period 3

In the following decade, perceived national competitiveness pressures saw medical biotechnology approvals expedited and the relaxation of regulatory oversight over food and agricultural applications. This deregulatory push was crucial to the United States biotechnology industry surging ahead of its competitors (principally Japan and the European Union).

Public concern grew around food and agricultural applications due to a perception that non-commercial and non-government scientists possessed limited capability to scrutinise the product-approval process. These concerns were exacerbated by the disbanding of the interagency scientific advisory board because of perceived conflicts of interest among its members.

Despite these concerns, the draft Framework enabled rapid growth in both medical and agricultural biotechnology products and allowed for the deft handling of difficult ethical challenges facing biotechnology-human cloning.

Period 4

In the mid-1990s, conflicting ideas around the regulation of food and agricultural biotechnology set off a protracted trade dispute between the United States and the European Union. This development was precipitated by United States corporations seeking expeditious market access for genetically modified crops.

In the lead up to this period, United States firms and governments had sought to shape regulatory institutions in Europe, believing their product-based regulatory principles would be adopted. But these principles attracted concerted resistance as consumers and activists espoused a process-based regulatory orientation (such that biotechnology applications would be subject to tailored forms of assessment). They demanded that all product evaluations be guided by the precautionary principle.

Further complicating relations, consumers and activists in Europe sought to incorporate social and ethical assessments into regulatory decision-making, challenging presumptions in the United States that biotechnology regulations should be strictly 'science based', that is, limited to the assessment of human, animal, and environmental harm. Public- and private-sector biotechnology advocates did not appreciate the depth of concern in Europe and, by continuing to promote their products, they triggered the formation of a pan-European consumer movement that secured a moratorium on the importation and use of agricultural biotechnology.

This course of events had enormous financial implications for biotechnology firms in Europe and the United States, a number of which were compelled to restructure. In response, sustained efforts were made by institutions to rebuild public trust in the science and regulation of biotechnology. This led to the establishment of the European Food Safety Authority, and biotechnology regulatory institutions in Europe converging with the Framework. Despite these efforts, the anti-biotechnology movement sustained pressure on national governments and continues to limit the use of agricultural biotechnology 25 years later.

The regulation of biotechnology holds salient lessons for other tech industries. First, scientific leadership, in particular open and wide-ranging exchanges concerning risk and purpose, can build public trust and goodwill in a sector and in the regulations that guide its development. Trust is extremely difficult to rebuild where it has been lost. Second, regulatory frameworks found effective in one context may not be readily transposable; firms accept considerable risk where their strategies presume convergence on a model found appropriate in one country or region.

3 Section Three: Tech Regulator Overviews

This section contains overviews of tech regulators in 14 jurisdictions:

- Australia
- China
- Estonia
- European Union
- Fiji
- Germany
- India
- Japan
- Republic of Ireland
- Republic of Korea
- Singapore
- United Kingdom
- United States (California)
- United States (Federal)

Each country organises itself differently, so it is not always possible to draw direct comparisons. However, these overviews will help deepen understandings of different approaches, highlighting where they converge and diverge as well as lessons and/or models that may be transferable to other jurisdictions.

Key Findings: How are jurisdictions organising themselves?

3.1 No jurisdiction has established a single, centralised tech regulator.

3.2 Australia[1], China[2], Estonia[3], Fiji[4], India[5], Republic of Korea[6], and Singapore[7] have established a domain specific regulator with responsibility for at least one element of tech regulation.

3.3 All jurisdictions are expanding the mandates of existing regulators, resulting in varying degrees of internal coordination and coherence. In most jurisdictions, the competition regulator has taken a lead role.

3.4 Australia[8], China[9], Japan[10], and the United Kingdom[11] are the only jurisdictions with formal coordination mechanisms among some tech regulators. China[12], Japan[13], and Republic of Korea[14] are the only jurisdictions with a formal mechanism for coordination among some tech regulators *and* tech-policy departments and agencies. The relative maturity of these coordination mechanisms is summarised in Table 5.

3.5 Despite the increasing prominence of cyber security, only half of these jurisdictions have a regulatory body responsible for cyber security with enforcement powers (as distinct from policy or operational responsibilities). These are Australia[15], China[16], Estonia[17], Germany[18], India[19], Republic of Korea[20], and Singapore.[21]

Section Three: Definitions and Scope

To define the boundaries of the jurisdiction overviews, this section applies a narrower definition of tech regulator than that listed in Table 3: Definition of terms.

For the purposes of the overviews, the term **'tech regulator'** includes:

- all regulators with digital technology-specific mandates (e.g., eSafety (Australia))
- all regulators with economy-wide mandates that encompass some oversight of digital technologies (e.g., competition and consumer protection, corporations, human rights, privacy, data protection, intellectual property, foreign investment, defence exports, national security, cyber security, and tax regulators)
- financial, telecommunications, media and broadcast regulators with industry-specific mandates that encompass some oversight of digital technologies
- coordinating bodies (e.g., DRCF (United Kingdom))

Government departments or agencies with purely tech-policy, operational, standard-setting, or law-enforcement responsibilities are beyond the scope of these overviews. Regulators with exclusive oversight of intelligence agencies are also excluded.

On a limited basis, entities that do not fall within the definition of a tech regulator, as listed above, have been included because of a novel approach that was judged by the contributing authors as worthy of highlighting. These entries are marked with an asterisk (*) and excluded from Table 4: Tech Regulator Overviews: Jurisdictions at a Glance.

Major Reports, Inquiries, and Related Initiatives conducted by each regulator between 2019 and 2022 are listed. Significant developments that pre-date this time period are included at the discretion of the contributing authors.

Significant developments that have not been captured by a specific entity are listed at the end of each overview.

Additions or comments on the overviews or the categorisation are welcomed. Please email: TechPolicyDesign@anu.edu.au

1. Australian eSafety Commissioner and Office of the National Data Commissioner.
2. Cyberspace Administration of China.
3. Estonian Information System Authority.
4. Fijian Online Safety Commission.
5. Indian Ministry of Electronics and Information Technology.
6. Korean Game Rating and Administration Committee and Korea Internet and Security Agency.
7. Cyber Security Agency of Singapore and Protection from Online Falsehoods and Manipulation Act Office.
8. Digital Platforms Regulators Forum.
9. Central Commission for Cybersecurity and Informatization and Cyberspace Administration of China.
10. Headquarters for Digital Market Competition.
11. Digital Regulation Cooperation Forum.
12. Cyberspace Administration of China.
13. Headquarters for Digital Market Competition.
14. Presidential Committee on the Fourth Industrial Revolution.
15. Department of Home Affairs, Cyber and Infrastructure Security Centre.
16. Cyberspace Administration of China.
17. Information System Authority.
18. Federal Office for Information Security.
19. National Critical Information Infrastructure Protection Centre.
20. Korea Internet and Security Agency.
21. Cyber Security Agency of Singapore.

Table 4: Tech Regulator Overviews: Jurisdictions at a Glance

	Australia	China	Estonia	European Union	Fiji	Germany	India	Japan	Republic of Ireland	Republic of Korea	Singapore	United Kingdom	United States (Federal)	United States (California)
Centralised, stand-alone, exclusively tech-focused regulator (multi-domain)	0	0	0	Not Directly Comparable	0	0	0	0	0	0	0	0	0	Not Directly Comparable
Centralised, stand-alone, exclusively tech-focused regulator (specific domain)[1]	2[2]	1[3]	1[4]		1[5]	0	1[6]	0	0	2[7]	2[8]	0	0	
Existing whole-of-economy regulators now with partial oversight of the tech-ecosystem[9]	10	7	8		4	8	9	6	9	10	6	9	10	
Existing financial, teleco, media and broadcast regulators now with partial oversight of the tech-ecosystem[10]	5	2	2		4	3	4	2	2	4	1	1	3	
Body with specific mandate to coordinate tech regulation across multiple regulators	1[11]	2[12]	0		0	0	0	1[13]	0	1[14]	0	1[15]	0	
Total tech regulator bodies	18	11[16]	11		9	11	14	9	11	17	8	11	13	

1. Note: new units or offices that have an exclusively tech-focused mandate, but which sit within ministries are not considered "standalone". Such entities are counted within the "Existing whole-of-economy regulators now with partial oversight the tech-ecosystem" category.
2. Australian eSafety Commissioner and Office of the National Data Commissioner.
3. Cyberspace Administration of China.
4. Estonian Information System Authority.
5. Fijian Online Safety Commission.
6. Indian Ministry of Electronics and Information Technology.
7. Korean Game Rating and Administration Committee and Korea Internet and Security Agency.
8. Cyber Security Agency of Singapore and Protection from Online Falsehoods and Manipulation Act Office.
9. See country overviews for details on bodies that fall within this category.
10. See country overviews for details on bodies that fall within this category.
11. *Australian Digital Platforms Regulators Forum*, established in 2022. See Australian Competition and Consumer Commission 2022, *Agencies form Digital Platforms Regulators Forum*, accessed 11 April 2022, www.accc.gov.au/media-release/agencies-form-digital-platform-regulators-forum.
12. Chinese Central Commission for Cybersecurity and Informatization, upgraded in 2018 (established in 2014 as the Central Leading Group for Cybersecurity and Informatization) and Cyberspace Administration of China, established in 2014. See Creemers, R, Triolo, P, Sacks, S, Lu, X, & Webster G 2018, *China's Cyberspace Authorities Set to Gain Clout in Reorganization*, New America, accessed 11 April 2022, www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/.
13. Japanese Headquarters for Digital Market Competition, established in 2019. See Prime Minister's Office of Japan 2019, *Establishment of Headquarters for Digital Market Competition*, Headquarters for Digital Market Competition, accessed 11 April 2022, www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_190927.pdf.
14. Korean Presidential Committee on the Fourth Industrial Revolution, established in 2017. See Presidential Committee on the 4th Industrial Revolution 2017, *About PCFIR*, accessed 11 April 2022, www.4th-ir.go.kr/en/overview.
15. The Digital Regulation Cooperation Forum, established in 2020. See Competition and Markets Authority, Information Commissioner's Office, Ofcom, and Financial Conduct Authority 2021, *The Digital Regulation Cooperation Forum*, accessed 11 April 2022, www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.
16. Note: The Cyberspace Administration of China has a dual listing: "Standalone exclusively tech focused regulator (specific domain)" and "Body with specific mandate to coordinate tech regulation across multiple regulators" (hence total equals 11, when quantity adds up to 12).

Table 5: Tech Regulator Overviews: Coordination Maturity Matrix

This index measures maturity in terms of longevity of coordination mechanisms.

Methodology

Coordination Maturity Score = (Maturity Weighting + 1 for every full year since establishment).
See end notes for country-specific calculations.

	Maturity Weighting	Australia	China	Estonia	European Union	Fiji	Germany	India	Japan	Republic of Ireland	Republic of Korea	Singapore	United Kingdom	United States (Federal)	United States (California)
		Coordination Maturity Score (per category)													
Coordination body for tech regulators (specific domain)	1	1[1]	0	0	Not Directly Comparable	0	0	0	0	0	0	0	3[2]	0	Not Directly Comparable
Coordination Body for Tech Regulators (multi domain)	2	0	0	0		0	0	0	0	0	0	0	0	0	
Coordination body for tech regulators and tech policy agencies (specific domain)	2	0	0	0		0	0	0	5[3]	0	5[4]	0	0	0	
Coordination body for tech regulators and tech policy agencies (multi domain)	3	0	20[5]	0		0	0	0	0	0	0	0	0	0	
Total coordination maturity score		1	20	0	N/A	0	0	0	5	0	5	0	3	0	N/A

1. Australian Digital Platforms Regulators Forum, established in 2022, coordinates "Digital Platform Regulators". **Coordination ranking 1 (1 (weighting)) + 0 (years).** See Australian Competition and Consumer Commission 2022, *Agencies form Digital Platforms Regulators Forum*, accessed 11 April 2022, www.accc.gov.au/media-release/agencies-form-digital-platform-regulators-forum.
2. The Digital Regulation Cooperation Forum, established in 2020, coordinates "online regulatory matters" with a focus on "digital service". **Coordination ranking 3 (1 (weighting)) + 2 (years)**. See Competition and Markets Authority, Information Commissioner's Office, Ofcom, and Financial Conduct Authority 2021, *The Digital Regulation Cooperation Forum*, accessed 11 April 2022, www.gov.uk/government/collections/the-digital-regulation-cooperation-forum.
3. Japanese Headquarters for Digital Market Competition, established in 2019, coordinates "digital markets and platforms". **Coordination ranking 5 (2 (weighting)) + 3 (years))**. See Prime Minister's Office of Japan 2019, *Establishment of Headquarters for Digital Market Competition*, Headquarters for Digital Market Competition, accessed 11 April 2022, www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_190927.pdf.
4. Korean Presidential Committee on the Fourth Industrial Revolution, established in 2017, coordinates "4th Industrial Revolution technologies". **Coordination ranking 5 (2 (weighting)) + 3 (years)**. See Presidential Committee on the Fourth Industrial Revolution 2017, *About PCFIR*, accessed 11 April 2022, www.4th-ir.go.kr/en/overview/.
5. Chinese Central Commission for Cybersecurity and Informatization, upgraded in 2018 (established in 2014 as the Central Leading Group for Cybersecurity and Informatization) and Cyberspace Administration of China, established in 2014, both coordination "multi domain". **Coordination ranking 20 (3 (weighting)) + 7 (years) x2 (bodies)**. See Creemers, R, Triolo, P, Sacks, S, Lu, X, & Webster G 2018, *China's Cyberspace Authorities Set to Gain Clout in Reorganization*, New America, accessed 11 April 2022, www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/.

Australia

Johanna Weaver and Sarah O'Connor, Australian National University

Australian Classification

Institutional Form: Independent statutory authority

Responsible Minister: The Minister for Communications, Urban Infrastructure, Cities and the Arts

Principal Instrument(s): *Guidelines for the Classification of Films (2012), Guidelines for the Classification of Computer Games (2012), National Classification Code (2005), Classification (Publications, Films and Computer Games) Act (1995)*

Mandate: Australian Classification is divided into the Australian Classification Board (ACB) and the Classification Review Board (CRB). The ACB is responsible for the classification of films, computer games, and publications intended for sale, advertisement, or exhibition in Australia in accordance with the *Classification (Publications, Films and Computer Games) Act* and supplementary instruments, including the National Classification Code. The ACB's classification decisions are reviewed by the CRB, which is responsible for making a fresh decision and issuing a public report on the reviewed decision. The Department of Infrastructure, Transport, Regional Development and Communication is reviewing the National Classification Scheme with a view to update the system to 'suit a modern content market' characterised by media convergence, large volumes of content and multipurpose platforms.[1]

Major Reports, Inquiries, and Related Initiatives:

- Review of Australian classification regulation (ongoing): [Inquiry Webpage] [Discussion Paper][2]

Australian Competition and Consumer Commission (ACCC)

Institutional Form: Independent statutory authority

Responsible Minister: The Treasurer

Principal Instrument(s): *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act (2021), National Broadband Network Companies Act (2011), Competition and Consumer Act (2010) (Consumer Data Right), Telecommunications Act (1997), Radiocommunications Act (1992)*

Mandate: The ACCC is responsible for the promotion of competition, fair trading and regulating the national infrastructure in Australia in accordance with the *Competition and Consumer Act* and a range of additional legislation. This responsibility extends to the economic regulation of the communications sector, including telecommunications and the National Broadband Network, broadcasting, and content sectors. In 2019, the ACCC completed the Digital Platforms Inquiry, reporting on the effects of digital search engines, social media platforms and other digital content aggregation platforms on competition in media and advertising service markets. In response to the findings of the inquiry, amendments were made to the *Competition and Consumer Act* to establish a mandatory code of conduct to rectify the bargaining power imbalances between Australian news media businesses and digital platforms.

Major Reports, Inquiries, and Related Initiatives:

- Digital Platform Services Inquiry 2020–25 (ongoing): [Inquiry Webpage][3]
- ACCC 2021 Compliance and Enforcement Priorities (2022): [Speech Transcript][4]
- Compendium of approaches to improving competition in digital markets (2021): [Report][5]
- Digital Advertising Services Inquiry (2021): [Inquiry Webpage] [Final Report][6]
- Digital Platforms Inquiry (2019): [Inquiry Webpage] [Final Report][7]
- Consumer Data Rights Rules Framework (2018): [Report][8]

Australian Communications and Media Authority (ACMA)

Institutional Form: Independent statutory authority

Responsible Minister: The Minister for Communications, Urban Infrastructure, Cities and the Arts

Principal Instrument(s): *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act (2021), Competition and Consumer Act (2010), Do Not Call Register Act (2006), Australian Communications and Media Authority Act (2005), Spam Act (2003), Interactive Gambling Act (2001), Telecommunications (Consumer Protection and Service Standards) Act (1999), Telecommunications (Carrier Licence Charges) Act (1997), Telecommunications (Numbering Charges) Act (1997), Telecommunications Act (1997), Radiocommunications Act (1992), Broadcasting Services Act (1992), Telecommunications (Interception and Access) Act (1979)*

Mandate: The ACMA is responsible for the regulation of communications and media services in Australia, including telecommunications, spectrum management, broadcasting, content, and datacasting. In accordance with the *Competition and Consumer Act, the* ACMA is responsible for registering news businesses in Australia and shares oversight of the News Media and Digital Platforms Mandatory Bargaining Code with the ACCC.

Major Reports, Inquiries, and Related Initiatives:

- Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act (2021): [Act][9]
- Communications and Media in Australia: Trends and Developments in telecommunications 2020–21 (2021): [Report][10]
- News Media Bargaining Code Guidelines (2021): [Guidelines][11]

*Australian Digital Health Agency (ADHA)

Institutional Form: Corporate Commonwealth entity

Responsible Minister: The Minister for Health and Aged Care

Principal Instrument(s): *Public Governance, Performance and Accountability (Establishing the Australian Digital Health Agency) Rule (2016)*

Mandate: The ADHA is responsible for the development, implementation, management, operation, and innovation of Australia's digital health national infrastructure (i.e., My Health Record system, Healthcare Identifiers Service, secure messaging delivery) as well as progressing digital health in Australia in accordance with the National Digital Health Strategy.

Major Reports, Inquiries, and Related Initiatives:

- National Digital Health Strategy (ongoing): [Initiative Webpage][12]
- Framework for Action: How Australia will deliver the benefits of digitally enabled health and care (2018): [Implementation Plan][13]
- Australia's Digital Health Strategy (2017): [Strategy][14]

Australian Human Rights Commission (AHRC)

(formerly the Human Rights and Equal Opportunity Commission)

Institutional Form: Independent statutory authority

Responsible Minister: The Attorney-General

Principal Instrument(s): *Age Discrimination Act (2004), Disability Discrimination Act (1992), Australian Human Rights Commission Act (1986) (formerly the Human Rights and Equal Opportunity Act (1986)), Sex Discrimination Act (1984), Racial Discrimination Act (1975)*

Mandate: The AHRC is Australia's national human rights institution. It is responsible for protecting human rights in Australia and internationally, including in the context of new technologies. It also investigates complaints about discrimination and human rights breaches. The AHRC conducted a major project on new and emerging technologies under the then Human Rights Commissioner, Edward Santow. The 3-year project considered human rights issues raised by new and emerging technologies. The project culminated in the Human Rights and Technology Final Report, which set out a roadmap for responsible innovation as well as a recommendation for the creation of a new AI Safety Commissioner.

Major Reports, Inquiries, and Related Initiatives:

- Human Rights and Technology (2021): [Initiative Webpage] [Final Report][15]
- Using artificial intelligence to make decisions-Addressing the problem of algorithmic bias (2020) [Technical Paper][16]
- Artificial Intelligence: governance and leadership (2019): [White Paper][17]

Australian Prudential Regulation Authority (APRA)

Institutional Form: Independent statutory authority

Responsible Minister: The Treasurer

Principal Instrument(s): *Australian Prudential Regulation Authority Regulations (2018), Corporate Law Economic Reform Program Act (1999), Australian Prudential Regulation Authority Act (1998), Financial Institutions Supervision Levies Collection Act (1998)*[18]

Mandate: The APRA is the prudential supervisor and resolution authority for much of the Australian financial services sector. It oversees Australia's authorised deposit-taking institutions, general, life and private health insurers, reinsurers, friendly societies and most of the superannuation industry. It is also responsible for the modernisation of prudential architecture, which involves the adaptation and creation of new prudential standards and guidance in response to the digital world and the digitisation of finance, including FinTech and RegTech.

Major Reports, Inquiries, and Related Initiatives:

- APRA Submission on fintech and regtech to the Senate Select Committee on Financial Technology and Regulatory Technology (2021): [APRA Submission] [Committee Webpage][19]
- Prudential Standard CPS 234 Information Security (2019): [Prudential Standard] [Prudential Practice Guide][20]

Australian Securities and Investment Commission (ASIC)

Institutional Form: Independent statutory authority

Responsible Minister: The Treasurer

Principal Instrument(s): *National Credit Consumer Protection Act (2009), Australian Securities and Investments Commission Act (2001), Corporations Act (2001)*

Mandate: ASIC is responsible for the regulation of Australian corporate, markets, financial services, and consumer credit. It provides guidance on operational risk management expectations and obligations, including assessing and improving the cyber resilience of all entities operating in Australia's financial markets. It operates an Innovation Hub, and an enhanced regulatory sandbox (previously FinTech Sandbox) to facilitate innovation, including FinTech and RegTech. The ASIC also regulates misleading or deceptive conduct in the promotion or issuing of crypto-assets or initial coin offering, for example, the use of social media to create the appearance of greater levels of public interest and engagement, having received delegated powers from the Australian Competition and Consumer Commission.

Major Reports, Inquiries, and Related Initiatives:

- Crypto-assets as underlying assets for ETPs and other investment products (2021): [Consultation Paper][21]
- ASIC's regtech initiatives 2019–20 (2021): [Report][22]
- Cyber resilience of firms in Australia's financial markets: 2020–21 (2021): [Report][23]
- Review of the ePayments Code: Further consultation (2021): [Consultation Paper][24]
- Product design and distribution obligations (2020): [Report][25]
- ASIC's regtech initiatives 2018–19 (2019): [Report][26]
- Cyber resilience of firms in Australia's financial markets: 2018–19 (2019): [Report][27]
- Market integrity rules for technological and operational resilience (2019): [Consultation Paper][28]

Australian Taxation Office (ATO)

Institutional Form: Australian Government department

Responsible Minister: The Treasurer

Principal Instrument(s): *A New Tax System (Goods and Services Tax) Act (1999), Income Tax Assessment Act (1997), Fringe Benefits Tax Assessment Act (1986), Taxation Administration Act (1953) Income Tax Assessment Act (1936)*

Mandate: The ATO is the principal revenue collection agency of the Australian Government and is responsible for the administration of Australia's taxation and superannuation systems. In May 2021, the Australian Government announced it would introduce a patent box for corporate income associated with patented inventions in the medical and biotechnology sectors that the ATO will administer. The ATO also has oversight of the Research and Development Tax Incentive.

Major Reports, Inquiries, and Related Initiatives:

- Patent Box (2021): [Discussion Paper][29]
- Research and Development Tax Incentive (2020): [Webpage][30]

Australian Transaction Reports and Analysis Centre (AUSTRAC)

Institutional Form: Statutory agency within Australian Government portfolio

Responsible Minister: The Minister for Home Affairs

Principal Instrument(s): *Anti-Money Laundering and Counter-Terrorism Financing Act (2006), Financial Transaction Reports Act (1998), Financial Transaction Reports Act (1988)*

Mandate: AUSTRAC is responsible for regulating anti-money laundering and counter-terrorism financing in accordance with the *Anti-Money Laundering and Counter-Terrorism Financing Act*. AUSTRAC uses financial intelligence and regulation to disrupt money laundering, terrorism financing, and other serious crime. AUSTRAC regulates more than 15,000 individuals and businesses in the financial, bullion, gambling, and digital currency exchange sectors. AUSTRAC is a member of the Financial Action Task Force (international watchdog for money laundering and terrorist financing)[31], as well as the Asia/Pacific Group on Money Laundering (regional watchdog for money laundering and terrorist financing).[32]

Major Reports, Inquiries, and Related Initiatives:

- Preventing Misuse and Criminal Communication Through Payment Text Fields: Financial Crime Guide (2021): [Report][33]
- Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (2020): [Report][34]
- Combating Online Sexual Abuse and Exploitation Through Financial Intelligence (2020): [Public Bulletin][35]

Department of Defence, Defence Export Controls (DEC)

Institutional Form: Branch within an Australian Government department

Responsible Minister: The Minister for Defence

Principal Instrument(s): *Defence Trade Controls Act (2021), Weapons of Mass Destruction (Prevention of Proliferation) Act (1995), Wassenaar Arrangement on Export Controls for Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Agreement) (1995), Customs (Prohibited Exports) Regulations (1958), Customs Act (1901)*

Mandate: The DEC is responsible for the regulation of military and dual-use goods and technology exports to people or places outside of Australia. The DEC assesses applications, issues authorisations (permits or licences), prohibits weapons-of-mass-destruction-related exports, provides recommendations to the Minister for Defence about export prohibitions, and undertakes compliance and engagement activities.

Major Reports, Inquiries, and Related Initiatives:

- Defence and Strategic Goods List (2021): [List][36]

Department of Home Affairs, Cyber and Infrastructure Security Centre (CISC)

Institutional Form: Group within an Australian Government department

Responsible Minister: The Minister for Home Affairs

Principal Instrument(s): *Security Legislation Amendment (Critical Infrastructure) Act (2021), Security of Critical Infrastructure Act (2018), Telecommunications Act (1997)*

Mandate: The CISC has a regulatory and partnership function to protect critical infrastructure in Australia. It has oversight of critical infrastructure cyber security obligations that came into effect on 2 December 2021, including mandatory cyber incident reporting. At the time of writing, critical infrastructure cyber security legislative proposals were before the Parliament. If passed, they will enact a framework for risk management programs, declarations of systems of national significance, and enhanced cyber security obligations.

Major Reports, Inquiries, and Related Initiatives:

- Security Legislation Amendment (Critical Infrastructure Protection) Bill (2022): [Bill][37]
- Security Legislation Amendment (Critical Infrastructure) Act (2021): [Act][38]
- Strengthening Australia's cyber security regulations and incentives (2021): [Discussion Paper][39]
- Australia's Cyber Security Strategy (2020): [Strategy][40]
- Security of Critical Infrastructure Act (2018): [Act][41]

Department of Treasury, Foreign Investment Review Board (FIRB)

Institutional Form: Independent non-statutory authority within an Australian Government department

Responsible Minister: The Treasurer

Principal Instrument(s): *Australia's Foreign Investment Policy (2021), Security of Critical Infrastructure Act (2018), Foreign Acquisitions and Takeovers Fees Impositions Act (2015), Foreign Acquisitions and Takeovers Act (1975)*

Mandate: The FIRB examines proposed foreign investments in Australia and provides advice and recommendations to the Treasurer and other ministers. It monitors compliance within the foreign-investment framework and provides guidance on foreign investment related to critical minerals, critical technologies, information technology, data, and the Cloud. Amendments to the *Security of Critical Infrastructure Act*, specifically the expansion of the scope of critical infrastructure assets and sectors, means more businesses are subject to the FIRB review process.[42] The FIRB has an advisory role and responsibility for making decisions rests with the Treasurer. The Treasury also has tech policy responsibilities that are outside the scope of this overview.

Major Reports, Inquiries, and Related Initiatives:

- Foreign Investment Reform (Protecting Australia's National Security) Act (2020): [Act][43]
- Foreign Acquisitions and Takeovers Fees Impositions Act (2020): [Act][44]
- Inquiry into Foreign Investment Proposals (2019): [Inquiry Webpage] [Final Report][45]

Digital Platforms Regulators Forum (DP-REG)

Institutional Form: Non-statutory forum

Responsible Minister: Not applicable

Principal Instrument(s): DP-REG Terms of Reference

Mandate: The DP-REG is a forum for Australian regulators to 'share information about, and collaborate on, cross-cutting issues and activities relating to the regulation of digital platforms'.[46] This includes search engines, digital content aggregators, social media services, private messaging services, media referral services, and electronic marketplaces. The DP-REG is not a forum for issues relating to cyber security or cybercrime. The DP-REG has an advisory role, which has no bearing on members' existing regulatory powers, legislative functions, or responsibilities. The standing members of the DP-REG are the Australian Competition and Consumer Commission, Office of the Australian Information Commissioner, Australian Communications and Media Authority, and the Office of the eSafety Commissioner. By agreement among members, other relevant Australian regulatory agencies may be invited to join the DP-REG or attend meetings on an ad-hoc basis.

Major Reports, Inquiries, and Related Initiatives:

- DP-REG Terms of Reference (2022): [Terms of Reference][47]

IP Australia

Institutional Form: Independent portfolio agency

Responsible Minister: The Minister for Industry, Science and Technology

Principal Instrument(s): *Intellectual Property Laws Amendment (Productivity Commission Response Part 2 and Other Measures) Act (2020), Designs Act (2003), Trade Marks Act (1995), Patents Act (1990)*

Mandate: IP Australia is responsible for the administration of Australia's intellectual property rights system, including trade marks, patents, designs and plant breeder's rights. At the international level, IP Australia is involved in developing standards for intellectual property rights data and the use of artificial intelligence and automation. It also co-leads the World Intellectual Property Organization (WIPO) Blockchain Task Force in drafting standards of use of blockchain technology.

Major Reports, Inquiries, and Related Initiatives:

- Committee on WIPO Standards (CWS): Report by the Blockchain Task Force (Task No. 59) (2021): [Report][48]
- Thaler v Commissioner of Patents [2021] FCA 879: [Federal Court of Australia Decision][49]
- Designs Amendment (Advisory Council on Intellectual Property Response) Act (2021): [Act][50]
- Designs Amendment (Advisory Council on Intellectual Property Response) Bill (2020): [Inquiry Webpage][51]
- Intellectual Property Laws Amendment (Productivity Commission Response Part 2 and Other Measures) Act (2020): [Act][52]
- IP Australia and the Future of Intellectual Property: Megatrends, scenarios and their strategic implications (2017): [Report][53]

Office of the Australian Information Commissioner (OAIC)

Institutional Form: Independent statutory agency

Responsible Minister: The Attorney-General

Principal Instrument(s): *Competition and Consumer (Consumer Data Right) Rules (2020), Treasury Laws Amendment (Consumer Data Right) Act (2019), Australian Information Commissioner Act (2010), Privacy Act (1988), Telecommunications Act (1997), Freedom of Information Act (1982), Telecommunications (Interceptions and Access) Act (1979)*

Mandate: The OAIC's purpose is to promote and uphold privacy and information access rights in accordance with the *Privacy Act* and the *Australian Privacy Principles, and Freedom of Information Act*. The OAIC also has regulatory powers with respect to-Consumer Data Right (jointly with the Australian Competition and Consumer Commission)[54], data retention obligations and the Notifiable Data Breaches Scheme.[55] The OAIC conducts investigations, handles complaints, and approves and registers enforceable codes.

Major Reports, Inquiries, and Related Initiatives:

- Facebook Inc v Australian Information Commissioner [2022] FCAFC 9 (2022): [Federal Court Judgement][56]
- Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54 (14 October 2021) (2021): [Determination][57]
- Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner (2021): [Discussion Paper] [Review Webpage][58]
- Privacy (Market and Social Research) Code (2021): [Code][59]
- Freedom of Information Regulatory Action Policy (2020): [Policy][60]
- Privacy (Credit Reporting) Code 2014 (Version 2.1) (2020): [Code][61]
- 2020 Australian Community Attitudes to Privacy Survey (2020): [Report][62]
- Treasury Laws Amendment (Consumer Data Right) Act (2019): [Act][63]
- Privacy Regulatory Action Policy (2018): [Policy][64]

Office of the eSafety Commissioner (eSafety)

Institutional Form: Independent statutory officer, supported by ACMA

Responsible Minister: The Minister for Communications, Urban Infrastructure, Cities and the Arts

Principal Instrument(s): *Online Safety Act (2021), Telecommunications Act (1997), Criminal Code Act (1995)*

Mandate: eSafety is responsible for the regulation of online safety in Australia. The eSafety Commissioner is an independent statutory officer and the Office's staff are employed by the Australian Communications and Media Authority. eSafety was established in 2015 and its powers were significantly expanded by the *Online Safety Act* that included an Adult Cyber Abuse Scheme, broadened the Cyberbullying Scheme for children, updated the Image-Based Abuse Scheme and Abhorrent Violent Conduct powers, strengthened information-gathering powers, expanded the Illegal and Restricted Content Scheme, and added the Basic Online Safety Expectations. eSafety is consulting on the development of industry codes, restricted access systems, and an Age Verification Roadmap.

Major Reports, Inquiries, and Related Initiatives:

- Basic Online Safety Expectations (2022): [Expectations][65]
- Online Safety Act (2021): [Act][66]
- eSafety Regulatory Posture and Regulatory Priorities 2021–2022 (2021): [Report][67]
- Adult Cyber Abuse Scheme (2021): [Regulatory Guidance][68]
- Cyberbullying Scheme (2021): [Regulatory Guidance][69]
- Image-Based Abuse Scheme (2021): [Regulatory Guidance][70]
- Online Content Scheme (2021): [Regulatory Guidance][71]
- Abhorrent Violent Conduct Powers (2021): [Regulatory Guidance][72]
- Draft Restricted Access Systems Declaration (2021): [Draft Declaration][73]
- Mandatory Age Verification Regime: Consultation (2021): [Consultation Webpage][74]
- Development of industry codes under the Online Safety Act (2021): [Position Paper][75]

*Office of the Gene Technology Regulator (OGTR)

Institutional Form: Independent statutory officer, supported by the Department of Health

Responsible Minister: The Minister for Aged Care and Senior Australians

Principal Instrument(s): *Gene Technology Regulations (2001), Gene Technology Agreement (2001), Gene Technology Act (2000)*

Mandate: The OGTR is responsible for protecting the health and safety of people, as well as the environment, from risks posed by gene technology. The OGTR priorities are the prohibition of dealings with genetically modified organisms unless authorised, monitoring and enforcement of legislation, assessing risk, establishing committees to provide expert advice, appointing statutory officers to make decisions under the legislation, and establishing a centralised, publicly available database of all genetically modified organisms approved in Australia.

Major Reports, Inquiries, and Related Initiatives:

- Gene Technology Technical Advisory Committee 13 December 2021 (2021): [Communique][76]

Office of the Independent National Security Legislation Monitor (INSLM)

Institutional Form: Independent statutory officer

Responsible Minister: The Attorney-General

Principal Instrument(s): *Independent National Security Legislation Monitor Act (2010)*

Mandate: The INSLM is responsible for reviewing the operation, effectiveness and implications of Australia's national security and counter-terrorism laws in accordance with the *Independent National Security Legislation Monitor Act*. The INSLM considers whether laws are proportionate to terrorism and national security threats and are necessary as well as whether the laws contain appropriate protections for individual rights.

Major Reports, Inquiries, and Related Initiatives:

- Trust But Verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters (2020): [Report][77]
- Telecommunications and Other Legislation Amendment (Assistance and Access) Act (2018): [Act][78]

Office of the Inspector-General of Intelligence and Security (IGIS)

Institutional Form: Independent statutory authority

Responsible Minister: The Attorney-General

Principal Instrument(s): *Telecommunications and Other Legislation Amendment (Assistance and Access) Act (2018), Inspector-General of Intelligence and Security Act (1986)*

Mandate: The IGIS is responsible for overseeing and reviewing the activities of Australia's intelligence agencies with respect to legality and propriety, and for consistency with human rights. The IGIS regularly inspects and monitors the activities of intelligence agencies and has the authority to independently initiate an inquiry. The IGIS also undertakes formal inquiries into the activities of intelligence agencies in response to complaints or reference from a minister. Specific to tech regulation, the IGIS has oversight of the use of the powers in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* by the Australian Security Intelligence Organisation, the Australian Signals Directorate, Australian Secret Intelligence Service, the Commonwealth Ombudsman, Australian Federal Police, Australian Criminal Intelligence Commission, and state and territory police.

Major Reports, Inquiries, and Related Initiatives: None issued

Office of the National Data Commissioner (ONDC)

Institutional Form: Independent statutory officer, supported by Prime Minister and Cabinet (PMC)

Responsible Minister: The Prime Minister

Principal Instrument(s): *Data Availability and Transparency Act (2022), Data Availability and Transparency (Consequential Amendments) Act 2022*

Mandate: The ONDC is responsible for streamlining the use of public sector data and the way in which it is shared. The *Data Availability and Transparency Act* establishes a data-sharing scheme to allow controlled access to Australian Government data. Accreditation in the scheme is overseen by the ONDC.

Major Reports, Inquiries, and Related Initiatives:

- Data Availability and Transparency Act (2022): [Act][79]
- Data Availability and Transparency (Consequential Amendments) Act (2022): [Act][80]
- Data Availability and Transparency (Consequential Amendments) Bill (2020): [Bill][81]
- Accreditation Framework Discussion Paper (2020): [Discussion Paper][82]
- Data Sharing and Release Legislative Reforms (2019): [Discussion Paper][83]

Reserve Bank of Australia, Payments Systems Board (PSB)

Institutional Form: Independent statutory board

Responsible Minister: The Treasurer

Principal Instrument(s): *Part 7.3 of the Corporations Act (2001), Payment Systems (Regulation) Act (1998), Payment Systems and Netting Act (1998), Cheques Act (1986), Reserve Bank Act (1959)*

Mandate: The PSB is responsible for the efficiency and competitiveness of the payments system in Australia. It administers the regulatory framework that implements Australian Government policies and priorities relating to the payments system in a manner that is consistent with financial system stability. The PSB is also responsible for determining the Reserve Bank of Australia's payments system policy with the goal of controlling risk in the financial system, while promoting efficiency in the payments system and competition in the market for payment services.

Major Reports, Inquiries, and Related Initiatives:

- Review of the Australian Payments System (2021): [Review Webpage][84]
- Select Committee on Australia as a Technology and Financial Centre (2021): [Final Report][85]
- Mobile Payment and Digital Wallet Financial Services (2021): [Joint Parliamentary Report][86]

Ongoing Parliamentary Committees, Inquiries, or Legislative Proposals (not previously referred to):

- Senate Select Committee on Foreign Interference through Social Media (ongoing): [Committee Webpage][87]
- Trusted Digital Identity Bill 2021 (ongoing): [Exposure Draft][88]
- Ransomware Payments Bill 2021 (No. 2) (ongoing): [Bill Webpage][89]
- Social Media (Basic Expectations and Defamation) Bill 2021 (ongoing): [Bill Webpage][90]
- Senate Select Committee on Social Media and Online Safety (2022): [Committee Webpage] [Final Report][91]
- Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (2021): [Inquiry Webpage] [Final Report][92]

Other

- Department of the Prime Minister and Cabinet: Australian Government regulator stocktake (ongoing): [Website][93]

Endnotes (Australia)

1. Department of Communication and the Arts 2020, *Review of Australian classification regulation*, accessed 30 March 2022, www.infrastructure.gov.au/sites/default/files/consultation/pdf/review-of-australian-classification-regulation.pdf, p. 5.

2. Department of Communication and the Arts 2020, *Review of Australian classification regulation*, accessed 30 March 2022, www.infrastructure.gov.au/have-your-say/review-australian-classification-regulation (webpage). See also the discussion paper: Department of Communication and the Arts 2020, *Review of Australian classification regulation*, accessed 30 March 2022, www.infrastructure.gov.au/sites/default/files/consultation/pdf/review-of-australian-classification-regulation.pdf.

3. Australian Competition and Consumer Commission 2022, *Digital Platform Services Inquiry 2020-2025*, accessed 30 March 2022, www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025.

4. Sims, R 2021, *ACCC 2021 Compliance and Enforcement Priorities*, transcript, Committee for Economic Development Australia (Conference), accessed 30 March 2022, www.accc.gov.au/speech/accc-2021-compliance-and-enforcement-priorities.

5. G7 2021, *Compendium of approaches to improving competition in digital markets*, accessed 30 March 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1044981/Compendium_of_approachess_to_improving_competition_in_digital_markets_publication.pdf.

6. Australian Competition and Consumer Commission 2021, *Digital advertising services inquiry*, accessed 30 March 2022, www.accc.gov.au/focus-areas/inquiries-finalised/digital-advertising-services-inquiry. See also the final report: Australian Competition and Consumer Commission (ACCC) 2021, *Digital advertising services inquiry*, accessed 30 March 2022, www.accc.gov.au/publications/digital-advertising-services-inquiry-final-report.

7. Australian Competition and Consumer Commission 2019, *Digital platforms inquiry*, accessed 30 March 2022, www.accc.gov.au/focus-areas/inquiries-finalised/digital-platforms-inquiry-0. See also the final report: Australian Competition and Consumer Commission 2019, *Digital platforms inquiry*, accessed 30 March 2022, www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

8. Australian Competition and Consumer Commission 2018, *Consumer Data Rights Rules Framework*, accessed 30 March 2022, www.accc.gov.au/system/files/ACCC%20CDR%20Rules%20Framework%20%28final%29.pdf.

9. *Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act (2021)* accessed 30 March 2022, www.legislation.gov.au/Details/C2021A00021.

10. Australian Communications and Media Authority 2021, *Communications and media in Australia: Trends and developments in telecommunications 2020–21*, accessed 30 March 2022, www.acma.gov.au/publications/2021-12/report/communications-and-media-australia-trends-and-developments-telecommunications-2020-21.

11. Australian Communications and Media Authority 2021, *News media bargaining code*, access 30 March 2022, www.acma.gov.au/news-media-bargaining-code.

12. Australian Digital Health Agency 2021, *National Digital Health Strategy*, accessed 30 March 2022, https://nationalstrategy.digitalhealth.gov.au.

13. Australian Digital Health Agency 2018, *Framework for Action: How Australia will deliver the benefits of digitally enabled health and care*, accessed 30 March 2022, www.digitalhealth.gov.au/sites/default/files/2020-11/Framework_for_Action.pdf.

14. Australian Digital Health Agency 2017, *Australia's Digital Health Strategy*, accessed 30 March 2022, www.digitalhealth.gov.au/about-us/strategies-and-plans/national-digital-health-strategy-and-framework-for-action.

15. Australian Human Rights Commission 2021, *Human Rights and Technology*, accessed 30 March 2022, https://tech.humanrights.gov.au/?_ga=2.255585224.1327761532.1643272340-1216567272.1643092263. See also the final report: Australian Human Rights Commission 2021, *Human Rights and Technology*, accessed 30 March 2022, https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2021_Final_Report.pdf.

16. Australian Human Rights Commission 2020, *Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias*, accessed 30 March 2022, https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2020_algorithmic_bias.pdf.

17. Australian Human Rights Commission 2019, *Artificial Intelligence: governance and leadership*, accessed 30 March 2022, https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2019_AI_whitepaper.pdf.

18. For a full list of APRA's enabling legislation, see: Australian Prudential Regulation Authority 2022, *Enabling legislation*, accessed 30 March 2022, www.apra.gov.au/enabling-legislation.

19. Australian Prudential Regulation Authority 2020, *Senate Select Committee on Financial Technology and Regulatory Technology*, accessed 30 March 2022, www.apra.gov.au/sites/default/files/2020-01/Senate%20Select%20Committee%20on%20Financial%20Technology%20and%20Regulatory%20Technology.pdf. See also: Select Committee on Australia as a Technology and Financial Centre 2021, *Australia as a Technology and Financial Centre,* accessed 30 March 2022, www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/AusTechFinCentre.

20. Prudential Standard CPS 234 Information Security 2019, accessed 30 March 2022, www.legislation.gov.au/Details/F2018L01745. See also: Australian Prudential Regulation Authority 2019, *Prudential Practice Guide: PG 234 Information Security*, accessed 30 March 2022, www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_0.pdf.

21. Australian Securities and Investment Commission 2021, *Crypto-assets as underlying assets for ETPS and other investment products*, accessed 30 March 2022, https://asic.gov.au/media/yhbgvq02/cp343-published-30-june-2021.pdf.

22. Australian Securities and Investment Commission 2021, *ASIC's regtech initiatives 2019–20*, accessed 30 March 2022, https://download.asic.gov.au/media/5937756/rep685-published-20-january-2021.pdf.

23. Australian Securities and Investment Commission 2021, *Cyber resilience of firms in Australia's financial markets: 2020–21*, accessed 30 March 2022, https://download.asic.gov.au/media/fmfdhegw/rep716-published-6-december-2021.pdf.

24. Australian Securities and Investment Commission 2021, *Review of the ePayments Code: Further consultation*, accessed 30 March 2022, https://download.asic.gov.au/media/eh2fceff/cp341-published-21-may-2021.pdf.

25. Australian Securities and Investment Commission 2020, *Product design and distribution obligations*, accessed 30 March 2022, https://download.asic.gov.au/media/5886971/rg274-published-11-december-2020.pdf.

26. Australian Securities and Investment Commission 2019, *ASIC's regtech initiatives 2018–19*, accessed 30 March 2022, https://download.asic.gov.au/media/5424092/rep653-published-20-december-2019.pdf.

27. Australian Securities and Investment Commission 2019, *Cyber resilience of firms in Australia's financial markets: 2018–19*, accessed 30 March 2022, https://download.asic.gov.au/media/5416529/rep651-published-18-december-2019.pdf.

28. Australian Securities and Investment Commission 2019, *Market integrity rules for technological and operational resilience*, accessed 31 March 2022, https://asic.gov.au/regulatory-resources/find-a-document/consultation-papers/cp-314-market-integrity-rules-for-technological-and-operational-resilience/.

29. Australian Taxation Office 2021, *Patent Box: Discussion paper on policy design*, accessed 31 March 2022, https://treasury.gov.au/sites/default/files/2021-07/c2021_177849.pdf.

30. Australian Taxation Office 2020, *Research and Development Tax Incentive*, accessed 31 March 2022, www.ato.gov.au/Business/Research-and-development-tax-incentive/.

31. Financial Action Task Force 2022, accessed 31 March 2022, www.fatf-gafi.org/about/whoweare/.

32. Asia/ Pacific Group on Money Laundering 2022, accessed 31 March 2022, www.apgml.org.

33. Australian Transaction Reports and Analysis Centre 2021, *Preventing Misuse and Criminal Communication Through Payment Text Fields: Financial Crime Guide,* accessed 31 March 2022, www.austrac.gov.au/sites/default/files/2021-11/Financial%20crime%20guide%20-%20Preventing%20misuse%20and%20criminal%20communication%20through%20payment%20text%20fields_0.pdf.

34. Financial Action Task Force 2020, *Virtual Assets-Red Flag Indicators of Money Laundering and Terrorist Financing*, accessed 31 March 2022, www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html.

35. Egmont Group of Financial Intelligence Units 2020, *Combating Online Child Sexual Abuse and Exploitation Through Financial Intelligence*, accessed 31 March 2022, https://egmontgroup.org/wp-content/uploads/2021/09/2020_Public_Bulletin_Combatting_Online_Child_Sexual_Abuse_and_Exploitation_Through_Financial_Intelligence.pdf.

36. Department of Defence 2021, *Defence and Strategic Goods List 2021*, accessed 31 March 2022, www.legislation.gov.au/Details/F2021L01198.

37. Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022, accessed 31 March 2022, www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6833.

38. Security Legislation Amendment (Critical Infrastructure) Act 2021, accessed 31 March 2022, www.legislation.gov.au/Details/C2021A00124.

39. Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives: An initiative of Australia's Cyber Security Strategy 2020* 2021, accessed 31 March 2022, www.homeaffairs.gov.au/reports-and-pubs/files/strengthening-australia-cyber-security-regulations-discussion-paper.pdf.

40. Department of Home Affairs 2020, *Australia's Cyber Security Strategy 2020*, accessed 31 March 2022, www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

41. *Security of Critical Infrastructure Act 2018*, accessed 31 March 2022, www.legislation.gov.au/Details/C2021C00570.

42. Moore, D & Lai, M 2021, *Critical infrastructure changes expand the FIRB rules*, Minter Ellison, accessed 31 March 2022, www.minterellison.com/articles/critical-infrastructure-changes-expand-the-firb-rules.

43. *Foreign Investment Reform (Protecting Australia's National Security) Act 2020,* accessed 31 March 2022, www.legislation.gov.au/Details/C2021C00358.

44. *Foreign Acquisitions and Takeovers Fees Imposition Amendment Act 2020,* accessed 31 March 2022, www.legislation.gov.au/Details/C2020A00115.

45. Parliament of Australia 2021, Inquiry into Foreign Investment Proposals, accessed 31 March 2022, www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Foreigninvestment. See also the final report from the inquiry: Economics References Committee 2021, *Greenfields, cash cows and the regulation of foreign investment in Australia*, accessed 31 March 2022, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024433/toc_pdf/Greenfields,cashcowsandtheregulationofforeigninvestmentinAustralia.pdf;fileType=application%2Fpdf.

46. Australian Communications and Media Authority 2022, *Digital Platform Regulators Forum (DP-REG) Terms of Reference,* accessed 31 March 2022, www.acma.gov.au/sites/default/files/2022-03/DP-REG%20Terms%20of%20Reference%20.pdf.

47. Australian Communications and Media Authority 2022, *Digital Platform Regulators Forum (DP-REG) Terms of Reference,* accessed 31 March 2022, www.acma.gov.au/sites/default/files/2022-03/DP-REG%20Terms%20of%20Reference%20.pdf.

48. Committee on WIPO Standards 2021, *Report by the Blockchain Task Force (Task No. 59)*, accessed 31 March 2022, www.wipo.int/edocs/mdocs/cws/en/cws_9/cws_9_7.pdf.

49. *Thaler v Commissioner of Patents [2021] FCA 879*, accessed 31 March 2022, www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2021/2021fca0879.

50. *Designs Amendment (Advisory Council on Intellectual Property Response) Act (2021),* accessed 31 March 2022, www.legislation.gov.au/Details/C2021A00100.

51. *Designs Amendment (Advisory Council on Intellectual Property Response) Bill (2020),* accessed 31 March 2022, https://parlwork.aph.gov.au/Bills/s1279.

52. Intellectual Property Laws Amendment (Productivity Commission Response Part 2 and Other Measures) Act (2020), accessed 31 March 2022, www.legislation.gov.au/Details/C2020A00009.

53. IP Australia 2017, *IP Australia and the Future of Intellectual Property: Megatrends, scenarios and their strategic implications*, accessed 31 March 2022, www.ipaustralia.gov.au/sites/default/files/ip_australia_and_the_future_of_intellectual_property.pdf.

54. Australian Competition and Consumer Commission 2022, *Consumer data right (CDR)*, accessed 31 March 2022, www.accc.gov.au/focus-areas/consumer-data-right-cdr-0.

55. Office of the Australian Information Commissioner n.d., *Notifiable data breaches*, accessed 31 March 2022, https://www.oaic.gov.au/privacy/notifiable-data-breaches.

56. *Facebook Inc v Australian Information Commissioner [2022] FCAFC 9,* accessed 31 March 2022, www.judgments.fedcourt.gov.au/judgments/Judgments/fca/full/2022/2022fcafc0009.

57. *Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54 (14 October 2021),* accessed 31 March 2022, www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html.

58. Falk A 2021, *Privacy Act Review – Discussion Paper: Submission by the Office of the Australian Information Commissioner*, accessed 31 March 2022, www.oaic.gov.au/__data/assets/pdf_file/0023/11894/OAIC-submission-to-Privacy-Act~scussion-Paper-December-2021.PDF. See also: the Review of the Privacy Act 1988 webpage, accessed 31 March 2022, www.ag.gov.au/integrity/consultations/review-privacy-act-1988.

59. Office of the Australian Information Commissioner 2021, *Privacy (Market and Social Research) Code 2021*, accessed 31 March 2022, www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/privacy-market-and-social-research-code-2021.

60. Office of the Australian Information Commissioner 2020, *Freedom of Information Regulatory Action Policy*, accessed 31 March 2022, www.oaic.gov.au/about-us/our-regulatory-approach/freedom-of-information-regulatory-action-policy.

61. Office of the Australian Information Commissioner 2020, *Privacy (Credit Reporting) Code 2014 (Version 2.1)*, www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/cr-code.

62. Office of the Australian Information Commissioner 2020, *Privacy (Credit Reporting) Code 2014 (Version 2.1),* accessed 31 March 2022, www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/cr-code.

63. *Treasury Laws Amendment (Consumer Data Right) Act (2019),* accessed 31 March 2022, http://classic.austlii.edu.au/au/legis/cth/num_act/tladra2019450/.

64. Office of the Australian Information Commissioner (OAIC) 2018, *Privacy Regulatory Action Policy*, accessed 31 March 2022, www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy.

65. Office of the eSafety Commissioner 2022, *The Basic Online Safety Expectations are a key element of the Online Safety Act,* accessed 31 March 2022, www.esafety.gov.au/about-us/who-we-are/basic-online-safety-expectations.

66. *Online Safety Act (2021)*, accessed 31 March 2022, www.legislation.gov.au/Details/C2022C00052.

67. Office of the eSafety Commissioner 2021, *eSafety Regulator Posture and Regulatory Priorities: 2021-22,* www.esafety.gov.au/sites/default/files/2021-11/OSA%20-%20Regulatory%20Posture%20and%20Priorities.pdf.

68. Office of the eSafety Commissioner 2021, *Adult Cyber Abuse Scheme,* accessed 31 March 2022, www.esafety.gov.au/sites/default/files/2021-12/ACA%20Scheme%20Regulatory%20Guidance%20%20FINAL.pdf.

69. Office of the eSafety Commissioner 2021, *Cyberbullying Scheme,* accessed 31 March 2022, www.esafety.gov.au/sites/default/files/2021-11/OSA%20-%20Cyberbullying%20Regulatory%20Guidance%20V3.pdf.

70. Office of the eSafety Commissioner 2021, *Image-Based Abuse Scheme, accessed 31 March 2022,* www.esafety.gov.au/sites/default/files/2021-11/OSA%20-%20IBA%20Scheme%20Regulatory%20Guidance.pdf.

71. Office of the eSafety Commissioner 2021, *Online Content Scheme,* accessed 31 March 2022, www.esafety.gov.au/sites/default/files/2021-12/eSafety-Online-Content-Scheme.pdf.

72. Office of the eSafety Commissioner 2021, *Abhorrent Violent Conduct Powers,* accessed 31 March 2022, www.esafety.gov.au/sites/default/files/2021-12/OSA-AVCP-Regulatory-Guidance.pdf.

73. Office of the eSafety Commissioner 2021, *Draft Restricted Access Systems Declaration,* accessed 31 March 2022, www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system.

74. Office of the eSafety Commissioner 2021, *Mandatory Age Verification Regime: Consultation,* accessed 31 March 2022, www.esafety.gov.au/about-us/consultation-cooperation/age-verification.

75. Office of the eSafety Commissioner 2021, *Development of industry codes under the Online Safety Act,* accessed 31 March 2022, www.esafety.gov.au/sites/default/files/2021-09/eSafety%20Industry%20Codes%20Position%20Paper.pdf.

76. Office of the Gene Technology Regulator 2021, *This Communiqué covers matters considered at the 28th videoconference of the Gene Technology Technical Advisory Committee (13 December 2021)*, accessed 31 March 2022, www.ogtr.gov.au/sites/default/files/2022-03/communique-gttac-meeting-13-december-2021.pdf.

77. Renwick, J 2020, *Trust But Verify: A report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters*, Independent National Security Legislation Monitor, www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf.

78. *Telecommunications and Other Legislation Amendment (Assistance and Access) Act (2018),* accessed 31 March 2022, www.legislation.gov.au/Details/C2021C00496.

79. *Data Availability and Transparency Act 2022,* accessed 11 April 2022, www.legislation.gov.au/Series/C2022A00011.

80. *Data Availability and Transparency (Consequential Amendments) Act 2022,* accessed 11 April 2022, www.legislation.gov.au/Details/C2022A00012.

81. *Data Availability and Transparency (Consequential Amendments) Bill (2020),* accessed 31 March 2022, www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6650.

82. Office of the National Data Commissioner 2020, *Accreditation Framework Discussion Paper*, accessed 31 March 2022, https://datacommissioner.gov.au/sites/default/files/2020-09/Accreditation%20Framework%20Discussion%20Paper.pdf.

83. Office of the National Data Commissioner 2019, *Data Sharing and Release Legislative Reforms*, accessed 31 March 2022, https://datacommissioner.gov.au/sites/default/files/2019-09/Data%20Sharing%20and%20Release%20Legislative%20Reforms%20Discussion%20Paper%20-%20Accessibility.pdf.

84. The Treasury 2020, *Review of the Australian Payments System*, accessed 31 March 2022, https://treasury.gov.au/review/review-australian-payments-system.

85. Commonwealth of Australia 2021, *Select Committee on Australia as a Technology and Financial Centre*, accessed 31 March 2022, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024747/toc_pdf/Finalreport.pdf;fileType=application/pdf.

86. Commonwealth of Australia 2021, *Mobile Payment and Digital Wallet Financial Services*, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024736/toc_pdf/MobilePaymentandDigitalWalletFinancialServices.pdf;fileType=application/pdf.

87. Commonwealth of Australia 2022, *Foreign Interference through Social Media,* accessed 31 March 2022, www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_through_Social_Media/ForeignInterference.

88. Commonwealth of Australia 2022, *Exposure Draft: Trusted Identity Bill 2021*, accessed 31 March 2022, www.digitalidentity.gov.au/sites/default/files/2021-09/Trusted%20Digital%20Identity%20Bill%202021%20exposure%20draft.pdf.

89. *Ransomware Payments Bill 2021 (No. 2),* accessed 31 March 2022, www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1313.

90. *Social Media (Basic Expectations and Defamation) Bill 2021,* accessed 31 March 2022, www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6791.

91. Commonwealth of Australia 2022, *Inquiry into Social Media and Online Safety*, accessed 31 March 2022, www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Media_and_Online_Safety/SocialMediaandSafety. See also: Commonwealth of Australia 2022, *Social Media and Online Safety*, accessed 11 April 2022, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024877/toc_pdf/SocialMediaandOnlineSafety.pdf;fileType=application%2Fpdf.

92. Commonwealth of Australia 2022, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018,* accessed 31 March 2022, www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018. See also: Commonwealth of Australia 2021, *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, accessed 11 April 2022, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024428/toc_pdf/ReviewoftheamendmentsmadebytheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf.

93. Department of Prime Minister and Cabinet n.d., *Australian Government regulator stocktake,* accessed 6 April 2022, https://deregulation.pmc.gov.au/priorities/regulator-best-practice-and-performance/regulator-stocktake.

China

Dr Rogier Creemers, Leiden University

Central Commission for Cybersecurity and Informatization (CCCI)

Institutional Form: Body subordinate to the Central Committee of the Chinese Communist Party

Responsible Minister: The General Secretary of the Chinese Communist Party (Chair of the Commission)

Principal Instrument(s): Not applicable

Mandate: The CCCI groups the heads and/or deputy heads of all important digital technology-related Party and State bodies, including regulators and the military. These include, amongst others, the Central Propaganda Committee, the Central Military Commission, the Central Political-Legal Committee, the Cyberspace Administration of China, the Ministry of Public Security, the Ministry Affairs, the People's Bank of China, the Ministry of Science and Technology, and the Ministry of Industry and Information Technology. Its predominant task is to set major policy directions in the digital field. It does not act as a regulator in its own right. Its most important recent policy decision is the 14th Five-Year Plan for National Informatisation, which outlines the priorities for digital policy over the years 2022–26.

Major Reports, Inquiries, and Related Initiatives:

- 14th Five-Year Plan for National Informatization (2021): [Report] (In Chinese) [Report] (Unofficial Translation)[1]

Cyberspace Administration of China (CAC)

Institutional Form: Dual Party and State body, ministerial rank

Responsible Minister: The Director of the CAC

Principal Instrument(s): *Data Security Law (2021, unofficial translation)*[2]*, Personal Information Protection Law (2021, official translation)*[3]*, Cybersecurity Law (2016, unofficial translation)*[4]*, Notice concerning Empowering the Cyberspace Administration of China to Be Responsible for Internet Information Content Management Work (2014, unofficial translation)*[5]

Mandate: The CAC acts as a policy coordinator associated with the CCCI and integrates the different regulatory steps taken by the various line ministries. As such, it makes policy decisions and drafts national digital strategies. The CAC has regulatory responsibilities in the fields of online content control (including broadcasting), data security, personal information protection, cyber security review of software and hardware products, and digital market oversight. It has bureaucratic authority over specialised technical bodies, including TC260 (which sets technical standards for cybersecurity), CNNIC (the Chinese DNS registry) and CNCERT/CC, (the Chinese Computer Emergency Response Team).

Major Reports, Inquiries, and Related Initiatives:

- 14th Five-Year Plan for the Development of the Digital Economy (2021): [Report] (In Chinese)[6]
- 14th Five-Year Plan for Advancing National Governmental Informatization (2021): [Report] (In Chinese)[7]
- Some Opinions concerning Promoting the Health and Orderly Development of the Platform Economy (Jointly with SAMR, MIIT, MOFCOM, PBoC and STA) (2021): [Report] (In Chinese)[8]
- Guiding Opinions on Strengthening the Comprehensive Governance of Network Information Service Algorithms (Jointly with MIIT, MPS, SAMR) (2021): [Report] (In Chinese) [Report] (Unofficial Translation)[9]
- Guiding Opinions concerning Strengthening Standardized Management Work of Live Streaming (Jointly with MIIT, MPS, SAMR) (2021): [Report] (In Chinese)[10]
- Opinions concerning Further Consolidating the Dominant Responsibility of Platform Companies for Information Content Management (2021): [Report] (In Chinese)[11]

Ministry of Industry and Information Technology (MIIT)

Institutional Form: Ministry

Responsible Minister: The Minister of Industry and Information Technology

Principal Instrument(s): *Cybersecurity Law (2016, unofficial translation)*[12], *Telecommunications Regulations of the People's Republic of China (2000, official translation)*[13]

Mandate: The MIIT is primarily responsible for regulating China's telecommunications and internet infrastructure, including the roll-out of 5G technology and related security protection tasks. It assists the CAC and the Ministry of Public Security to carry out their responsibilities relating to harmful information, data security and cybercrime. The MIIT has administrative oversight of the China Academy for Information and Communication Technologies, a research body that issues regular reports and white papers on the development of ICT infrastructure specifically, and digital policy implementation more broadly.

Major Reports, Inquiries, and Related Initiatives:

- Guiding Opinions concerning Accelerating the Promotion of the Application and Industrial Development of Blockchain Technologies (Jointly with CAC) (2021): [Report] (In Chinese)[14]
- Big Data (2021): [White Paper] (In Chinese)[15]
- Internet Law and Regulation (2021): [White Paper] (In Chinese)[16]
- Blockchain (2021): [White Paper] (In Chinese)[17]
- Fintech (2021): [White Paper] (In Chinese)[18]

Ministry of Public Security (MPS)

Institutional Form: Ministry

Responsible Minister: The Minister of Public Security

Principal Instrument(s): *Data Security Law (2021, unofficial translation)*[19], *Personal Information Protection Law (2021, official translation)*[20], *Critical Information Infrastructure Security Protection Regulations (2021, unofficial translation)*[21], *Cybersecurity Law (2016, unofficial translation)*[22], *Criminal Law (1997, official translation)*[23], *and 2020 amendment, (unofficial translation)*[24]

Mandate: The MPS is responsible for domestic policing and security, and responds to suspected cybercrime activities. More specifically in the digital realm, it is responsible for the Multi-Level Protection System that imposes differentiated security requirements and compliance thresholds on network operators depending on the degree of importance of their systems. This system encompasses critical information infrastructure protection and is connected to the data-security protection regime. The MPS has a substantive administrative enforcement role, in coordination with other line ministries.

Major Reports, Inquiries, and Related Initiatives:

- Guiding Opinions on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System (2020): [Report] (In Chinese) [Report] (Unofficial Translation)[25]

Ministry of Commerce (MOFCOM)

Institutional Form: Ministry

Responsible Minister: The Minister of the Ministry of Commerce

Principal Instrument(s): *Anti-Foreign Sanctions Law (2021, unofficial translation)*[26]*, Export Control Law (2020, official translation)*[27]*, Foreign Investment Law (2019, official translation)*[28]*, National Security Law (2015, official translation)*[29]*, Foreign Trade Law (2004, official translation)*[30]

Mandate: The MOFCOM is responsible for foreign trade, import and export regulation and foreign direct investment, as well as bilateral and multilateral economic cooperation. It has oversight responsibility for regulating foreign investment and the fledgling Chinese export control regime. The MOFCOM is the primary entity in charge of the Unreliable Entity List, a newly established, and at the time of writing never-used tool for retaliating against companies deemed to boycott China for non-commercial purposes. The MOFCOM plays an important role in China's new anti-foreign sanctions regime.

Major Reports, Inquiries, and Related Initiatives:

- Guiding Opinions concerning the Establishment of Internal Compliance Mechanisms for Export Operators of Dual-Use Goods (2021): [Report] (In Chinese)[31]

State Administration of Market Regulation (SAMR)

Institutional Form: Ministry-level entity under the State Council

Responsible Minister: The Director of the SAMR

Principal Instrument(s): *E-Commerce Law (2018, unofficial translation)*[32]*, Anti-Monopoly Law (2007, official translation)*[33]*, Consumer Protection Law (1993, official translation)*[34]

Mandate: The SAMR regulates consumer markets as well as the licensing of corporate entities for overall market access. Sector-specific licensing may be necessary for specific activities. In the digital realm, it has primary responsibility for consumer protection and competition regulation. It also oversees China's intellectual property regulator.

Major Reports, Inquiries, and Related Initiatives:

- Guiding Opinions concerning Implementing the Dominant Responsibility of Online Food and Beverage Platforms and Realistically Ensuring the Rights and Interests of Delivery Personnel (Jointly with CAC, MPS, MOFCOM) (2021): [Report] (In Chinese)[35]
- Guiding Opinions concerning Strengthening Online Direct Marketing Activity Oversight (2020): [Report] (In Chinese)[36]
- Implementation Opinions concerning Launching Commercial Encryption Monitoring and Certification Work (Jointly with SCA) (2020): [Report] (In Chinese)[37]

China Banking and Insurance Regulatory Commission (CBIRC)

Institutional Form: Ministry-level entity under the State Council

Responsible Minister: The Director of the CBIRC

Principal Instrument(s): *Law on Commercial Banks (2003, official translation)*[38]*, Law on the Regulation of and Supervision over the Banking Industry (2006, official translation)*[39]

Mandate: The CBIRC is the regulator of banking and insurance services in China. It regulates the elements of FinTech related to online banking, lending, and insurance services, as well as online payments. It works together with the People's Bank of China.

Major Reports, Inquiries, and Related Initiatives: Refer to People's Bank of China for relevant materials.

China Securities Regulatory Commission (CSRC)

Institutional Form: Ministry-level entity under the State Council

Responsible Minister: The Director of the CSRC

Principal Instrument(s): *Securities Law (2019, official translation)*[40]*, Securities Investment Fund Law (2012, official translation)*[41]

Mandate: The CSRC administers the stock market listings of Chinese companies domestically and internationally. It has played a major role in recent moves to limit the foreign listings of fintech companies, for example, Ant Group, as well as Chinese platform companies holding significant amounts of personal information and important data, for example, Didi. The CSRC also plays a role in monitoring and regulating foreign investments in China.

Major Reports, Inquiries, and Related Initiatives: Refer to People's Bank of China for relevant materials.

People's Bank of China (PBoC)

Institutional Form: Central Bank

Responsible Minister: The Governor of the People's Bank of China

Principal Instrument(s): *Credit Reporting Industry Regulations (2013, official regulations)*[42], *Law on the Regulation of and Supervision over the Banking Industry (2006, official translation)*[43]

Mandate: The PBoC is China's central bank and has authority over China's monetary system, including the ongoing trials of a Central Bank Digital Currency (under development). PBoC issues licences to lenders who fall under the supervision of CBIRC and SAMR. It issues ratings to consumer finance companies and is in charge of the credit reporting industry.

Major Reports, Inquiries, and Related Initiatives:

- Fintech Development Plan (2022–25) (2021): [Report] (In Chinese)[44]
- Progress of Research and Development of E-CNY in China (2021): [Report] (Official translation)[45]
- Opinions concerning Standardising Open-Source Technology Application and Development in the Financial Sector (Jointly with CAC, MIIT, CBIRC and CSRC) (2021): [Report] (In Chinese)[46]
- Fintech Development Plan (2019–21) (2019): [Report] (In Chinese)[47]

*National Information Security Standardization Technical Committee/ Technical Committee 260 (TC260)

Institutional Form: Standardisation body subordinate to the CAC

Responsible Minister: The Director of the CAC

Principal Instrument(s): *Guidelines for the Construction of the Online Data Security Standards System (2020, unofficial translation)*[48], *Standardization Law (2017, unofficial translation)*[49], *Cybersecurity Law (2016, unofficial translation)*[50]

Mandate: TC260 is a technical committee subordinate to the CAC. Its presidency is held by the Chief Engineer of CAC and its membership consists of representatives from expert bodies and knowledge institutions as well as domestic and international companies (although the latter are not permitted to join specific working groups working on classified information). The TC260 formulates standards that are mostly voluntary, although they do serve as accepted best practices and companies need to demonstrate, in enforcement or court cases, why they have deviated from the standards. TC260 standards can also be mandatory, for example, through inclusion in regulations.

Major Reports, Inquiries, and Related Initiatives:

- 5G Cybersecurity Standardization (2021): [White Paper] (In Chinese)[51]
- Cybersecurity State Sensing Technology Standardization (2020): [White Paper] (In Chinese)[52]
- Artificial Intelligence Security Standardization (2019): [White Paper] (In Chinese)[53]
- Internet of Things Cybersecurity Standardization (2019): [White Paper] (In Chinese)[54]

China National Intellectual Property Administration (CNIPA)

Institutional Form: Administrative body subordinate to the SAMR

Responsible Minister: The Director of the SAMR

Principal Instrument(s): *Patent Law (2020, unofficial translation)*[55], *Trademark Law (2001, official translation)*[56]

Mandate: The CNIPA performs dual roles in China's intellectual property system. It functions as the Chinese patent office and reviews applications, issues patents and has responsibility for enforcement. It is also in charge of the administration of trade marks.

Major Reports, Inquiries, and Related Initiatives:

- Guiding Opinions concerning Further Strengthening Foreign Intellectual Property Dispute Response Mechanisms (2021): [Report] (In Chinese)[57]
- Opinions concerning Strengthening Intellectual Property Dispute Mediation Work (2021): [Report] (In Chinese)[58]
- Opinions concerning Strengthening Cooperation and Coordination in Strengthening Intellectual Property Protection (Jointly with MPS) (2021): [Report] (In Chinese)[59]

State Cryptography Administration (SCA)

Institutional Form: Administrative body subordinate to the State Council

Responsible Minister: The Director of the SCA

Principal Instrument(s): *Cryptography Law (2019, official translation)*[60]

Mandate: The SCA is responsible for cryptography regulation, including technical standards. It supports cryptography research and developments, evaluation, and certification and assists law enforcement bodies in investigations involving cryptographic leaks or cryptography-related technical expertise. The SCA coordinates the education and training of cryptography professionals.

Major Reports, Inquiries, and Related Initiatives: Refer to State Administration of Market Regulation (SAMR).

National Health Commission (NHC)

Institutional Form: Ministry-level body subordinate to the State Council

Responsible Minister: The Director of the NHC

Principal Instrument(s): *Regulation for Medical Device Administration and Supervision (2021, unofficial translation)*[61], *Personal Information Protection Law (2021, official translation)*[62], *Data Security Law (2021, unofficial translation)*[63], *Basic Medical, Healthcare and Health Promotion Law (2019, official translation)*[64], *Cybersecurity Law (2016, unofficial translation)*[65]

Mandate: The NHC is responsible for public health, disease control and prevention as well as the administration of healthcare institutions and professionals. It regulates digital medical devices as well as the collection and use of personal information. The NHC oversees medical research and is responsible for managing data-security-related aspects of drug, device, and treatment development. The NHC conducts trials to develop digitised long-distance healthcare services.

Major Reports, Inquiries, and Related Initiatives:

- Guiding Opinions concerning Advancing the Secure and Orderly Management of Hospitals (Jointly with CAC and MPS) (2021): [Report] (In Chinese)[66]
- Guiding Opinions concerning Accelerating the Advance of Electronic Certification Building and Application in the Healthcare Sector (2020): [Report] (In Chinese)[67]

Ongoing Parliamentary Committees, Inquiries, or Legislative Proposals (not previously referred to):

- State Council General Office Guiding Opinions concerning Further Perfecting Restraint Structures for Trust-Breaking and Building Long-Term Mechanisms for Sincerity Building(2021): [Report] (In Chinese)[68]
- State Council General Office Guiding Opinions concerning Accelerating the Advance of Social Credit System Construction and Building Credit-Based Novel Oversight Mechanisms (2021): [Report] (In Chinese)[69]

Endnotes (China)

1. Central Commission for Cybersecurity and Informatization 2021, *14th Five-Year Plan for National Informatization* (In Chinese), accessed 29 March 2022, www.gov.cn/xinwen/2021-12/28/5664873/files/1760823a103e4d75ac681564fe481af4.pdf. For an unofficial translation, see: Creemers, R, Dorwart, H, Neville, K, Schaefer, K, Costigan, J & Webster, G 2022, *Translation: 14th Five-Year Plan for National Informatization – Dec. 2021*, DIGI China, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

2. Digi China 2021, *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.

3. *Personal Information Protection Law of the People's Republic of China*, Stanford University, accessed 29 March 2022, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

4. Creemers R, Webster, G & Triolo, P 2018, *Cybersecurity Law of the People's Republic of China*, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

5. Creemers, R 2014, *Notice concerning Empowering the Cyberspace Administration of China to Be Responsible for Internet Information Content Management Work*, China Copyright and Media, accessed 29 March 2022, https://chinacopyrightandmedia.wordpress.com/2014/08/26/notice-concerning-empowering-the-cyberspace-administration-of-china-to-be-responsible-for-internet-information-content-management-work/.

6. Cyberspace Administration of China 2021, *14th Five-Year Plan for the Development of the Digital Economy* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm.

7. Cyberspace Administration of China 2021, *14th Five-Year Plan for Advancing National Governmental Informatization* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/zhengceku/2022-01/06/content_5666746.htm.

8. Cyberspace Administration of China 2021, *Some Opinions concerning Promoting the Health and Orderly Development of the Platform Economy (Jointly with SAMR, MIIT, MOFCOM, PBoC and STA)* (In Chinese), accessed 29 March 2022, www.ndrc.gov.cn/xxgk/zcfb/tz/202201/t20220119_1312326.html.

9. Cyberspace Administration of China 2021, *Guiding Opinions on Strengthening the Comprehensive Governance of Network Information Service Algorithms (Jointly with MIIT, MPS, SAMR)* (In Chinese), accessed 29 March 2022, www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1779/202109/t20210929_568182.html. For an unofficial translation, see Tai, K, Creemers, R, Laskai, L & Webster, G 2021, *Translation: Guiding Opinions on Strengthening Overall Governance of Internet Information Service Algorithms*, DIGI China, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-guiding-opinions-on-strengthening-overall-governance-of-internet-information-service-algorithms/.

10. Cyberspace Administration of China 2021, *Guiding Opinions concerning Strengthening Standardized Management Work of Live Streaming (Jointly with MIIT, MPS, SAMR)* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/zhengceku/2021-02/10/content_5586472.htm.

11. Cyberspace Administration of China 2021, *Opinions concerning Further Consolidating the Dominant Responsibility of Platform Companies for Information Content Management* (In Chinese), accessed 29 March 2022, www.cac.gov.cn/2021-09/15/c_1633296789845827.htm.

12. Creemers, R, Webster, G & Triolo, P 2018, *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

13. *Telecommunications Regulations of the People's Republic of China,* accessed 29 March 2022, www.china.org.cn/business/laws_regulations/2010-01/20/content_19273945.htm.

14. Ministry of Industry and Information Technology 2021, *Guiding Opinions concerning Accelerating the Promotion of the Application and Industrial Development of Blockchain Technologies (Jointly with CAC)* (In Chinese), accessed 29 March 2022, www.cac.gov.cn/2021-06/07/c_1624629407537785.htm.

15. Ministry of Industry and Information Technology 2021, *Big Data: White Paper* (In Chinese), accessed 29 March 2022, www.caict.ac.cn/english/research/whitepapers/202112/P020211228472393829284.pdf.

16. Ministry of Industry and Information Technology 2021, *Internet Law and Regulation: White Paper* (In Chinese), accessed 29 March 2022, www.caict.ac.cn/english/research/whitepapers/202112/t20211228_394731.html.

17. Ministry of Industry and Information Technology 2021, *Blockchain: White Paper* (In Chinese), accessed 29 March 2022, www.caict.ac.cn/english/research/whitepapers/202112/t20211228_394676.html.

18. Ministry of Industry and Information Technology 2021, *Fintech: White Paper* (In Chinese), accessed 29 March 2022, www.caict.ac.cn/english/research/whitepapers/202112/t20211224_394512.html.

19. Digi China 2021, *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.

20. *Personal Information Protection Law of the People's Republic of China*, accessed 29 March 2022, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

21. Creemers, R, Sacks, S & Webster, G 2021, *Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)*, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/.

22. Creemers, R, Webster, G & Triolo, P 2018, *Cybersecurity Law of the People's Republic of China*, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

23. Permanent Mission of the People's Republic of China to the United Nations and Other International Organizations in Vienna 1997, *Criminal Law of the People's Republic of China*, accessed 29 March 2022, www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm.

24. *P.R.C. Criminal Law Amendment 11*, accessed 29 March 2022, www.chinalawtranslate.com/en/criminal-law-amendment-11/.

25. Ministry of Public Security 2020, *Guiding Opinions on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System* (In Chinese), accessed 29 March 2022, http://gaj.cq.gov.cn/zslm_245/fzgl/gafg/202106/t20210623_9421169.html. For an unofficial translation, see Wang An, G 2020, *Guiding Opinions on Implementing the Cybersecurity Multi-Level Protection System and Critical Information Infrastructure Security Protection System*, China Copyright and Media, accessed 29 March 2022, https://chinacopyrightandmedia.wordpress.com/2020/07/22/guiding-opinions-on-implementing-the-cybersecurity-multi-level-protection-system-and-critical-information-infrastructure-security-protection-system/.

26. *Law of the PRC on Countering Foreign Sanctions*, accessed 29 March 2022, www.chinalawtranslate.com/en/counteringforeignsanctions/.

27. *Export Control Law of the People's Republic of China,* accessed 29 March 2022, www.npc.gov.cn/englishnpc/c23934/202112/63aff482fece44a591b45810fa2c25c4.shtml.

28. *Foreign Investment Law of the People's Republic of China*, accessed 29 March 2022, https://en.ndrc.gov.cn/policies/202105/t20210527_1281403.html.

29. *National Security Law of the People's Republic of China (2015)*, accessed 29 March 2022, https://govt.chinadaily.com.cn/s/201812/11/WS5c0f1b56498eefb3fe46e8c9/national-security-law-of-the-peoples-republic-of-china-2015-effective.html.

30. *Foreign Trade Law of The People's Republic of China*, accessed 29 March 2022, http://english.mofcom.gov.cn/article/policyrelease/Businessregulations/201303/20130300045871.shtml.

31. Ministry of Commerce 2021, *Guiding Opinions concerning the Establishment of Internal Compliance Mechanisms for Export Operators of Dual-Use Goods* (In Chinese), accessed 29 March 2022, www.mofcom.gov.cn/article/zwgk/zcfb/202104/20210403056267.shtml.

32. *E-Commerce Law of the People's Republic of China,* European Union Intellectual Property Office, accessed 29 March 2022, https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf.

33. *Anti-monopoly Law of the People's Republic of China*, 29 April 2022, http://english.mofcom.gov.cn/article/policyrelease/Businessregulations/201303/20130300045909.shtml.

34. *Law of the People's Republic of China on the Protection of Consumer Rights and Interests*, accessed 29 March 2022, www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/12/content_1383812.htm.

35. State Administration of Market Regulation 2021, *Guiding Opinions concerning Implementing the Dominant Responsibility of Online Food and Beverage Platforms and Realistically Ensuring the Rights and Interests of Delivery Personnel (Jointly with CAC, MPS, MOFCOM)* (In Chinese), accessed 29 March 2022, www.laodongfa.com/LaborLaw/info.aspx?itemid=8406.

36. State Administration of Market Regulation (SAMR) 2020, *Guiding Opinions concerning Strengthening Online Direct Marketing Activity Oversight* (In Chinese), accessed 29 March 2022, https://gkml.samr.gov.cn/nsjg/ggjgs/202011/t20201106_323092.html.

37. State Administration of Market Regulation 2020, *Implementation Opinions concerning Launching Commercial Encryption Monitoring and Certification Work (Jointly with SCA)* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/zhengceku/2020-04/01/content_5497919.htm.

38. *Law of the People's Republic of China on Commercial Banks,* accessed 29 March 2022, www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/12/content_1383716.htm.

39. *Law of the People's Republic of China on Regulation of and Supervision over the Banking Industry*, accessed 29 March 2022,www.china.org.cn/english/DAT/214819.htm.

40. *Securities Law of the People's Republic of China*, accessed 29 March 2022, www.npc.gov.cn/englishnpc/c23934/202109/9886ca6f805e4663a9a725d6f72066dd.shtml.

41. *Securities Investment Fund Law of the People's Republic of China*, accessed 29 March 2022, http://english.www.gov.cn/services/investment/2014/08/23/content_281474982978075.htm.

42. Credit Reference Center, People's Bank of China 2013, *Regulation on Credit Reporting Industry*, accessed 29 March 2022, www.pbccrc.org.cn/crc/jgyhfw/201309/1ca0f775b50744cabaf83538288d77a9/files/e8a8bf080ed64f48914a652da1d8fdc3.pdf.

43. *Law of the People's Republic of China on Regulation of and Supervision over the Banking Industry*, accessed 29 March 2022, www.china.org.cn/english/DAT/214819.htm.

44. People's Bank of China 2021, *Fintech Development Plan (2022-2025)* (In Chinese), accessed 29 March 2022, www.jinronghu.com/news/36310.html.

45. People's Bank of China 2021, *Progress of Research and Development of E-CNY in China* (Official translation), accessed 29 March 2022, www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf.

46. People's Bank of China 2021, *Opinions concerning Standardising Open-Source Technology Application and Development in the Financial Sector (Jointly with CAC, MIIT, CBIRC and CSRC)* (In Chinese), accessed 29 March 2022, www.pbc.gov.cn/zhengwugongkai/4081330/4081344/4081395/4081686/4364505/index.html.

47. People's Bank of China 2019, *Fintech Development Plan (2019-2021)* (In Chinese), accessed 29 March 2022, www.fintechtimes.com.cn/imagez/fintech-2019-2021.pdf.

48. Creemers R 2020, *Guidelines for the Construction of the Online Data Security Standards System*, China Copyright and Media, https://chinacopyrightandmedia.wordpress.com/2020/04/10/guidelines-for-the-construction-of-the-online-data-security-standards-system/.

49. *Standardization Law of People's Republic of China (4 November 2017)*, accessed 29 March 2022, www.sesec.eu/app/uploads/2018/01/Annex-I-China-Stadnardization-Law-20171104.pdf.

50. Creemers, R, Webster, G & Triolo, P 2018, *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

51. National Information Security Standardization Technical Committee/Technical Committee 260 2021, *5G Cybersecurity Standardization: White Paper* (In Chinese), accessed 29 March 2022, www.tc260.org.cn/upload/2020-11-09/1604914831845079890.pdf.

52. National Information Security Standardization Technical Committee/Technical Committee 260 2020, *Cybersecurity State Sensing Technology Standardization: White Paper* (In Chinese), accessed 29 March 2022, www.tc260.org.cn/file/5gwlaq.pdf.

53. National Information Security Standardization Technical Committee/Technical Committee 260 2019, *Artificial intelligence Security Standardization: White Paper* (In Chinese), accessed 29 March 2022, www.tc260.org.cn/file/rgznaqbz.pdf.

54. National Information Security Standardization Technical Committee/Technical Committee 260 2019, *Internet of Things Cybersecurity Standardization: White Paper* (In Chinese), accessed 29 March 2022, www.tc260.org.cn/file/wlwaqbz.pdf.

55. *Patent Law of the People's Republic of China*, China Patents & Trademarks No. 1, accessed 29 March 2022, www.cpahkltd.com/UploadFiles/20201222110401200.pdf.

56. *Trademark Law of the People's Republic of China*, accessed 29 March 2022, www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/13/content_1384018.htm.

57. China National Intellectual Property Administration 2021, *Guiding Opinions concerning Further Strengthening Foreign Intellectual Property Dispute Response Mechanisms* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/zhengceku/2021-12/04/content_5655845.htm.

58. China National Intellectual Property Administration 2021, *Opinions concerning Strengthening Intellectual Property Dispute Mediation Work* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/zhengceku/2021-10/29/content_5647702.htm.

59. China National Intellectual Property Administration 2021, *Opinions concerning Strengthening Cooperation and Coordination in Strengthening Intellectual Property Protection (Jointly with MPS)* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/zhengceku/2021-05/24/content_5611192.htm.

60. *Cryptography Law of the People's Republic of China*, accessed 29 March 2022, www.npc.gov.cn/englishnpc/c23934/202009/dfb74a30d80b4a2bb5c19678b89a4a14.shtml.

61. *Regulations on the Supervision and Administration of Medical Devices,* accessed 29 March 2022, www.easychinapprov.com/ordinance-739-nmpa.

62. *Personal Information Protection Law of the People's Republic of China*, accessed 29 March 2022, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm.

63. Digi China 2021, *Translation: Data Security Law of the People's Republic of China* (Effective Sept. 1, 2021), Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.

64. *Law of the People's Republic of China on Basic Medical and Health Care and the Promotion of Health*, accessed 29 March 2022, www.npc.gov.cn/englishnpc/c23934/202012/0e545b3ed6544a-4fa93a1bb2feb13b3a.shtml.

65. Creemers, R, Webster, G & Triolo, P 2018, *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, Stanford University, accessed 29 March 2022, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

66. National Health Commission 2021, *Guiding Opinions concerning Advancing the Secure and Orderly Management of Hospitals (Jointly with CAC and MPS)* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/zhengceku/2021-09/28/content_5639773.htm.

67. National Health Commission 2020, *Guiding Opinions concerning Accelerating the Advance of Electronic Certification Building and Application in the Healthcare Sector* (In Chinese), accessed 29 March 2022, www.nhc.gov.cn/guihuaxxs/gongwen12/202010/64d370e60e6647709d847300fec16abe.shtml.

68. State Council General Office 2021, *Guiding Opinions concerning Further Perfecting Restraint Structures for Trust-Breaking and Building Long-Term Mechanisms for Sincerity Building* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/content/2020-12/18/content_5570954.htm.

69. State Council General Office 2021, *Guiding Opinions concerning Accelerating the Advance of Social Credit System Construction and Building Credit-Based Novel Oversight Mechanisms* (In Chinese), accessed 29 March 2022, www.gov.cn/zhengce/content/2019-07/16/content_5410120.htm.

Estonia

Kadri Kaska, e-Governance Academy, and Elsa Neeme, NATO Cooperative Cyber Defence Centre of Excellence

Bank of Estonia (Eesti Pank)

Institutional Form: Constitutional body

Responsible Minister: Not applicable

Principal Instrument(s): *Credit Institutions Act (1999), Bank of Estonia (Eesti Pank) Act (1993)*

Mandate: As the central bank of the Republic of Estonia and a member of the Eurosystem, the primary aim of the Bank of Estonia is to maintain price stability. It is tasked with supporting other economic policy objectives (co-)defining and implementing European Union monetary policy, holding and managing foreign currency reserves, and promoting the stability of the financial system. Its role as a technology regulator relates to promoting the efficient operation of digital payment systems and exercising oversight. The Bank of Estonia issues technical requirements for the electronic submission of reports to itself and the Financial Supervision Authority, including digital data exchange requirements. It also establishes continuity requirements of payment services and cash circulation in case of emergencies.

Major Reports, Inquiries, and Related Initiatives:

- Joint report into the technical possibilities for a digital euro. A New Solution – Blockchain & eID (2021): [Report][1]

Consumer Protection and Technical Regulatory Authority (Tarbijakaitse ja Tehnilise Järelevalve Amet) (TTJA)

Institutional Form: Government authority*

Responsible Minister: The Minister of Economic Affairs and Communications

Principal Instrument(s): *Media Services Act (2019), Consumer Protection Act (2015), Estonian Public Broadcasting Act (2007), Electronic Communications Act (2004), Information Society Services Act (2004), Public Information Act (2000)*

Mandate: The TTJA is responsible for safety regulation, market regulation, and compliance with legal obligations in a broad range of areas. These include electronic communications and broadcasting, spectrum management, media services and consumer rights. It oversees and guides the implementation of the abovementioned legal acts, exercises supervision over market players, and can issue administrative acts and apply coercive measures. The TTJA oversees crime prevention and conducts misdemeanour proceedings as an extrajudicial body in cases provided by law. Its administrative acts in specific cases are binding for the addressees. The reports and guidance it issues are non-binding *per se*, although compliance is considered as adequate implementation of legal requirements. The TTJA imposes access and cost obligations on network and service providers with significant market power and authorises roaming surcharges and resolves disputes regarding high-speed communication networks.

Major Reports, Inquiries, and Related Initiatives:

- Guide for e-Commerce Entrepreneurs (2021): [Report] (In Estonian)[2]
- Elimination of unjustified location restrictions or geo-blocking (2021): [Report] (In Estonian)[3]
- Guide for telecommunications operators: unilateral amendment of the terms of a telecommunications service contract (2021): [Report] (In Estonian)[4]
- E-commerce market in Estonia and website compliance with legal requirements (2019): [Report Summary] (In Estonian)[5]

* Estonia has 2 kinds of authorities of executive power: *governmental authorities*, whose main function assigned by law or pursuant to law, is to exercise executive power and *state authorities administered by governmental authorities* with no executive powers but providing services to government authorities or that perform assigned functions in cultural, educational, social, or other areas. All tech regulators in Estonia fall to the first category, i.e., of government authorities.

Data Protection Inspectorate (Andmekaitse Inspektsiooni) (AKI)

Institutional Form: Government authority

Responsible Minister: The Minister of Justice

Principal Instrument(s): *Personal Data Protection Act (2018), EU General Data Protection Regulation Directive (GDPR) (2016), Public Information Act (2000)*

Mandate: The AKI exercises state and administrative supervision over compliance with the requirements of the *Personal Data Protection Act* and *Public Information Act* as well as with the European Union's GDPR. It can issue advice, opinions and recommendations to the public, controllers, and processors of personal data. The AKI enforces compliance with privacy law requirements, initiates misdemeanour proceedings and imposes sanctions in case of breaches. It can demand rectification or erasure of personal data and restrictions on, or termination of processing of, personal data. It has the right to immediately apply security measures to protect personal data provided for in the *Substitutional Performance and Non-Compliance Levies Act*. The AKI may initiate supervision proceedings in response to a complaint or on its own initiative. It also has a key role in the management of the national information system.

Major Reports, Inquiries, and Related Initiatives:

- Annual Report 2020: Compliance with the Public Information Act and Ensuring the Protection of Personal Data (2020): [Report][6]
- Legitimate interest (2020): [Guidelines] (In Estonian)[7]
- General Guidelines for Personal Data Processing (2019): [Guidelines] (In Estonian)[8]
- Cross-border DPIA list (2019): [Guidelines][9]

Estonian Competition Authority (Konkurentsiamet)

Institutional Form: Government authority

Responsible Minister: The Minister of Justice

Principal Instrument(s): *Electronic Communications Act (2004), Competition Act (2001)*

Mandate: The Competition Authority oversees competition and control of market concentrations. It promotes competition, conducts analyses and makes recommendations to improve competitiveness and makes proposals for legislation to be passed or amended. The Consumer Protection and Technical Regulatory Authority, in regulating competition in the telecommunications market, consults with the Competition Authority on spectrum assignment, licensing and competition analysis to apply the competition law in a consistent manner. Due to the Consumer Protection and Technical Regulatory Authority holding the weight of telecommunications market competition, inquiries and action by the Competition Authority in the area have been scarce.

Major Reports, Inquiries, and Related Initiatives:

- Assessment of market situation in telecommunications markets (2021): [Report] (In Estonian)[10]
- Opinion about granting 5G frequency licenses (2019): [Report][11]

Estonian Tax and Customs Board (Maksu-ja Tolliamet) (EMTA)

Institutional Form: Government authority

Responsible Minister: The Minister of Finance

Principal Instrument(s): *Customs Act (2017), Value-Added Tax Act (2003), Taxation Act (2002), Social Tax Act (2000), Income Tax Act (1999)*

Mandate: The EMTA administers state revenues, implements national tax and customs policy, ensures compliance with trade and customs legislation, and implements tax laws, customs rules and related legislation. The EMTA was an early adopter of e-government services and has introduced automated tax reporting for natural and legal persons, has automated the issuing of tax decisions and uses a digital tariff system. The digital tax reporting and processing requirements are defined in the Regulation No. 15 of 14 March 2019 of the Minister of Finance concerning digital handling in the e-tax environment, which the EMTA administers.

Major Reports, Inquiries, and Related Initiatives:

- Technical information for developers and technical specifications for tax and customs systems (2022): [Guidelines] (In Estonian)[12]
- Electronic administration in the Tax and Customs Board e-service environment, Regulation No. 15 of 14 March 2019 of the Minister of Finance (2019): [Regulation] (In Estonian)[13]

Financial Intelligence Unit (Rahapesu Andmebüroo) (RAB)

Institutional Form: Government authority

Responsible Minister: The Minister of Finance

Principal Instrument(s): *Money Laundering and Terrorist Financing Prevention Act (2017)*

Mandate: The RAB is responsible for the prevention of money laundering and terrorist financing. Its tasks include strategic analysis and supervision of compliance, with appropriate enforcement powers, including virtual currency services. The RAB may revoke a financial service provider's activity licence in cases of non-compliance. The RAB strategy for 2022-2026 upgrades the unit into a financial risk analysis and risk management centre, including the further implementation of its intelligent digital solutions.

Major Reports, Inquiries, and Related Initiatives:

- Risks Related to Virtual Asset Service Providers in Estonia (2022): [Report][14]
- Survey of Service Providers of Virtual Currency (2020): [Report][15]

Financial Supervision Authority (Finantsinspektsioon) (FI)

Institutional Form: Autonomous supervisory authority

Responsible Minister: The Minister of Finance of the Republic of Estonia

Principal Instrument(s): *Money Laundering and Terrorist Financing Prevention Act (2017), Insurance Activities Act (2015), Payment Institutions and E-money Institutions Act (2009), Financial Supervision Authority Act (2001), Securities Market Act (2001), Credit Institutions Act (1999)*

Mandate: The FI is a financial supervision and crisis resolution authority with independent decision-making capacity. It is responsible as a supervisory institution for crisis preparedness and crisis management in Estonia's financial sector, preventing threats to financial stability, protecting funds, and ensuring the uninterrupted functioning of credit institutions. It has oversight of the implementation of identification requirements and data verification procedure using ICT means, established by a regulation of 26 October 2017 from the Minister of Finance.[16] The FI is part of the European Single Supervisory Mechanism. It does not exercise oversight over virtual currency providers.

Major Reports, Inquiries, and Related Initiatives:

- Supervision policy for facilitating an innovative financial sector (2021): [Report] (In Estonian)[17]
- Barriers to innovation (2021): [Report] (In Estonian)[18]
- Requirements for the organisation of information technology and information security of the subject of financial supervision (2020): [Guidelines] (In Estonian)[19]
- Memorandum to the representatives of payment agencies on the implementation of secure authentication (2020): [Memorandum] (In Estonian)[20]

Information System Authority (Riigi Infosüsteemi Amet) (RIA)

Institutional Form: Government agency

Responsible Minister: The Minister of Economic Affairs and Communications

Principal Instrument(s): *Cybersecurity Act (2018), Emergency Act (2017), Electronic Identification and Trust Services for Electronic Transactions Act (2016), Electronic Communications Act (2004), Public Information Act (2000), Identity Documents Act (1999)*

Mandate: The RIA coordinates the development and administration of Estonia's digital infrastructure to provide interoperability of the national information system. It regulates cyber security and handles security incidents in computer networks. It regulates the national information system (national digital identity, election information systems and the national secure data exchange backbone), manages the cyber security protection of critical information infrastructure and defines the system of security measures for government information systems. The RIA is responsible for national cyber emergency preparedness and is the lead authority in cyber crisis resolution with a specific crisis mandate. In 2022, the RIA published the National Cybersecurity Standard (E-ITS) for central and local governments as well as for essential service providers. A legislative amendment submitted to the Parliament in February 2022 proposes mandatory implementation of the E-ITS standard (or its equivalent).

Major Reports, Inquiries, and Related Initiatives:

- Estonian Cybersecurity Standard (E-ITS) (2022): [E-ITS Webpage] (In Estonian)[21]
- Annual Cybersecurity Assessment 2022 (2022): [Report] (In Estonian; English translation forthcoming)[22]
- Code Repository documentation (2020): [General Terms] [Data Protection Requirements] [User Guidelines] (In Estonian)[23]
- X-Road Guidelines (2020): [X-Road Portal] (in Estonian)[24]
- sahver.eesti.ee public file repository documentation (2020): [General Terms] [Data Protection Requirements] [Guidelines] (In Estonian)[25]
- Mobile voting feasibility study and risk analysis (2020): [Report][26]
- Guidelines for enterprise cybersecurity (2019): [Guidelines] (in Estonian)[27]

Ministry of Economic Affairs and Communications (Majandus-ja Kommunikatsiooniministeerium) (MKM)

Institutional Form: Government department

Responsible Minister: The Minister of Entrepreneurship and Information Technology

Principal Instrument(s): *Media Services Act (2010), Electronic Communications Act (2004), Government of the Republic Act (1995)*

Mandate: The MKM oversees economic competitiveness and creates and implements policy for balanced and sustainable development. The MKM also oversees the management, organisation and supervision of public sector digital development and national cyber security. It is responsible for the organisation of crisis management and essential service continuity. It has a joint role in radio spectrum management with the Consumer Protection and Technical Regulatory Authority and decides on licence terms for free access television and radio service licenses. The MKM plays a lead role in national 5G risk assessment, defining security requirements (adopted by the Government in December 2021) and managing the tender for 3410–3800 MHz 5G spectrum from January 2022.

Major Reports, Inquiries, and Related Initiatives:

- Analysis of the legal framework pertaining to the provision and use of governmental cloud services (2021): [Report] (In Estonian)[28]
- Analysis on granting access to Estonia's public sector digital services for individuals holding EU e-authentication devices (2021): [Report] (In Estonian)[29]
- 5G Use Case Study (2021): [Summary][30]

The Estonian Patent Office (Patendiamet)

Institutional Form: Government authority

Responsible Minister: The Ministry of Justice

Principal Instrument(s): *Principles of Legal Regulation of Industrial Property Act (2003), Trade Marks Act (2002), Industrial Design Protection Act (1997), Patents Act (1994), Utility Models Act (1994), Copyright Act (1992)*

Mandate: The Estonian Patent Office administers legal protection of intellectual property as well as copyright and related rights. It provides legal protections for patents, trade marks, utility models, industrial designs, geographical indications and integrated circuits. The Patent Office resolves out-of-court disputes concerning the legal protection of intellectual property and implements copyright and related rights. It also arranges international cooperation for the legal protection of industrial property proceeding from international agreements and participates in international institutions dealing with the legal protection of industrial property. It oversees compliance with the operation of collective rights management organisations under the *Copyright Act*. The Patent Office is the competent authority in Estonia for exchanging information regarding so-called orphan works. It develops and operates digital information systems, including the registers for patents, utility models, trade and service marks, industrial designs, and others.

Major Reports, Inquiries, and Related Initiatives:

- Guidelines for processing patent applications and patents (2020): [Guidelines] (In Estonian)[31]

Statistics Estonia (Statistikaamet)

Institutional Form: Government authority

Responsible Minister: The Minister of Finance

Principal Instrument(s): *Official Statistics Act (2010), Public Information Act (2000)*

Mandate: Statistics Estonia produces official statistics, provides data-sharing services and exercises state and administrative supervision under the *Official Statistics Act (2010)*. It is also responsible for coordinating the system of classifications and for data governance and exercises administrative supervision over compliance with data governance requirements. It does not duplicate tasks of other public agencies in digital society development, information society services, the state information system, the protection of personal data, or ensuring cybersecurity. Statistics Estonia focuses on three data management requirements: maintaining an up-to-date and meaningful overview of the databases and datasets used in analyses and statistics; harmonising data descriptions so that data, including open data, can be found quickly, described once and in high quality; and monitoring and improving data quality so that users can quickly verify that the data is accurate, complete, and current. Statistics Estonia manages the classification system and monitors uniform classifications used in databases and information systems.

Major Reports, Inquiries, and Related Initiatives:

- Estonian Data Governance Action Plan (2018–22): [Action Plan] (In Estonian)[32]

Ongoing Parliamentary Committees, Inquiries, or Legislative Proposals (not previously referred to):

- Act Amending the Cybersecurity Act, Public Information Act and Estonian Public Broadcasting Act (531 SE): [Parliamentary Proceedings][33]
- Act Amending the Consumer Protection Act (424 SE): [Parliamentary Proceedings] (relating to consumer rights in online shopping)[34]
- Accessibility of Products and Services Act (511 SE): [Parliamentary Proceedings] (relating to accessibility of technologies for people with disabilities)[35]
- Act Amending the State Secrets and Classified Foreign Information Act and the Public Information Act (410 SE): [Parliamentary Proceedings] (relating to digital processing)[36]
- Draft legislation regulating the field of crowdfunding and crypto assets (2021): [Legislative Intent] (In Estonian)[37]
- Legislative intent on regulating virtual currencies (2019): [Legislative Intent][38]

Endnotes (Estonia)

1. Eesti Pank, Banco de España, Banca d'Italia, Deutsche Bundesbank, Latvijas Banka, De Nederlandsche Bank, Central Bank of Ireland, Bank of Greece & the European Central Bank 2021, *Work stream 3: A New Solution – Blockchain & eID,* Eesti Pank, accessed 29 March 2022, https://haldus.eestipank.ee/sites/default/files/2021-07/Work%20stream%203%20-%20A%20New%20Solution%20-%20Blockchain%20and%20eID_1.pdf.

2. Consumer Protection and Technical Regulatory Authority 2021, *Guide for e-Commerce Entrepreneurs* (In Estonian), accessed 29 March 2022, https://ttja.ee/media/309/download.

3. Consumer Protection and Technical Regulatory Authority 2021, *Elimination of unjustified location restrictions or geoblocking* (In Estonian), accessed 29 March 2022, https://ttja.ee/media/307/download.

4. Consumer Protection and Technical Regulatory Authority 2021, *Guide for telecommunications operators: unilateral amendment of the terms of a telecommunications service contract* (In Estonian), accessed 29 March 2022, https://ttja.ee/media/1128/download.

5. Consumer Protection and Technical Regulatory Authority 2019, *E-commerce market in Estonia and website compliance with legal requirements* (In Estonian), accessed 29 March 2022, https://ttja.ee/eraklient/ametist/lisainfo-ja-dokumendid/uuringud#e-kaubandus-2019.

6. Data Protection Inspectorate 2020, *Annual Report 2020: Compliance with the Public Information Act and Ensuring the Protection of Personal Data,* accessed 29 March 2022, www.aki.ee/sites/default/files/inglisekeelne%20aastaraamat/estonia_annualreport_2020.pdf.

7. Data Protection Inspectorate 2020, *Legitimate interest* (In Estonian), accessed 29 March 2022, www.aki.ee/sites/default/files/dokumendid/oigustatud_huvi_juhend_aki_26.05.2020.pdf.

8. Data Protection Inspectorate 2019, *General Guidelines for Personal Data Processing* (In Estonian), accessed 29 March 2022, www.aki.ee/sites/default/files/dokumendid/kaamerate_juhend_10.11.2021.pdf.

9. Data Protection Inspectorate 2019, *Cross-border DPIA list*, accessed 29 March 2022, www.aki.ee/en/guidelines-legislation/cross-border-dpia-list.

10. Estonian Competition Authority 2021, *Assessment of market situation in telecommunications markets* (In Estonian), accessed 29 March 2022, www.konkurentsiamet.ee/sites/default/files/Dokumentide-failid/konkurentsiameti_hinnang_eesti_telekommunikatsiooni_turust_0.pdf.

11. Estonian Competition Authority 2019, *Opinion about granting 5G frequency licences*, accessed 29 March 2022, www.konkurentsiamet.ee/en/competition-supervision-control-concentrations/competition-supervision/proposals-and-recommendations.

12. Estonian Tax and Customs Board 2022, *Technical information for developers and technical specifications for tax and customs systems* (In Estonian), accessed 29 March 2022, www.emta.ee/ariklient/e-teenused-koolitused/e-teenuste-kasutamine/tehniline-info-arendajale.

13. *Electronic administration in the Tax and Customs Board e-service environment, Regulation No. 15 of 14 March 2019 of the Minister of Finance* (In Estonian), accessed 29 March 2022, www.riigiteataja.ee/akt/123122021025?leiaKehtiv.

14. Financial Intelligence Unit 2022, *Risks Related to Virtual Asset Service Providers in Estonia*, accessed 29 March 2022, https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#the-risks-related-to.

15. Financial Intelligence Unit 2020, *Survey of Service Providers of Virtual Currency*, accessed 29 March 2022, https://fiu.ee/en/annual-reports-and-surveys-estonian-fiu/surveys#a-survey-of-service-.

16. Riigi Teataja 2021, *Infotehnoloogiliste vahendite abil isikusamasuse tuvastamise ja andmete kontrollimise tehnilised nõuded ja kord*, accessed 29 March 2022, www.riigiteataja.ee/akt/104122020009.

17. Financial Supervision Authority 2021, *Supervision policy for facilitating an innovative financial sector* (In Estonian), accessed 29 March 2022, www.fi.ee/et/juhendid/pangandus-ja-krediit/nouded-finantsjarelevalve-subjekti-infotehnoloogia-ja-infoturbe-korraldusele.

18. Financial Supervision Authority 2021, *Barriers to innovation* (In Estonian), accessed 29 March 2022, https://fi.ee/et/juhendid/makseteenused/margukiri-makseasutuste-esindajatele.

19. Financial Supervision Authority 2020, *Requirements for the organisation of information technology and information security of the subject of financial supervision* (In Estonian), accessed 29 March 2022, www.fi.ee/sites/default/files/2021-06/FI soovituslik juhend_Finantsinspektsiooni j%C3%A4relevalvepoliitika uuendusmeelse finantssektori soodustamiseks_KINNITATUD.pdf.

20. Financial Supervision Authority 2020, *Requirements for the organisation of information technology and information security of the subject of financial supervision* (In Estonian), accessed 29 March 2022, https://fi.ee/et/finantsinspektsioon/innovatsioonikeskus/innovatsioonitorked.

21. Information System Authority 2022, *Estonian Cybersecurity Standard (E-ITS)* (In Estonian), accessed 29 March 2022, https://eits.ria.ee/.

22. Information System Authority 2022, *Annual Cybersecurity Assessment 2022* (In Estonian), accessed 29 March 2022, www.ria.ee/sites/default/files/content-editors/kuberturve/ria_kyberturvalisuse_aastaraamat_2022_est_veeb.pdf.

23. Information System Authority 2020, *Code Repository documentation* (In Estonian), accessed 29 March 2022, (General Terms), www.ria.ee/sites/default/files/koodivaramu_uldtingimused.pdf, (Data protection requirements) www.ria.ee/sites/default/files/koodivaramu_teenuse_andmekaitsetingimused.pdf, (User guidelines) www.ria.ee/sites/default/files/sisselogimine_-_koodivaramu_muudetud.pdf.

24. Information System Authority 2020, *X-Road Guidelines* (In Estonian), accessed 29 March 2022, https://abi.ria.ee/xtee/et/x-tee-juhend/x-teega-liitumine.

25. Information System Authority 2020, *sahver.eesti.ee public file repository documentation* (In Estonian), accessed 29 March 2022, (General Terms) www.ria.ee/sites/default/files/content-editors/RIA/sahver.eesti.ee_uldtingimused.pdf,(Data protection requirements) www.ria.ee/sites/default/files/content-editors/RIA/sahver.eesti.ee_andmekaitsetingimused.pdf, (Guidelines) www.ria.ee/sites/default/files/content-editors/RIA/sahver.eesti.ee_juhend.pdf.

26. Cybernetica 2020, *Mobile voting feasibility study and risk analysis*, accessed 29 March 2022, www.valimised.ee/sites/default/files/uploads/eng/2020_m-voting-report.pdf.

27. Information System Authority 2020, *Guidelines for enterprise cybersecurity* (In Estonian), accessed 29 March 2022, www.ria.ee/sites/default/files/lisa_5._ettevotte_kyberturvalisuse_lyhijuhend_eesti_keeles.pdf.

28. Ministry of Economic Affairs and Communications 2021, *Analysis of the legal framework pertaining to the provision and use of governmental cloud services* (In Estonian), accessed 29 March 2022, www.mkm.ee/sites/default/files/privaatpilveteenuse_oigusanaluus_final_2021._1.pdf.

29. Ministry of Economic Affairs and Communications 2021, *Analysis on granting access to Estonia's public sector digital services for individuals holding EU e-authentication devices* (In Estonian), accessed 29 March 2022, www.mkm.ee/sites/default/files/lopparuanne_08.10_002_3.pdf.

30. Ministry of Economic Affairs and Communications 2021, *5G Use Case Study*, accessed 29 March 2022, www.mkm.ee/sites/default/files/5g_use_case_study_i_stage_summary.pdf.

31. The Estonian Patent Office n.d., *Guidelines for processing patent applications and patents* (In Estonian), accessed 29 March 2022, www.epa.ee/et/patenditaotluste-ja-patentide-menetlemise-juhised/sisukord.

32. Statistics Estonia 2018, *Estonian Data Governance Action Plan (2018-2022)* (In Estonian), accessed 29 March 2022, www.stat.ee/sites/default/files/2020-08/Eesti andmehalduse juhtimise tegevuskava_0.pdf.

33. *Act Amending the Cybersecurity Act, Public Information Act and Estonian Public Broadcasting Act (531 SE) (Parliamentary Proceeding)* (In Estonian), accessed 29 March 2022, www.riigikogu.ee/tegevus/eelnoud/eelnou/cd3107f9-b19c-4ed4-b6a7-7379fa3bf6b9/K%C3%BCberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringh%C3%A4%C3%A4lingu seaduse muutmise seadus.

34. *Act Amending the Consumer Protection Act (424 SE) (Parliamentary Proceeding) (*In Estonian), accessed 29 March 2022, www.riigikogu.ee/tegevus/eelnoud/eelnou/cd3107f9-b19c-4ed4-b6a7-7379fa3bf6b9/Küberturvalisuse%20seaduse,%20avaliku%20teabe%20seaduse%20ja%20Eesti%20Rahvusringhäälingu%20seaduse%20muutmise%20seadus.

35. *Accessibility of Products and Services Act (511 SE) (Parliamentary Proceeding)* (In Estonian), accessed 29 March 2022, www.riigikogu.ee/tegevus/eelnoud/eelnou/c5fb4aca-3bdd-4e6a-9a41-75cff097146d.

36. *Act Amending the State Secrets and Classified Foreign Information Act and the Public Information Act (410 SE) (Parliamentary Proceeding)* (In Estonian), accessed 29 March 2022, www.riigikogu.ee/tegevus/eelnoud/eelnou/6b80b26c-3ddd-4f2a-bd50-3bb6feff9479/Riigisaladuse ja salastatud v%C3%A4listeabe seaduse ning avaliku teabe seaduse muutmise seadus.

37. Eelnõude infosüsteem 2021, *Draft legislation regulating the field of crowdfunding and crypto assets* (Legislative Intent) (In Estonian), accessed 29 March 2022, https://eelnoud.valitsus.ee/main#N7eoXeeJ.

38. Ministry of Finance 2021, *A draft regulation regulating the field of crowdfunding and crypto assets has been sent to the Ministry of Justice for approval*, accessed 29 March 2022, www.fin.ee/en/news/draft-regulation-regulating-field-crowdfunding-and-crypto-assets-has-been-sent-ministry.

European Union

Dr Patryk Pawlak, European Union Institute for Security Studies

The European Union (EU) does not fit neatly into a template used to analyse the regulatory ecosystem of an individual state. With the exception of a few policy domains, where the European Commission (EC) enjoys exclusive competence, most of the decisions taken in Brussels are made by all member states represented in the Council of the European Union and elected members of the European Parliament acting jointly as co-legislators. In other words, whenever 'Brussels decides' it is de facto all 27 European Union capitals deciding jointly. It is the Court of Justice of the European Union's responsibility to settle any questions about the interpretation of the Union's treaties.

European Commission (EC)

Institutional Form: European Union institution

Responsible Minister: The President of the European Commission, the Commissioner for Competition and Chairing the Commissioners' Group on a Europe Fit for the Digital Age, The Commissioner for Internal Market

Principal Instrument(s): *Treaty on the Functioning of the European Union and Treaty on European Union (latest amendments in 2009 by the Treaty of Lisbon)*

Mandate: The EC has important roles as a regulator. At the institutional level, the EC has exclusive right of legislative initiative, which means it sets the European Union's policy agenda and proposes solutions in the technology domain. The legislative proposals or policy papers are adopted as the law (usually after a long legislative process) by the Council of the European Union (the Council) and the European Parliament. The EC also acts as the 'guardian of the Treaties', which means it is responsible for ensuring that individual member states implement the European Union's laws at the national level. If this is not the case, it can launch infringement procedures in front of the Court of Justice. At the regulatory level, the EC has powers regarding trans-border data flows and the enforcement of the competition rules against firms and states involving state aid, merger controls, cartels, and monopolies in the tech sector. It has conducted past probes into Google, Amazon, Apple and Facebook. One of the mechanisms for the transfer of personal data to third countries is the adequacy finding decision that can only be issued by the EC. While the European Union initiates regulatory processes in other areas such as the internal market, data protection, innovation policy, industrial policy and taxation, the formal decisions and implementation remains with member states. For instance, the Digital Services Act package (composed of the *Digital Services Act* and the *Digital Markets Act*) that will upgrade rules governing digital services in the European Union was proposed by the EC but its final shape is a result of the compromise between the Council and the European Parliament. The Court of Justice also plays an important role in adjudicating cases concerning the application of European Union law, including the ground-breaking 'Digital Rights Ireland' invalidating the European Union's data retention directive, the Schrems II ruling which invalidated the EU-US Privacy Shield Certification, and Google's action against the decision of the Commission finding that Google abused its dominant position.

Major Reports, Inquiries, and Related Initiatives:

- Digital Services Act (2022): [Webpage]
- Declaration on European Digital Rights and Principles (2022): [Declaration][1]
- Communication: 2030 Digital Compass: The European way for the Digital Decade (2021): [Communication][2]
- Google and Alphabet v Commission (Google Shopping) (2021): [Judgement][3]
- Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (2020): [Judgement][4]
- Artificial Intelligence Act (2021): [Act][5]
- Data Governance Act (2020): [Act][6]
- Digital Markets Act (2020): [Proposal]*
- The European Electronic Communications Code (2018): [Directive][7]
- Digital Rights Ireland invalidating the EU data retention directive (2014): [Directive][8]

Body of the European Regulators of Electronic Communications (BEREC)

Institutional Form: European Union agency

Responsible Minister: The European Commissioner for Internal Market (Directorate-General for Communications Networks, Content and Technology)

Principal Instrument(s): *Directive (EU) 2018/1972 establishing the European Electronic Communications Code (2018)*

Mandate: The BEREC fosters the independent, consistent, and high-quality regulation of digital markets for the benefit of the European Union and its citizens. The BEREC oversees the consistent application of the European Union's regulatory framework to promote an effective internal market in the telecommunication sector. The national regulatory authorities in member states and the EC take account of any opinion, recommendation, guidelines, advice, or regulatory practice adopted by the BEREC.

Major Reports, Inquiries, and Related Initiatives:

- BEREC Opinion on NIS 2 Directive (2021): [Opinion][9]
- BEREC Opinion on Roaming Regulation (2021): [Opinion][10]
- BEREC Opinion on Digital Markets Act (2021): [Opinion][11]
- BEREC Guidelines on Very High Capacity Networks (2020): [Guidelines][12]
- BEREC Guidelines on the Implementation of the Open Internet Regulation (2020): [Guidelines][13]

European Banking Authority (EBA)

Institutional Form: European Union body

Responsible Minister: The Board of Supervisors (main decision-making body), the Members of the Board of Supervisors shall act independently and in the Union's interest

Principal Instrument(s): *Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority) (2010)*

Mandate: The EBA is a single regulatory and supervisory framework for the European Union's banking sector. It implements a standard set of rules to regulate and supervise banking to create an efficient, transparent, and stable single market in European Union banking products. The EBA may develop draft regulatory technical standards that are submitted for adoption by the EC. The EBA's priorities include dimensions of fintech regulation, including in relation to artificial intelligence, digital identities, regulatory technology (RegTech), and financial supervision technology (SupTech). It also supports the development of European Union regulatory frameworks in the areas of crypto-assets, ICT, and security risk management.

Major Reports, Inquiries, and Related Initiatives:

- European Commission's Digital Finance Strategy (2020): [Strategy][14]
- Regulation on Markets in Crypto-assets (2020): [Proposal][15]
- Regulation on a pilot regime for market infrastructures based on distributed ledger technology (2020): [Proposal][16]
- Report with advice for the European Commission on crypto-assets (2019): [Report][17]
- EBA FinTech Roadmap (2018): [Roadmap][18]

* Article 46(1) of the GDPR (General Data Protection Regulation) states that "a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection". The following jurisdictions are recognised by the EC as providing adequate protection: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom under the GDPR and the LED and Uruguay. The adequacy finding decisions in favour of the United States have been invalidated by the Court of Justice.

European Central Bank (ECB)

Institutional Form: European Union institution

Responsible Minister: The President (independent body)

Principal Instrument(s): *The Treaty on the Functioning of the European Union*

Mandate: The ECB manages the Euro currency, keeps prices stable, and manages economic and monetary policy on behalf of the 19 European Union member states that use the Euro. Decisions, including setting interest rates and deciding which other monetary policy tools to use, are taken by the Governing Council. The most prominent role of the ECB in relation to technology concerns the introduction of digital currencies. In 2021, the ECB launched a digital Euro project to investigate issues regarding design and distribution.

Major Reports, Inquiries, and Related Initiatives:

- Report on a digital euro (2020): [Report][19]

European Data Protection Supervisor (EDPS)

Institutional Form: European Union body

Responsible Minister: The Supervisor (independent)

Principal Instrument(s): *Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices, and agencies and on the free movement of such data (2018)*

Mandate: The EDPS oversees European Union institutions and bodies with respect to privacy of personal data. It supervises the European Union's processing of personal data for compliance with privacy rules and advises European Union legislators on data protection and monitoring new technologies that may affect data protection. The advisory role is particularly relevant as the European Commission is often required to consult the EDPS on issues with 'an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.'[20]

Major Reports, Inquiries, and Related Initiatives:

- EDPS Opinion on the Proposal for a Regulation on Markets in Crypto-assets (2021): [Opinion][21]
- EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act): [Opinion][22]
- EDPS Opinion on the Pilot regime for market infrastructures based on Distributed Ledger Technology (2021): [Opinion][23]
- EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification, and acceptance of interoperable certificates on vaccination, testing and recovery (2021): [Opinion][24]
- EDPB-EDPS Joint Opinion on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Artificial Intelligence Act) (2021): [Opinion][25]
- EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI) (2019): [Opinion][26]

European Data Protection Board (EDPB)

Institutional Form: European Union body

Responsible Minister: The Chair (independent body)

Principal Instrument(s): *EU General Data Protection Regulation Directive (GDPR) (2016), Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Data Protection Law Enforcement Directive, 2016)*

Mandate: The EDPB ensures that laws related to the *General Data Protection Regulation* (GDPR) and the *Data Protection Law Enforcement Directive* are consistently applied in all relevant countries to promote cooperation among the national data protection authorities in the European Union, Norway, Liechtenstein, and Iceland. The EDPB provides guidance (including guidelines, recommendations, and best practice) to clarify the GDPR, adopts consistency findings to make sure the GDPR is interpreted consistently by all national regulatory bodies, and advises the European Commission on data protection issues and proposed European Union legislation. Like the European Data Protection Supervisor, the EDPB also issues opinions and guidelines on technological developments in the context of the *GDPR* and *Data Protection Law Enforcement Directive*. The Coordinated Enforcement Framework (CEF) provides a structure for coordinating recurring annual activities by the EDPB supervisory authorities. The CEF is the foundation on which the annual coordinated action is built (the 'rulebook' for coordinated action). The objective of the CEF is to facilitate joint actions in the broad sense in a flexible but coordinated manner, ranging from joint awareness raising and information gathering to an enforcement sweep and joint investigations. This contributes to compliance with the GDPR, ensuring the rights and freedoms of citizens and reducing the risk of services based on new technologies in the field of data protection.

Major Reports, Inquiries, and Related Initiatives:

- Guidelines 02/2021 on virtual voice assistants (2021): [Guidelines][27]
- EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679, 20 October, Version 1.1 (2021): [Guidelines][28]
- Guidelines 8/2020 on the targeting of social media users, Version 2.0 (2021): [Guidelines][29]
- Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications (2020): [Guidelines][30]
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020): [Guidelines][31]
- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0 (2020): [Guidelines][32]

*European Union Agency for the Space Programme (EUSPA)

Institutional Form: European Union agency

Responsible Minister: The European Commissioner for Internal Market (Directorate-General for Defence Industry and Space)

Principal Instrument(s): *Regulation (EU) 2021/696 establishing the Union Space Programme and the European Union Agency for the Space Programme (2021)*

Mandate: The EUSPA manages public interests related to the European Global Navigation Satellite System (GNSS), the European Geostationary Navigation Overlay System (GNSOS) and Galileo, the Earth observation program, Copernicus, and the European Union Governmental Satellite Communications (GOVSATCOM) program. The EUSPA is responsible for developing future generations of these systems, the evolution of their services, and the extension of their coverage. A core task for the EUSPA is the security of the European Union Space Programme. This includes security accreditation of all components of the space program through the Security Accreditation Board.

Major Reports, Inquiries, and Related Initiatives:

- EUSPA EO and GNSS Market Report (2022): [Report][33]

European Union Intellectual Property Office (EUIPO)

Institutional Form: European Union agency

Responsible Minister: The European Commissioner for Internal Market (Directorate-General for Internal Market, Industry, Entrepreneurship, and SMEs)

Principal Instrument(s): *Regulation (EU) 2017/1001 on the European Union trade mark (2017), Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs (2002)*

Mandate: The EUIPO manages European Union trade mark and design rights, the Observatory on Infringements of Intellectual Property Rights, and the Orphan Works Database. Its core business is the registration of European Union trade marks and registered community designs, which are valid throughout the European Union. It also hosts the European Observatory on Infringements of Intellectual Property Rights which fights against piracy and counterfeiting.

Major Reports, Inquiries, and Related Initiatives:

- Study on the Impact of Artificial Intelligence on the Infringement and Enforcement of Copyright and Designs (2022): [Report][35]

Endnotes (European Union)

1. European Commission) 2022, *Declaration on European Digital Rights and Principles*, Policy and Legislation, accessed 29 March 2022, https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Communication.

2. European Commission 2021, *Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, 2030 Digital Compass: the European way for the Digital Decade*, EUR-Lex, accessed 29 March 2022, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

3. General Court of the European Union 2021, *Judgment in Case T-612/17 Google and Alphabet v Commission (Google Shopping)*, accessed 29 March 2022, Court of Justice of the European Union, https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210197en.pdf.

4. Court of Justice of the European Union 2020, *Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Court of Justice of the European Union*, accessed 29 March 2022, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

5. European Commission 2021, *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, EUR-Lex, accessed 29 March 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

6. European Commission 2020, *Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, EUR-Lex, accessed 29 March 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.

7. *Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance)*, EUR-Lex, accessed 29 March 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694&qid=1647906195725.

8. *Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance),* Official Journal of the European Union, accessed 29 March 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972.

9. Court of Justice of the European Union 2014, *Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others*, accessed 29 March 2022, https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

10. Body of the European Regulators of Electronic Communications 2021, *Opinion on the proposed NIS 2 Directive and its effect on Electronic Communications*, accessed 29 March 2022, https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/9949-berec-opinion-on-the-proposed-nis-2-directive-and-its-effect-on-electronic-communications.

11. Body of the European Regulators of Electronic Communications 2021, *Opinion on the proposal of the Commission for amending the Roaming Regulation*, accessed 29 March 2022, https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/9934-berec-opinion-on-the-proposal-of-the-commission-for-amending-the-roaming-regulation.

12. Body of the European Regulators of Electronic Communications 2021, *Opinion on the European Commission's proposal for a Digital Markets Act*, accessed 29 March 2022, https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/9879-berec-opinion-on-the-european-commissions-proposal-for-a-digital-markets-act.

13. Body of the European Regulators of Electronic Communications 2020, *Guidelines on Very High Capacity Networks*, accessed 29 March 2022, https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9439-berec-guidelines-on-very-high-capacity-networks.

14. Body of the European Regulators of Electronic Communications 2020, *Guidelines on the Implementation of the Open Internet Regulation*, accessed 29 March 2022, https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation.

15. European Commission 2020, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU*, EUR-LEX, accessed 29 March 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591.

16. European Commission 2020, *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, EUR-LEX, accessed 29 March 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593.

17. European Commission 2020, *Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology (Text with EEA relevance)*, EUR-LEX, accessed 29 March 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0594.

18. European Banking Authority (EBA) 2019, *Report with advice for the European Commission on crypto-assets,* accessed 29 March 2022, www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf.

19. European Banking Authority 2018, *The EBA's FINTECH Roadmap: Conclusions from the consultation on the EBA's approach to financial technology (FINTECH), accessed 29 March 2022,* www.eba.europa.eu/sites/default/documents/files/documents/10180/1919160/79d2c-bc6-ce28-482a-9291-34cfba8e0c02/EBA%20FinTech%20Roadmap.pdf.

20. European Central Bank 2020, *Report on the digital euro*, accessed 29 March 2022, www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

21. *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the Protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*, EUR-LEX, accessed 29 March 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725.

22. European Data Protection Supervisor 2021, *EDPS Opinion on the Proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, accessed 29 March 2022, https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-regulation-markets-crypto_en.

23. European Data Protection Supervisor and European Data Protection Board 2021, *EDPS - EDPB Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, accessed 29 March 2022, https://edps.europa.eu/node/7140_en.

24. European Data Protection Supervisor 2021, *EDPS Opinion on the Pilot regime for market infrastructures based on Distributed Ledger Technology*, accessed 29 March 2022, https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-pilot-regime-market-infrastructures_en.

25. European Data Protection Board and European Data Protection Supervisor 2021, *EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery*, accessed 29 March 2022, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042021-proposal_en.

26. European Data Protection Supervisor and European Data Protection Board 2021, *EDPS - EDPB Joint Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, accessed 29 March 2022, https://edps.europa.eu/node/7140_en.

27. European Data Protection Board and European Data Protection Supervisor 2019, *EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI)*, accessed 29 March 2022, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12019-processing_en.

28. European Data Protection Board 2021, *Guidelines 02/2021 on virtual voice assistants*, accessed 29 March 2022, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_en.

29. European Data Protection Board 2021, *EDPB Document on Coordinated Enforcement Framework under Regulation 2016/679 Version 1.1*, accessed 29 March 2022, https://edpb.europa.eu/sites/default/files/files/file1/edpb_documents_20201020_coordinatedenforcementframework_en.pdf.

30. European Data Protection Board 2021, *Guidelines 8/2020 on the targeting of social media users Version 2.0*, accessed 29 March 2022, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf.

31. European Data Protection Board 2021, *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*, accessed 29 March 2022, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012020-processing-personal-data-context_en.

32. European Data Protection Board 2020, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak,* accessed 29 March 2022, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en.

33. European Data Protection Board 2020, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, accessed 29 March 2022, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

34. European Union Agency for the Space Programme 2020, *EUSPA EO and GNSS Market Report,* Publications Office of the European Union, Luxembourg, accessed 29 March 2022, www.euspa.europa.eu/sites/default/files/uploads/euspa_market_report_2022.pdf.

35. European Union Intellectual Property Office 2022, *Impact of Technology Deep Dive Report 1: Study on the Impact of Artificial Intelligence on the Infringement and enforcement of copyright and designs*, accessed 29 March 2022, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs/2022_Impact_AI_on_the_Infringement_and_Enforcement_CR_Designs_FullR_en.pdf.

Fiji

Cherie Lagakali, Global Forum on Cyber Expertise

Telecommunications Authority of Fiji (TAF)

Institutional Form: Independent statutory authority

Responsible Minister: The Minister for Economy, Civil Service, Communications, Housing and Community Development

Principal Instrument(s): *Telecommunications Act (2008), Telecommunications Promulgation (2008)*

Mandate: The TAF implements Fiji's telecommunications policy, licensing the provision of telecommunications services and oversees spectrum, broadcasting, equipment, frequency links to spectrum and compliance. The TAF also mediates the resolution of disputes between licensees or between licensees and consumers, as well as protecting consumer interests and promoting consumer awareness relating to telecommunications. In 2017, the TFA facilitated a Fiji-IXP Steering committee which led to establishing Fiji-IX, where all local traffic is routed through the IX Switch.[1]

Major Reports, Inquiries, and Related Initiatives:

- Fiji joins the IXP community (2017): [APNIC Blog][2]

Online Safety Commission (OSC)

Institutional Form: Independent statutory authority

Responsible Minister: The Minister for Economy, Civil Service, Communications, Housing and Community Development

Principal Instrument(s): *Online Safety Regulations (2019), Online Safety Act (2018)*

Mandate: The OSC has a dual education role about using digital spaces safely and personal responsibility when using digital spaces. It provides support for people experiencing harmful online communication by receiving and responding to complaints from any individual who has reason to believe that he or she is the target or recipient of electronic communication intended or likely to cause harm. The OSC gives Fijians a platform to resolve concerns related to electronic communication abuse such as online bullying, trolling, and image-based abuse. It also educates digital communication users to be responsible and safe online. The current areas of focus are online child abuse, COVID-19 online safety, and being safe online. The OSC works with Australia's Office of the eSafety Commissioner to tackle online abuse. Supported by the Vuvale Partnership between the two nations through Australia's Cyber Cooperation Program, the partnership began with a Commissioner-to-Commissioner conversation about online safety and its impacts between the two nations.[3]

Major Reports, Inquiries, and Related Initiatives:

- Online Safety Act (2018): [Act][4]
- Online Safety Regulations (2019): [Regulations][5]

Fijian Competition and Consumer Commission (FCCC)

Institutional Form: Independent statutory authority

Responsible Minister: The Ministry of Commerce, Trade, Tourism and Transport

Principal Instrument(s): *Section 7 of the Fijian Competition and Consumer Commission Act (2010)*

Mandate: The FCCC administers compliance of consumer protection laws within the *Competition and Consumer Act*. The FCCC controls and regulates prices of industries and markets where competition is diminished or limited, including electricity, telecommunications, ports, maritime and airport sectors.

Major Reports, Inquiries, and Related Initiatives:

- FCCC Approves Acquisition of Digicel Fiji (Pte) Limited by Telstra Corporation Limited (2022): [Press Release][6]
- Digital Transformation to Protect Social and Economic Rights of all Fijians (2020): [Press Release][7]

Fiji Financial Intelligence Unit (FIU)

Institutional Form: Independent administrative statutory authority

Responsible Minister: The Minister for Justice, the Governor of the Reserve Bank

Principal Instrument(s): *Financial Transactions Reporting Act (2004)*

Mandate: The FIU combats money laundering, terrorism financing and other serious crimes. It safeguards Fiji's financial system by collecting and analysing financial transactions and other information, disseminating financial intelligence, administering regulatory compliance to the anti-money laundering and counter-terrorist financing measures, public education and awareness, domestic, and international coordination.

Major Reports, Inquiries, and Related Initiatives:

- Cryptocurrency, Trading and Illegal Pyramid Selling Schemes (2021): [Press Release][8]
- Financial Intelligence Unit Strategic Plan (2020–2024): [Strategy][9]
- Financial Transactions Reporting Act (2004): [Act][10]

Reserve Bank of Fiji (RBF)

Institutional Form: Independent statutory authority

Responsible Minister: The Minister for Economy, Civil Service, Communications, Housing and Community Development

Principal Instrument(s): *Personal Properties Securities Regulations (2019), Fair Reporting of Credit Act (2016), The Companies Act (2015), Constitution (2013), Fiji National Provident Fund Decree (2011), RBF (Amendment) Decree (2009), Financial Transactions Reporting (FTR) Act (2004), FTR Regulations (2004), Payment and Settlement Systems Oversight Regulations (2004), Insurance Act (1998), Banking Act (1995), Exchange Control Act (Rev.1985), Reserve Bank of Fiji Act (1983)*

Mandate: The RBF is Fiji's central bank. It protects the value of currency for balanced and sustainable growth, formulates monetary policy, promotes price stability, and issues Fiji's currency. The RBF promotes monetary stability through low and stable inflation and maintains an adequate level of foreign reserves. It provides banking, registry, and foreign exchange services to the government and is a lender of last resort to commercial banks. The RBF also has oversight of Fiji's payment system, FIJICLEAR, which is used by all commercial banks to settle interbank and customer payments. The RBF continues to facilitate the adoption of digital modes of payments in the country through Fiji's two Mobile Network Operators: Vodafone Fiji Limited and Digicel Fiji.

Major Reports, Inquiries, and Related Initiatives:

- Media Note No.1 - Stakeholder Consultation on Draft National Payment System Regulations (2022): [Consultation][11]
- RBF Partners with UNCDF for Parametric Insurance Product – Fintech Regulatory Sandbox (2022): [Sandbox][12]

Media Industry Development Authority (MIDA)

Institutional Form: Independent statutory authority

Responsible Minister: The Attorney-General, the Minister for Information

Principal Instrument(s): *Media Industry Development Act (2010)*

Mandate: The MIDA encourages, promotes, and facilitates the development of media organisations and services in Fiji. It also advises and makes recommendations to the minister on matters, measures and regulations related to the media. The MIDA's role is also to facilitate the provision of media services that serve the national interest and promote local content in print and broadcast media. The aim is to maintain Fiji's media at a high standard of quality and range of subject matter in the content.

Major Reports, Inquiries, and Related Initiatives:

- Media Industry Development (Amendment) Bill (2015): [Bill][13]

Fiji Human Rights and Anti-Discrimination Commission (FHRADC)

Institutional Form: Independent statutory authority

Responsible Minister: The Prime Minister and President

Principal Instrument(s): *Human Rights and Anti-Discriminating Commission Act (2009)*

Mandate: The FHRADC is a human rights institution and has responsibilities to promote the protection and observance of human rights in public and private institutions as well as to develop a culture of human rights in Fiji.

Major Reports, Inquiries, and Related Initiatives:

- Fiji Human Rights Report (2020): [Report][14]

Fiji Revenue and Customs Authority (FRCA)

Institutional Form: Statutory authority

Responsible Minister: The Minister for Economy, Civil Service, Communications, Housing and Community Development

Principal Instrument(s): *Income Tax (Submarine Network Cable Investment Incentives) Regulations (2021), Income Tax (ICT Infrastructure Investment Incentives) Regulations (2021), Income Tax Act (2015), Tax Administration Act (2009), Fiji Revenue and Customs Authority (Change of Name) Act 1999 (No 30 of 1999), Fiji Revenue and Customs Authority Act (1998), Fiji Revenue and Customs Service Act (1998), Value Added Tax Act (1991), Customs Act (1986), Customs Tariff Act (1986), Customs Regulations (1986)*

Mandate: The FRCA collects taxes and duties on behalf of the government, provides quality advice on taxation and customs matters, facilitates trade and travel, and protects Fiji's borders. The FRCA's organisational structure is realigning to take advantage of internal synergies and technological advancements that will be easier for taxpayers, traders, and travellers to comply with and make the FRCA more efficient and effective. The FRCA implements regulation to establish submarine cables and ICT infrastructure.

Major Reports, Inquiries, and Related Initiatives:

- Income Tax (Submarine Network Cable Investment Incentives) Regulations (2021): [Regulations][15]
- Income Tax (ICT Infrastructure Investment Incentives) Regulations (2021): [Regulations][16]
- FRCS Strategic Plan (2021- 2024): [Strategic Plan][17]

*Ministry of Communication, Digital Government Transformation Office (DGTO)

Institutional Form: Department under the Ministry of Communications

Responsible Minister: The Director-General for Digital Government Transformation, Cybersecurity and Communications who is also the (Acting) Permanent Secretary for the Ministry of Communications

Principal Instrument(s): *Cybercrime Act (2021)*

Mandate: The DGTO is responsible for the regulation of cyber security in Fiji through the Ministry of Communication, which itself is responsible for keeping Fijians connected locally and globally and providing efficient, competitive, cost-effective, and accessible telecommunication and postal services.

Major Reports, Inquiries, and Related Initiatives:

- National Security and Defence Council in its meeting (2018): [Report][18]

Office of the Attorney-General, Fiji Intellectual Property Office (FIPO)

Institutional Form: Office within the Attorney-General's Office

Responsible Minister: The Minister for Justice

Principal Instrument(s): *Trade Marks Act (2021), Patents Act (2021), Designs Act (2021)*

Mandate: The FIPO is responsible for copyright laws that adhere to international laws and the registration of trade marks and petitions for patent in Fiji through the Office of the Attorney-General. Until 2021 Fiji's trademark and patent laws were outdated. As a result, Fiji was neither a member of the Paris Convention nor the Patent Cooperation Treaty. After more than 70 years, on 19 August 2021, the Parliament of Fiji tabled and passed the acts below. The passing of these Acts is a significant step forward for Fiji's trade mark, patent, and design laws as they become more aligned and compliant to international standards and practices.

Major Reports, Inquiries, and Related Initiatives:

- Trade Marks Act (2021): [Act][19]
- Patents Act (2021): [Act][20]
- Designs Act (2021): [Act][21]

Endnotes (Fiji)

1. Telecommunications Authority of Fiji n.d., *Fiji – Internet Exchange Point*, accessed 29 March 2022, www.taf.org.fj/Publications/Fiji-IX.aspx.

2. Robbie Mitchell 2017, *Fiji joins the IX community*, APNIC, accessed 29 March 2022, https://blog.apnic.net/2017/12/01/fiji-joins-ix-community/.

3. MSQUARE Productions n.d., *Australia & Fiji: Commissioner to Commissioner (Full Length) (Video)*, Vimeo, accessed 29 March 2022, https://vimeo.com/520722254/aa6d863434.

4. *Online Safety Act 2018,* accessed 29 March 2022, https://laws.gov.fj/Acts/DisplayAct/2462.

5. *Online Safety Regulations 2019,* accessed 29 March 2022, https://laws.gov.fj/Acts/DisplayAct/2463.

6. Fijian Competition and Consumer Commission 2022, *FCCC Approves Acquisition of Digicel Fiji (Pte) Limited by Telstra Corporation Limited*, accessed 29 March 2022, https://fccc.gov.fj/wp-content/uploads/2022/03/MR-FCCC-Approves-Acquisition-of-Digicel-Pacific-and-Telstra-Corporation-Limited-_Draft-1-Final.pdf.

7. Fijian Competition and Consumer Commission 2020, *Digital Transformation to Protect Social and Economic Rights of all Fijians*, accessed 29 March 2022, https://fccc.gov.fj/wp-content/uploads/2020/10/Press-Release-FCCC-UNDP-Signing-Final.pdf.

8. Fiji Financial Intelligence Unit 2021, *Cryptocurrency Trading & Illegal Pyramid Selling Schemes*, accessed 29 March 2022, www.fijifiu.gov.fj/getattachment/5c1ce2ad-3192-46f0-9186-333a4e06cdcd/attachment.aspx.

9. Fiji Financial Intelligence Unit 2020, *Financial Intelligence Unit Strategic Plan*, accessed 29 March 2022, www.fijifiu.gov.fj/getattachment/Publications/Strategic-Plans/Strategic-Plan-2020-2024/FIU-STRATEGIC-PLAN-2020-2024.pdf.aspx.

10. Financial Transactions Reporting Act 2004, accessed 29 March 2022, www.fijifiu.gov.fj/getattachment/Law-Regulations/FTR-Act/ftrAct2004.pdf.aspx.

11. Reserve Bank of Fiji 2022, *Media Note No 1 – Stakeholder Consultation on Draft National Payment System Regulations,* accessed 29 March 2022, www.rbf.gov.fj/media-note-no-1-stakeholder-consultation-on-draft-national-payment-system-regulations/.

12. Reserve Bank of Fiji 2022, *RBF partners with UNCDF for Parametric Insurance Product*, accessed 29 March 2022, www.rbf.gov.fj/joint-press-release-rbf-partners-with-uncdf-for-parametric-insurance-product-becomes-first-solution-admitted-for-testing-in-fintech-regulatory-sandbox/.

13. *Media Industry Development (Amendment) Bill 2015*, accessed 29 March 2022, www.parliament.gov.fj/wp-content/uploads/2017/03/Bill-No-15-Media-Industry-Development-Amendment-1.pdf.

14. Fiji Human Rights and Anti-Discrimination Commission 2020, *FIJI 2020 Human Rights Report*, accessed 29 March 2022, www.state.gov/wp-content/uploads/2021/03/FIJI-2020-HUMAN-RIGHTS-REPORT.pdf.

15. *Income Tax (Submarine Network Cable Investment Incentives) Regulations*, accessed 29 March 2022, www.frcs.org.fj/wp-content/uploads/2021/09/SIG-2021-20-Submarine-Network-Cable-Investment-Incentive.pdf.

16. *Income Tax (ICT Infrastructure Investment Incentives) Regulations (2021)*, accessed 29 March 2022, www.frcs.org.fj/wp-content/uploads/2021/09/SIG-2021-25-ICT-Infrastructure-Investment-Incentives.pdf.

17. Fiji Revenue and Customs Authority 2021, *Strategic Plan 2021 – 2024: Helping Fiji Grow*, accessed 29 March 2022, www.frcs.org.fj/wp-content/uploads/2021/04/FRCS-SPLAN-2021-2024.pdf.

18. Ministry of Defence and National Security 2020, *Presentation to the Standing Committee on Foreign Affairs and Defence*, accessed 29 March 2022, www.parliament.gov.fj/wp-content/uploads/2020/05/Appendices-MoDNS-AR-2016-2017.pdf.

19. *Trademarks Act 2021,* accessed 29 March 2022, www.parliament.gov.fj/wp-content/uploads/2021/08/Act-No.-36-Trademarks02.pdf.

20. *Patents Act 2021,* accessed 29 March 2022, www.parliament.gov.fj/wp-content/uploads/2021/08/Act-No.-37-Patents.pdf.

21. *Designs Act 2021,* accessed 29 March 2022, www.parliament.gov.fj/wp-content/uploads/2021/08/Act-No.-38-Designs.pdf.

Germany

Lola Attenberger, The European School of Management and Technology (EMST Berlin)

Federal Commissioner for Data Protection and Freedom of Information (BfDI)

Institutional Form: Independent statutory authority

Responsible Minister: The Federal Commissioner for Data Protection and Freedom of Information

Principal Instrument(s): *Federal Data Protection Act (BDSG, 2017), EU General Data Protection Regulation Directive (GDPR) (2016), Freedom of Information Act (IFG, 2006), Safety Review Act (1994)*

Mandate: The BfDI administers the data protection law for Germany's federal public bodies, as well as for certain social security institutions. The BfDI monitors these bodies to ensure implementation and compliance with the legal provisions on data protection. It also supervises telecommunications and postal service companies.

Major Reports, Inquiries, and Related Initiatives:

- Consultation procedure of the Federal Commissioner for Data Protection and Freedom of Information (2021): [Webpage] (In German)[1]
- Anonymization under the GDPR with special regard to the telecommunications industry (2020): [Webpage] [Position Paper] (In German)[2]
- Overview about major resolutions and statements of the board of the state-level data protection authorities: [Webpage] (In German)[3]

Federal Office for Information Security (BSI)

Institutional Form: Federal authority

Responsible Minister: The Federal Minister of Interior and Community

Principal Instrument(s): *IT Security Act 2.0 (2020), IT-Security Law (2015), Act on the Federal Office for Information Security (BSI Act – BSIG) (2009), Ordinance on the Designation of Critical Infrastructures under the BSI Act (BSI Critical Infrastructure Ordinance - BSI-KritisV)*

Mandate: The BSI protects government networks and secures central network transitions. With the amendment of the BSI Act in 2009, the BSI's mandate was expanded to include the development of binding security standards for the procurement and use of IT for federal authorities. The *IT Security Act 2.0* further expanded the BSI's powers to include obligations for operators of critical infrastructure to maintain a critical infrastructure register, use state of the art attack-detection systems, submit documents required for an assessment by BSI and, in the event of a significant disruption, an obligation to release information necessary to manage the disruption. According to section 8a of the BSI Act, operators of essential services are obliged to prove the implementation of appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems.

Major Reports, Inquiries, and Related Initiatives:

- IT-Grundschutz (Basic Protection) (2021): [Webpage][4]
- Cabinet approves draft IT Security Act 2.0 (2021): [Draft] (In German)[5]
- The State of IT Security in Germany 2020 (2020): [Report][6]
- Orientation guide to documentation of compliance according to Section 8a (3) BSIG (2020): [Download and Links for Operators and Auditors] (In German)[7]

Federal Ministry for Interior (BMI)

Institutional Form: Federal ministry

Responsible Minister: The Federal Minister of Interior and Community

Principal Instrument(s): *IT Security Act 2.0 (2020) Act on the Federal Office for Information Security (BSI Act – BSIG) (2009)*

Mandate: The BMI is responsible for the internal security of Germany. For example, pursuant to section 9b of the *BSI Act*, the operator of a critical infrastructure shall notify BMI of the planned first-time use of a critical component prior to its use. Operators must also obtain a certificate of 'trustworthiness' for critical components. The BMI can prohibit the planned initial or further use of a critical component vis-à-vis the operator of the critical infrastructure. The BSI also maintains the federal law enforcement agencies of the Federal Police and the Federal Criminal Police Office, and is responsible for the domestic intelligence agency, the Federal Office for the Protection of the Constitution.

Major Reports, Inquiries, and Related Initiatives:

- The Cybersecurity Strategy for Germany (2021): [Strategy][8]

Federal Cartel Office (Bundeskartellamt) (BKartA)

Institutional Form: Independent authority

Responsible Minister: The Federal Minister for Economic Affairs and Climate Action

Principal Instrument(s): *Act Amending the Act against Restraints of Competition for a focused, proactive, and digital competition law 4.0 and amending other competition law provisions ("GWB-Digitalisierungsgesetz" - GWB Digitalisation Act, 2021), Competition Register Act (WRegG, 2017), Act Against Restraints of Competition (GWB, 2013)*

Mandate: The BKartA is Germany's independent competition authority and manages any restraints of competition that affect Germany. The work of the BKartA is based on the *Act Against Restraints of Competition* and, where appropriate, European competition law. Following the tenth amendment of the *GWB Digitalisation Act*, pursuant to section 19a, the BKartA has the power to determine whether a firm is of paramount significance for competition across markets and can prohibit engagement in anti-competitive conduct.

Major Reports, Inquiries, and Related Initiatives:

- Resolution recommendation and report of the Committee on Economic Affairs and Energy (9th Committee) (2021): [Legislative Memorandum] (In German)[9]
- Draft bill of the Federal Ministry for Economic Affairs and Energy (2021): [Memorandum] (in German)[10]
- Guidelines for the setting of fines in cartel administrative offence proceedings (2021): [Guidelines][11]
- Working Paper – Algorithm and Competition (2019): [Working Paper][12]

Federal Network Agency (Bundesnetzagentur) (BNetzA)

Institutional Form: Independent authority

Responsible Minister: The Federal Minister for Economic Affairs and Climate Action, and the Federal Minister for Digital and Transport

Principal Instrument(s): *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic Identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS regulation 2014), Grid Expansion Acceleration Act (NABEG, 2011), Electromobility Compatibility Act and the Act on Radio Equipment and Telecommunications Terminal Equipment, Act on Digital Signature (SiG, 1997), Telecommunications Act (TKG, 1996)*

Mandate: The BNetzA fosters competition to reduce trade barriers, ensure free trade, and protect the public from unsafe equipment. The BNetzA monitors products that have been placed on the market with respect to electromagnetic compatibility in line with the *Electromobility Compatibility Act* and the *Act on Radio Equipment and Telecommunications Terminal Equipment*. It is also the competent authority under the *Digital Signature Act.*

Major Reports, Inquiries, and Related Initiatives:

- Finding from the consultation on blockchain technology in the network sectors (2020): [Webpage and Report] (In German)[13]

Federal Office for Economic Affairs and Export Control (BAFA)

Institutional Form: Federal authority

Responsible Minister: The Federal Minister for Economic Affairs and Export Control

Principal Instrument(s): *Regulation (EU) 2021/821 setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (EU Dual-Use Regulation, 2021), Union General Export Authorisations (UGEAs, Annex II of Regulation (EU) 2021/821), Foreign Trade and Payments Act (AWG, 2013, last amended 2021), Treaty on the Functioning of the European Union (TFEU, 2009, last amended 2012), Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community (2009), Act to Protect against Threats to the Security of the Federal Republic of Germany from the Dissemination of High-quality Remote Sensing Data (SatDSiG, 2007)*

Mandate: The BAFA administers foreign trade and payments, business promotion, and energy. It is also responsible for export control and implementing import regulations adopted as part of the European Union's common trade policy. The BAFA grants import licenses and surveillance documents for items of trade and industry that are subject to quantitative restriction or supervision by the European regulations. It translates the common trade policy of the European Union into individual decisions. It also implements the embargo resolutions adopted by international organisations, for example, arms embargoes imposed by the United Nations or the European Union.

Major Reports, Inquiries, and Related Initiatives: None issued

German Patent and Trade Mark Office (DPMA)

Institutional Form: Federal authority

Responsible Minister: The Federal Minister of Justice

Principal Instrument(s): *Act on the Copyright Liability of Online Content Sharing Service Providers (UrhDaG, 2021), Federal Act Governing Access to Information held by the Federal Government (2005), DPMA Ordinance, Patent Costs Act (2001), Trade Mark Act (1994), Semiconductor Protection Act (1987), Utility Model Ordinance (1986), Patent Act (1980), Patent Ordinance, Act on International Patent Conventions (InPatÜbkG, 1976)*

Mandate: The DPMA is responsible for the protection of intellectual property in Germany. It examines inventions, grants patents, registers trade marks, utility models and designs, administers intellectual property rights and provides intellectual property information to the public.

Major Reports, Inquiries, and Related Initiatives:

- Guidelines for the Examination Procedure (P2796.1) (current version is being updated, version from 2019): [Guidelines][14]
- Guidelines for the Classification of Patent and Utility Model Applications (P2733.1) (current version is being updated, version from 2019): [Guidelines][15]

Federal Financial Supervisory Authority (BaFin)

Institutional Form: Independent regulatory authority

Responsible Minister: The Federal Minister of Finance

Principal Instrument(s): *Financial Market Integrity Strengthening Act (FISG) (2021), German Banking Act (Kreditwesengesetz – KWG, 1961, last amended 2021), Act Establishing the Federal Financial Supervisory Authority (Finanzdiestleistungsaufsichtsgesetz – FinDAG, 2002, last amended 2011), Act on Administrative Enforcement (2010), Securities Trading Act (Wertpapierhandelsgesetz – WpHG)*

Mandate: The BaFin is responsible for the proper functioning, stability, and integrity of the German financial system at the national and international levels. The BaFin controls balances from capital-oriented corporations in accordance with the *Financial Market Integrity Act*. Depending on their structure, FinTech businesses may require authorisation by the BaFin.

Major Reports, Inquiries, and Related Initiatives:

- Consultation on a planned General Administrative Act regarding Futures with additional payment obligations (2022): [Webpage][16]
- Big data meets artificial intelligence: Challenges and implications for the supervision and regulation of financial services (2019): [Report] [Summary][17]

German Central Bank (Deutsche Bundesbank)

Institutional Form: Independent regulatory authority

Responsible Minister: The Federal Minister of Finance

Principal Instrument(s): *Act on the Prudential Supervision of Payment Services (Payment Services Supervision Act, Zahlungsdiensteaufsichtsgesetz, 2017, last amended 2021), Supervision of Financial Conglomerates Act (Finanzkonglomerate-Aufsichtsgesetz – FKAG, 2013, last amended 2021), German Banking Act (Kreditwesengesetz – KWG, 1961, last amended 2021)*

Mandate: The Deutsche Bundesbank is the central bank of Germany. It administers the monetary policy of the Euro system. It maintains the financial and monetary system, banking supervision, non-cash payments, and cash. The *German Banking Act* forms the legal basis for the supervision of credit institutions and financial services institutions. The legal basis for the supervision of payment institutions and e-money institutions is the *Payment Services Oversight Act*. Almost all the provisions of this Act transpose the *European Payment Services Directive*. The supervision of the *Financial Conglomerates Act* is designed to limit regulatory arbitrage and provides for supplementary supervision of financial conglomerates.

Major Reports, Inquiries, and Related Initiatives:

- Money in programmable applications – Cross-sector perspectives from the German Economy (2020): [Initiative][18]
- How can collateral management benefit form DLT? – Project BLOCKBASTER (2020): [Report][19]
- Cash in the age of payment diversity – International Cash Conference 2019 (2019): [Conference Volume][20]
- Procedural rules of the Deutsche Bundesbank for retrieval of electronic account information - Rules electronic account information (2018): [Rules][21]

Federal Central Tax Office (Bundeszentralamt für Steuern) (BZSt)

Institutional Form: Federal authority

Responsible Minister: The Federal Minister of Finance

Principal Instrument(s): *Corporate Income Tax Modernization Act (KöMoG) (2021), Financial Administration Act (Finanzverwaltungsgesetz – FVG, 1971, last amended 2021), Act on Implementing the Changes to the EU Mutual Assistance Directive and Other Measures against Base Erosion and Profit Shifting (BEPS Implementation Act, BGBl. I 2016, 3000) (2016), Value Added Tax Act (Umsatzsteuergesetz – UStG, 1994), Corporate Income Tax Act (KStG)*

Mandate: The BZSt is responsible for administering sections of the Germany's tax code. It performs numerous tasks with a national and international dimension which are assigned to it by the *Financial Administration Act (FVG)*.

Major Reports, Inquiries, and Related Initiatives: None issued

Federal Office of Justice (Bundesministerium der Justiz) (BfJ)

Institutional Form: Federal administrative authority

Responsible Minister: The Federal Minister of Justice

Principal Instrument(s): *Act Implementing the Digitization Directive (DiRUG) (2021), Act to strengthen consumer protection in competition and trade law (2021), Act on Applications for an Injunction (Unterlassungsklagengesetz, UKlaG, 2001, last amended 2021), Commercial Code (Handelsgesetzbuch, HGB, 1897, last amended 2021), Act on Regulatory Offences (1987, last amended 2019), Unfair Competition Act (UWG) (2010, last amended 2019), Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act, 2017)*

Mandate: The BfJ has oversight of the *Network Enforcement Act*. In accordance with this act, social network providers that receive more than 100 complaints per calendar year about unlawful content are obliged to produce half-yearly German-language reports on the handling of those complaints. The report must be published in the Federal Gazette and on social network providers' own website no later than one month after the half-year period has ended. The provider of a social network must maintain an effective and transparent procedure for handling complaints about unlawful content. Offences under the *Network Enforcement Act* may be sanctioned even if it is not committed in the Federal Republic of Germany.

Major Reports, Inquiries, and Related Initiatives:

- Online trade in the area of conflict between consumer protection and sustainability (2020): [Policy Brief] (In German)[22]

*Germatik (Gesellschaft mit beschränkter Haftung) (GmbH)

Institutional Form: Limited liability company

Responsible Minister: The Federal Minister of Health

Principal Instrument(s): *Act on Secure Digital Communications and Applications in Healthcare and on the Amendment of Other Laws (E-Health Law, 2015), German Social Code (SGB) Book Five (V) (1988)*

Mandate: The Gematik operates and develops the telematics infrastructure and electronic health card in Germany. It also administers specialist applications and additional applications for communication between healthcare professionals, payers, and insured people. The Germatik defines and enforces standards for services, components, and applications in telematics infrastructure so that this central infrastructure remains secure, efficient, and user-friendly.

Major Reports, Inquiries, and Related Initiatives:

- Whitepaper TI 2.0 – Arena für digitale Medizin (2021): [Whitepaper] (In German)[23]
- Interoperability 2.0 based on the Health IT Interoperability Governance Regulation (IOP-Governance-Verordnung – GIGV) (2021): [Regulation] (In German)[24]

Ongoing Parliamentary Committees, Inquiries, or Legislative Proposals (not previously referred to):

- Committee on Education, Research and Technology Assessment (ongoing): [Committee Webpage][25]
- Committee on Digital Affairs (ongoing): [Committee Webpage][26]
- Draft law on the introduction of electronic proof of identity with a mobile device (2021): [Draft Law] (In German)[27]
- Relevant recent acts, related to the Civil Code (BGB):
  - *Law regulating the sale of things with digital elements and other aspects of the contract of sale (2021)*: [Act] (In German)[28]
  - *Act implementing the Directive on certain aspects of contract law relating to the provision of digital content and digital services (2021)*: [Act] (In German)[29]
  - *Act Amending the Civil Code and the Introductory Act to the Civil Code (BGB) in Implementation of the EU Directive on Better Enforcement and Modernization of Union Consumer Protection Rules and Repealing the Regulation Transferring Responsibility for the Implementation of Regulation (EC) No. 2006/2004 to the Federal Ministry of Justice and Consumer Protection (enters into force on 28 May 2022)*: [Act] (In German)[30]
  - *Implementation of Regulation (EC) No. 2006/2004 as the Act Amending the Civil Code and the Introductory Act to the Civil Code (BGB) in Implementation of the EU Directive on Better Enforcement and Modernization of Union Consumer Protection Rules (enters into force on 28 May 2022)*: [Act] (In German)[31]

Endnotes (Germany)

1. Federal Commissioner for Data Protection and Freedom of Information 2021, *Consultation procedure of the Federal Commissioner for Data Protection and Freedom of Information* (In German), accessed 29 March 2022, www.bfdi.bund.de/DE/DerBfDI/Inhalte/Konsultationsverfahren/KI-Strafverfolgung/KI-Strafverfolgung-Thesen-BfDI.html.

2. Federal Commissioner for Data Protection and Freedom of Information 2020, Anonymization under the GDPR with special regard to the telecommunications industry (In German), accessed 29 March 2022, www.bfdi.bund.de/DE/DerBfDI/Konsultationsverfahren/Anonymisierung-TK/Anonymisierung-TK_node.html.

3. Datenschutzkonferenz n.d., *Overview about major resolutions and statements of the board of the state-level data protection authorities* (In German), accessed 29 March 2022, www.datenschutzkonferenz-online.de.

4. *IT-Grundschutz (Basic Protection),* accessed 29 March 2022, www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html.

5. *Bundesministerium des Innern und für Heimat 2020, Kabinett beschließt Entwurf für IT-Sicherheitsgesetz 2.0* (In German), accessed 29 March 2022, www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/it-sig-2-kabinett.html.

6. *The State of IT Security in Germany in 2020*, accessed 29 March 2022, www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2020.html.

7. Federal Office for Information Security 2020, *Orientation guide to documentation of compliance according to Section 8a (3) BSIG* (In Germany), accessed 29 March 2022, www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/KRITIS-Downloads/kritis-downloads_node.html.

8. Federal Ministry for Interior and Community 2021, *Cyber Security Strategy for Germany*, accessed 29 March 2022, www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html.

9. *Resolution recommendation and report of the Committee on Economic Affairs and Energy (9th Committee) 2021* (In German), accessed 29 March 2022, https://dserver.bundestag.de/btd/19/258/1925868.pdf.

10. *Draft bill of the Federal Ministry for Economic Affairs and Energy 2021* (In German), accessed 29 March 2022, www.bmwi.de/Redaktion/DE/Downloads/G/gwb-digitalisierungsgesetz-referentenentwurf.pdf?__blob=publicationFile&v=10.

11. Federal Cartel Office 2021, *Guidelines for the setting of fines in cartel administrative offence proceedings*, accessed 29 March 2022, www.bundeskartellamt.de/SharedDocs/Publikation/EN/Leitlinien/Guidelines_setting_fines_Oct_2021.html.

12. Federal Cartel Office 2019, *Working Paper - Algorithms and Competition*, accessed 29 March 2022, www.bundeskartellamt.de/SharedDocs/Publikation/EN/Berichte/Algorithms_and_Competition_Working-Paper.html?nn=4677870.

13. Federal Network Agency 2020, *Findings from the consultation on blockchain technology in the network sectors* (In German), accessed 29 March 2022, www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Grundsatzpapier/grundsatzpapier-node.html.

14. German Patent and Trade Mark Office 2019, *Guidelines for the Examination Procedure (P2796.1)*, accessed 29 March 2022, www.dpma.de/docs/english/formulare/patent_eng/p2796_1.pdf.

15. German Patent and Trade Mark Office 2019, *Guidelines for the Classification of Patent and Utility Model Applications (P2733.1)*, www.dpma.de/docs/english/formulare/patent_eng/p2733_1.pdf.

16. Federal Financial Supervisory Authority 2022, *Consultation on a planned General Administrative Act regarding Futures with additional payment obligations,* accessed 29 March 2022, www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Aufsichtsrecht/Verfuegung/vf_220203_anhoerung_allgvfg_Futures_en.html.

17. Federal Financial Supervisory Authority 2018, *Big Data meets artificial intelligence: Challenges and implications for the supervision and regulation of financial services*, accessed 29 March 2022, www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.html?nn=11506564.; For a summary of the study, see: Federal Financial Supervisory Authority 2019, *Big data meets artificial intelligence – results of the consultation on BaFin's report*, accessed 29 March 2022, www.bafin.de/SharedDocs/Veroeffentlichungen/EN/BaFinPerspektiven/2019_01/bp_19-1_Beitrag_SR3_en.html.

18. German Central Bank 2020, *Money in programmable applications: Cross-sector perspectives from the German economy*, accessed 29 March 2022, www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf.

19. German Central Bank 2020, *How Can Collateral Management Benefit from DLT?: Project "Blockbaster"*, accessed 29 March 2022, www.bundesbank.de/resource/blob/823072/4d14afd4b6dbffa94a46ee52f46e99bd/mL/how-can-collateral-management-benefit-from-dlt-data.pdf.

20. German Central Bank 2019, *International Cash Conference 2019: Cash in the age of payment diversity*, accessed 29 March 2022, www.bundesbank.de/resource/blob/854150/29a4f4258f6c30e43297eec39726d8c9/mL/cash-in-the-age-of-payment-diversity-data.pdf.

21. German Central Bank 2018, *Procedural rules electronic account information* (In German), accessed 29 March 2022, www.bundesbank.de/en/tasks/payment-systems/publications/procedural-rules-electronic-account-information-626568.

22. Federal Office of Justice 2020, *Online trade in the area of conflict between consumer protection and sustainability* (In German), accessed 29 March 2022, www.bmj.de/SharedDocs/Downloads/DE/News/PM/113020_PolicyBrief.html.

23. Germatik 2021, *Whitepaper TI 2.0 – Arena für digitale Medizin* (In German), accessed 29 March 2022, www.gematik.de/media/gematik/Medien/Telematikinfrastruktur/Dokumente/gematik_Whitepaper_Arena_digitale_Medizin_TI_2.0_Web.pdf.

24. *Interoperability 2.0 based on the Health IT Interoperability Governance Regulation (IOP-Governance-Verordnung – GIGV)*, accessed 29 March 2022, www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/guv-19-lp/gigv.html.

25. Deutscher Bundestag n.d., *Committee on Education, Research and Technology Assessment*, accessed 29 March 2022, www.bundestag.de/en/committees/a18.

26. Deutscher Bundestag n.d., *Committee on Digital Affairs*, accessed 29 March 2022, www.bundestag.de/en/committees/a23.

27. Deutscher Bundestag 2021, *Draft law on the introduction of electronic proof of identity with a mobile device* (In German), accessed 29 March 2022, https://dserver.bundestag.de/btd/19/281/1928169.pdf.

28. *Law regulating the sale of things with digital elements and other aspects of the contract of sale 2021,* accessed 29 March 2022, www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Warenkaufrichtlinie.html (In German).

29. *Act implementing the Directive on certain aspects of contract law relating to the provision of digital content and digital services 2021,* accessed 29 March 2022, www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Bgbl_Digitale_Inhalte.html (In German).

30. *Act Amending the Civil Code and the Introductory Act to the Civil Code (BGB) in Implementation of the EU Directive on Better Enforcement and Modernization of Union Consumer Protection Rules and Repealing the Regulation Transferring Responsibility for the Implementation of Regulation (EC) No. 2006/2004 to the Federal Ministry of Justice and Consumer Protection* (enters into force on 28 May 2022), accessed 29 March 2022, www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Bgbl_Modernisierungsrichtlinie.html (In German).

31. *Implementation of Regulation (EC) No. 2006/2004 as the Act Amending the Civil Code and the Introductory Act to the Civil Code (BGB) in Implementation of the EU Directive on Better Enforcement and Modernization of Union Consumer Protection Rules* (enters into force on 28 May 2022), accessed 29 March 2022, www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Bgbl_Modernisierungsrichtlinie.html (In German).

India

Jhalak M. Kakkar, Shashank Mohan, Bilal Mohamed and Mira Swaminathan,
National Law University Delhi

Central Consumer Protection Authority (CCPA)

Institutional Form: Statutory authority

Responsible Minister: The Chief Commissioner, CCPA

Principal Instrument(s): *Consumer Protection (E-Commerce) Rules (2020), Consumer Protection Act (2019)*

Mandate: The CCPA regulates matters involving violation of consumer rights, misleading or false advertisements, unfair trade practices and enforces consumer rights. Since 2020, the Department of Consumer Affairs issued the *Consumer Protection (E-Commerce) Rules* to regulate marketplace e-commerce entities. The Rules seek to prevent unfair trade practices in e-commerce, protect the interest of consumers, and ensure transparency in e-commerce platforms.

Major Reports, Inquires, and Related Initiatives:

- The Consumer Protection (E-Commerce) Rules (2020): [Rules][1]

Competition Commission of India (CCI)

Institutional Form: Statutory authority

Responsible Minister: The Chairperson, CCI

Principal Instrument(s): *Competition Act (2002)*

Mandate: The CCI is responsible for promoting and sustaining competition and protecting the interests of consumers. It oversees the freedom of trade in India and eliminates practices that have adverse effects on competition. The CCI provides opinion on competition issues referred to it from statutory authorities. It also undertakes competition advocacy, promotes public awareness, and provides training on competition issues. The CCI has powers to review the actions of technology companies. In 2021, the CCI ordered an investigation into Google following allegations from news publishers of anti-competitive practices that denied fair advertising revenue to news publishers. In the same year, the CCI also invoked its powers to start an investigation against Facebook and WhatsApp, terming the proposed privacy policy update as amounting to an imposition of unfair terms and conditions upon the users.

Major Reports, Inquires, and Related Initiatives:

- Suo Moto order directing the Director General to investigate WhatsApp and Facebook's practices with regards the updated terms of service and privacy policy for WhatsApp users (2021): [CCI Order][2]
- Together We Fight Society vs. Apple Inc. & Another (2021): [Order][3]
- Discussion Paper on Blockchain Technology and Competition (2021): [Paper][4]
- Digital News Publishers Association vs. Alphabet Inc. and Others (2021): [Order][5]
- CCI Market Study on E-Commerce (2020): [Key Findings and Observations]
- Kshitiz Arya and another vs. Google LLC and others (2020): [Order][6]
- XYZ vs. Alphabet Inc. and Others (2020): [Order][7]
- Mr Umar Javeed and Others vs. Google LLC and Others (2018): [Order][8]

Department for Promotion of Industry and Internal Trade (DPIIT)

Institutional Form: Department within a Federal Government Ministry

Responsible Minister: The Minister of Commerce and Industry

Principal Instrument(s): Not applicable

Mandate: The DPIIT is responsible for determining the industrial policy and handles matters related to foreign direct investment. It also promotes investment for industrial development. The DPIIT, through the Office of the Controller General of Patents, Designs and Trade Marks, administers patent and intellectual property legislation. Since 2018, the DPIIT has oversight of matters relating to e-commerce and released a Draft National e-Commerce Policy that proposed setting up a legal and technological framework for restrictions on cross-border data flow and specific conditions regarding collection and processing of sensitive data.

Major Reports, Inquires, and Related Initiatives:

- Draft National e-Commerce Policy (2019): [Policy][9]
- Draft Copyright (Amendment) Rules (2019): [Document][10]

Ministry of Commerce and Industry, Directorate-General for Foreign Trade (DGFT)

Institutional Form: Department under a Federal Ministry

Responsible Minister: The Minister of Commerce and Industry

Principal Instrument(s): *The Foreign Trade (Development & Regulations) Act (1992)*

Mandate: The DGFT regulates and promotes foreign trade. It formulates India's Foreign Trade Policy under the statutory authorisation provided by Section 5 of the *Foreign Trade (Development and Regulation) Act (1992)*. The policy regulates the import and export of certain types of technologies.

Major Reports, Inquires, and Related Initiatives:

- Gazette Notification prohibiting foreign drones (2022): [Gazette Notification][11]

Department of Revenue (DoR)

Institutional Form: Department within a Federal Government Ministry

Responsible Minister: The Minister of Finance

Principal Instrument(s): *Goods and Services Tax Act (2017), Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act (2015), Prevention of Money Laundering Act (2002), Foreign Exchange Management Act (1999), Income Tax Act (1961)*

Mandate: The DoR controls matters relating to the direct and indirect union taxes through the Central Board of Direct Taxes (CBDT) and the Central Board of Indirect Taxes and Customs (CBIC). The DoR investigates economic offences and enforces economic laws. While the CBDT is responsible for the administration of direct tax laws through the Income Tax Department, the CBIC is tasked with the formulation of policy concerning levy and collection of customs, central excise duties, central goods and services tax and the Integrated Goods and Services Tax. The growth of e-commerce has led to the DoR extending its regulation. This is shown in the CBDT's notification of the *Equalisation Levy (Amendment) Rules* to extend the levy to include the e-commerce sector. Additionally, in the recent Parliament Budget Session, the Finance Minister announced a 30 per cent tax on any direct income from the transfer of any virtual digital asset.

Major Reports, Inquiries, and Related Initiatives:

- The Finance Bill (2022): [Bill] [Budget Speech][12]
- The Finance Act (2020): [Gazette Notification][13]
- Equalisation Levy (Amendment) Rules (2020): [Gazette Notification][14]

*Election Commission of India (ECI)

Institutional Form: Constitutional authority

Responsible Minister: The Chief Election Commissioner, ECI

Principal Instrument(s): *Article 324 of the Indian Constitution (1950*)

Mandate: The ECI is responsible for administering election processes for unions and states in India, as well as administering elections to the Lok Sabha, Rajya Sabha, State Legislative Assemblies in India and to the offices of the President and Vice President. In 2019, the ECI formed a committee to review and suggest modifications in the provisions of section 126 and other sections of the R*epresentation of the People Act (1951)*, specifically regarding new digital technologies. The ECI also issued cyber security guidelines to states, which included a special audit of ICT applications, cyber hygiene of electoral staff, and detailed application and infrastructure level guidelines.

Major Reports, Inquires, and Related Initiatives:

- Committee to examine the provisions of Section 126 of Representation of People Act, 1951 (2019): [Order][15]
- IAMAI's Voluntary Code of Ethics for Elections (2019): [Code][16]

Insurance Regulatory and Development Authority of India (IRDAI)

Institutional Form: Statutory authority

Responsible Minister: Chairperson, IRDAI

Principal Instrument(s): *Insurance Regulatory and Development Authority Act (1999)*

Mandate: The IRDAI regulates and licenses India's insurance and reinsurance industries. The IRDAI issues guidance to regulated entities to protect financial systems. The IRDAI created a regulatory sandbox to allow fintech organisations to test products and services in a controlled phase. In 2021, in light of increasing cyber-attacks in the financial sector, the IRDAI formed a committee to review the provisions and scope of the *Information and Cyber Security Guidelines (2017)*.

Major Reports, Inquires, and Related Initiatives:

- Amendments to the Guidelines on Information and Cyber Security for Insurers (2020): [Amendments][17]
- Report of the Working Group (WG) for insurance of Remotely Piloted Aircraft System (RAPS) Drone Technology (2020): [Exposure Draft][18]
- Insurance Regulatory and Development Authority of India (Regulatory Sandbox) Regulations (2019): [Gazette Notification][19]
- Report of Committee on Regulatory Sandbox in Insurance Sector in India (2019): [Report][20]

Ministry of Electronics and Information Technology (MeitY)

Institutional Form: Ministry under the Government of India

Responsible Minister: The Minister of Electronics and Information Technology

Principal Instrument(s): *Information Technology Act (2000)*

Mandate: The MeitY promotes the sustainable growth of electronics, IT and IT-enabled services industries, and enhances India's e-governance systems. It adopts a multipronged approach that includes developing human resources, promoting research, development and innovation, and enhancing efficiency through digital services. The MeitY has oversight of statutory organisations such as the Indian Computer Emergency Response Team, the Unique Identification Authority of India, and the Controller of Certifying Authorities. It is also responsible for enforcing the provisions of the *IT Act* and making subordinate legislation under it. In the last two years, the MeitY has invoked its blocking powers under section 69A of the *IT Act* to block a host of apps on the basis that they were engaging in activities that undermined the integrity of India. In 2021, the MeitY introduced the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021)* to prescribe rules and due diligence requirements for online intermediaries and digital media entities. The rules were developed along with the Ministry of Information and Broadcasting.

Major Reports, Inquires, and Related Initiatives:

- Draft India Data Accessibility & Use Policy (2022 - ongoing): [Paper][21]
- Draft India Enterprise Architecture (InDEA) Framework 2.0 (2022): [Paper][22]
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021): [Gazette Notification][23]
- National Strategy on Blockchain (2021): [Paper][24]
- Expert Committee Report on Non-Personal Data Governance Framework (2020): [Report][25]
- Draft Data Centre Policy (2020): [Paper][26]
- Consultation Paper on Strategy for National Digital Open Ecosystems (NODE) (2020): [Whitepaper][27]
- Notification of the Aarogya Setu Data Access and Knowledge Sharing Protocol (2020): [Guidelines][28]
- MeitY issues order for blocking apps under Section 69A of the Information Technology Act (2020): [Press Release][29]
- Committee of Experts' Report on Data Protection Bill (2018): [Report][30]

Ministry of Information and Broadcasting (MIB)

Institutional Form: Ministry under the Government of India

Responsible Minister: The Minister of Information and Broadcasting

Principal Instrument(s): *The Sports Broadcasting Signals [Mandatory Sharing with Prasar Bharati] Act (2007), The Sports Broadcasting Signals (Mandatory Sharing with Prasar Bharati) Act (2007), Information Technology Act (2000), The Cable Television Networks [Regulation) Act (1995), The Press Council Act (1978), The Cinematograph Act (1952)*

Mandate: The MIB regulates content of private satellite channels and networks of multi-system operators and local cable operators. The MIB's oversight includes digital news publishers and over-the-top (internet-based) platforms. The MIB requires online news and current affairs publishers to provide information about their content and complete periodic compliance reports. The MIB has emergency powers to block apps and certain social media accounts that are found to be 'detrimental to the sovereignty and integrity of India, security of the State, and public order'.

Major Reports, Inquires, and Related Initiatives:

- Ministry of Information and Broadcasting orders blocking of Apps, website and social media accounts linked to banned organisation Sikhs For Justice (2022): [Press Release][31]
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021): [Rules][32]

National Critical Information Infrastructure Protection Centre (NCIIPC)

Institutional Form: Statutory authority

Responsible Minister: Prime Minister's Office

Principal Instrument(s): *Information Technology Act (2000)*

Mandate: The NCIIPC is responsible for protecting critical information infrastructure from unauthorised access, modification, use, disclosure, disruption, incapacitation, or distraction. This is done through raising information security awareness among all stakeholders. The NCIIPC is empowered under Section 70A of the *Information Technology Act (2000)* as the national nodal agency and consults with stakeholders to issue guidelines, advisories, and vulnerabilities or audit notes relating to the protection of critical information infrastructure. It has powers to call for information and give directions to the sectors that affect its security.

Major Reports, Inquires, and Related Initiatives:

- Cyber Security Audit Baseline Requirements (2020): [Guidelines][33]
- Guidelines for Identification of Critical Information Infrastructure (2019): [Guidelines][34]

*National Health Authority (NHA)

Institutional Form: Office within a Federal Government Ministry

Responsible Minister: The Chief Executive Officer, NHA

Principal Instrument(s): Not applicable

Mandate: The NHA implements India's public health insurance and assurance scheme - *Ayushman Bharat Pradhan Mantri Jan Arogya Yojana* - and manages the technological infrastructure and implementation of the National Digital Health Mission. The NHA issues guidelines and policies to build India's National Digital Health Ecosystem. The NHA proposed a draft Health Data Retention Policy in 2021 which detailed the use of data within the National Digital Health Mission Ecosystem.

Major Reports, Inquires, and Related Initiatives:

- Consultation Paper on Proposed Health Data Retention Policy (2021): [Paper][35]
- Consultation Paper on Unified Health Interface (2021): [Paper][36]
- Consultation Paper on Health Facility Registry (2021): [Paper][37]
- Consultation Paper on Healthcare Professionals Registry (2021): [Paper][38]
- Health Data Management Policy (2020): [Policy][39]

National Human Rights Commission (NHRC)

Institutional Form: Statutory authority

Responsible Minister: The Chairperson, NHRC

Principal Instrument(s): *Protection of Human Rights Act (PHRA) (1993)*

Mandate: The NHRC promotes and protects human rights in India. It has various functions that include establishing a commission for enquiring into human rights violations, studying international frameworks on human rights (including digital rights) and studying the accessibility of digital infrastructures in India. For example, the NHRC provides digital facilities for online access to education for all children and ensures Child Welfare Committees and Juvenile Justice Boards proceedings are conducted using digital modes. While the NHRC is empowered to carry out investigations, it cannot enforce its decisions and has advisory powers only.

Major Reports, Inquires, and Related Initiatives: None issued

Reserve Bank of India (RBI)

Institutional Form: Statutory authority

Responsible Minister: RBI Governor

Principal Instrument(s): *Reserve Bank of India Act (1934)*

Mandate: The RBI is the regulator and supervisor of India's financial system. It prescribes broad parameters of banking operations for the banking and financial systems. It maintains public confidence in the systems, protects depositor interests, and provides cost-effective banking services to the public. In recent years, the RBI has explored measures to regulate FinTech and related areas. In 2018, an inter-regulatory Working Group released a report on 'FinTech and Digital Banking' to review and re-orient the existing regulatory framework. Recommendations from the report resulted in the RBI operating a regulatory sandbox to enable responsible innovation in financial services and increase efficiency of services. The RBI has strengthened its cyber security capabilities and has issued a policy paper, 'Technology Vision for Cyber security for Urban Co-operative Banks (UCBs)'.

Major Reports, Inquires, and Related Initiatives:

- Action against Paytm Payments Bank Ltd under section 35 A of the Banking Regulation Act, 1949 (2021): [Press Release][40]
- Enabling Framework for Regulatory Sandbox (2021): [Report][41]
- Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps (2021): [Report][42]
- Technology Vision for Cyber security for Urban Co-operative Banks – 2020–2023 (2020): [Vision Document][43]
- Report of the Working Group on FinTech and Digital Banking (2018): [Report][44]

Securities and Exchange Board (SEBI)

Institutional Form: Statutory authority

Responsible Minister: The Chairperson, SEBI Board

Principal Instrument(s): *Securities and Exchange Board of India Act (1992)*

Mandate: The SEBI protects the interests of investors in securities by prohibiting and preventing unfair trade practices through the regulation of the securities markets. With the use of online platforms for trading and a rise in 'new-age technology companies' opting for initial public offerings, SEBI plays a role in the regulation of practices that are shaped by these emerging technologies. In December 2021, SEBI sought comments from stakeholders on the practice of algorithmic trading by retail investors. In June 2020, SEBI imposed an INR 150,000 fine on an individual for circulating Unpublished Price Sensitive Information (UPSI) through WhatsApp.

Major Reports, Inquires, and Related Initiatives:

- Consultation Paper on Algorithmic Trading by Retail Investors (2021): [Paper][45]
- Consultation Paper on Review of Certain Aspects of Public Issue Framework Under SEBI (Issue of Capital and Disclosure Requirements) Regulations (2021): [Paper][46]
- Discontinuation of usage of pool accounts for transactions in units of Mutual Funds on the Stock Exchange Platforms (2021): [Circular][47]
- Adjudication Order in the matter of circulation of UPSI through WhatsApp messages in the scrip of Ambuja Cements Ltd. (2020): [Order][48]
- New Framework For Tech Companies To Issue DVR Shares And Undertake IPOs (2019): [Framework][49]
- Consultation Paper on Disclosures for 'Basis of Issue Price' section in offer document under SEBI (Issue of Capital and Disclosure Requirements), Regulations (2019): [Paper]
- Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants (2018): [Document][50]

Telecom Regulatory Authority of India (TRAI)

Institutional Form: Statutory authority

Principal Instrument(s): *Telecom Regulatory Authority of India Act (1997)*

Responsible Minister: The Chairperson, TRAI

Mandate: The TRAI regulates India's telecommunications services and protects the interests of service providers and consumers in the telecommunications sector. The TRAI provides a fair and transparent policy environment that promotes a level playing field and facilitates fair competition. The directions, orders and regulations issued by TRAI cover a wide range of subjects including tariffs, inter-connectivity, and quality of service. In August 2021, TRAI released a report, 'Enabling Unbundling of Different Layers Through Differential Licensing', which included a set of recommendations to enhance the sharing of network resources, reduction of cost, investment, and strengthening of the service delivery, especially in the backdrop of 5G service uptake.

Major Reports, Inquires, and Related Initiatives:

- Recommendations on Enabling Unbundling of Different Layers Through Differential Licensing (2021): [Recommendations][51]
- Consultation Paper on Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India (2021): [Recommendations][52]
- Consultation Paper on "Market Structure/Competition in cable TV services" (2021): [Paper][53]
- Recommendations on Regulatory Framework for Over-The-Top (OTT) Communication Services (2020): [Recommendations][54]

Unique Identification Authority of India (UIDAI)

Institutional Form: Statutory authority

Responsible Minister: The Minister of Electronics and Information Technology

Principal Instrument(s): *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act (2016)*

Mandate: The UIDAI issues unique identification numbers (named "Aadhaar") to all residents of India for the purpose of identity authentication. It administers the Aadhaar system through operating and managing policy at all stages of the Aadhaar life cycle. This encompasses developing the policy, procedures, and systems for issuing Aadhaar numbers as well as ensuring appropriate authentication and security of identity information. The UIDAI issues binding directions and rules for entities within the Aadhaar ecosystem. The UIDAI has the power to create subordinate legislation and exercise quasi-judicial powers to suspend enrolment agencies and registrars.

Major Reports, Inquiries, and Related Initiatives:

- Guidelines on use of Aadhaar under section 7 of the Aadhaar Act 2016 (as amended by the Aadhaar and Other Laws (Amendment) Act, 2019) by the State Governments (2019): [Document][55]
- Circular 6 of 2019 – Implementation of Virtual ID, UID Token and Limited e -KYC (2019): [Document][56]

Ongoing Parliamentary Committees, Inquiries, or Legislative Proposals (not previously referred to):

- Parliamentary Standing Committee on Communications and IT Report on 'Suspension Of Telecom Services/Internet And Its Impact'(2021): [Report][57]
- Parliamentary Joint Committee Report on the Personal Data Protection Bill, 2019 (2021): [Report]
- The DNA Technology (Use and Application) Regulation Bill (2019): [Draft Policy][58]
- Report of the Committee to propose specific actions to be taken in relation to Virtual Currencies (2019): [Report][59]

Endnotes (India)

1. *The Consumer Protection (E-Commerce) Rules*, The Gazette of India, accessed 29 March 2022, https://consumeraffairs.nic.in/sites/default/files/E%20commerce%20rules.pdf.

2. Competition Commission of India 2021, *Suo Moto order directing the Director General to investigate WhatsApp and Facebook's practices with regards the updated terms of service and privacy policy for WhatsApp users*, accessed 29 March 2022, www.cci.gov.in/sites/default/files/SM01of2021_0.pdf.

3. Competition Commission of India 2021, *Together We Fight Society vs. Apple Inc. & Another*, accessed 29 March 2022, www.cci.gov.in/sites/default/files/24-of-2021.pdf.

4. Competition Commission of India 2021, *Discussion paper on blockchain technology and competition*, accessed 29 March 2022, www.cci.gov.in/sites/default/files/whats_newdocument/Blockchain.pdf.

5. Competition Commission of India 2021, *Digital News Publishers Association vs. Alphabet Inc. and Others*, accessed 29 March 2022, www.cci.gov.in/sites/default/files/order_41_2021.pdf.

6. Competition Commission of India 2020, *Market Study on e-Commerce in India: Key Findings and Observations,* accessed 29 March 2022, www.cci.gov.in/sites/default/files/whats_newdocument/Market-study-on-e-Commerce-in-India.pdf.

7. Competition Commission of India 2020, *XYZ vs. Alphabet Inc. and Others (2020)*, accessed 29 March 2022, www.cci.gov.in/sites/default/files/07-of-2020.pdf.

8. Competition Commission of India 2018, *Mr. Umar Javeed & Others vs. Google LLC & Others*, 29 March 2022, www.cci.gov.in/sites/default/files/39-of-2018.pdf.

9. Department for Promotion of Industry and Internal Trade 2019, *Draft National e-Commerce Policy: India's Data for India's Development*, accessed 29 March 2022, https://dpiit.gov.in/sites/default/files/Draft-National_e-commerce_Policy_23February2019.pdf.

10. Department for Promotion of Industry and Internal Trade 2019, *Draft Copyright (Amendment) Rules,* The Gazette of India, accessed 29 March 2022, www.ipindia.gov.in/writereaddata/Portal/News/529_1_pdfgazette.pdf.

11. Ministry of Commerce and Industry, Directorate General for Foreign Trade 2022, *Notification prohibiting foreign drones*, The Gazette of India, accessed 29 March 2022, www.medianama.com/wp-content/uploads/2022/02/233253.pdf.

12. *The Finance Bill, 2022*, accessed 29 March 2022, www.incometax-india.gov.in/budgets%20and%20bills/2022/finance_bill.pdf. See also: Government of India 2022, *Speech of Nirmala Sitharaman, Minister of Finance*, accessed 29 March 2022, www.indiabudget.gov.in/doc/budget_speech.pdf.

13. *The Finance Act, 2020*, The Gazette of India, accessed 29 March 2022, https://egazette.nic.in/WriteReadData/2020/218938.pdf.

14. *Equalisation Levy (Amendment) Rules*, The Gazette of India, accessed 29 March 2022, www.incometaxindia.gov.in/communications/notification/notification_87_2020.pdf.

15. Committee to examine the provisions of Section 126 of Representation of People Act, 1951 (2019) accessed 29 March 2022, https://archive.org/details/ecicommitteereportsection126/mode/2up.

16. Internet and Mobile Association of India 2019, *Voluntary Code of Ethics for the General Election 2019*, accessed 29 March 2022, https://static.pib.gov.in/WriteReadData/userfiles/IAMAI-ECI%20VCE.pdf. See also: Press Information Bureau 2019, *Report of the Committee on Section 126 of the Representation of the People Act, 1951 Submitted to The Commission*, press release, accessed 8 April 2022, https://pib.gov.in/newsite/PrintRelease.aspx?relid=187412.

17. Insurance Regulatory and Development Authority of India 2020, *Amendments to the Guidelines on Information and Cyber Security for Insurers,* accessed 30 March 2022, www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo4315&flag=1.

18. Insurance Regulatory and Development Authority of India 2020, *Report of the Working Group (WG) for insurance of Remotely Piloted Aircraft System (RAPS) Drone Technology*, accessed 30 March 2022, www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo4244&flag=1.

19. Insurance Regulatory and Development Authority of India 2019, *Insurance Regulatory and Development Authority of India (Regulatory Sandbox) Regulations,* The Gazette of India, accessed 29 March 2022, www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/Regulations/Consolidated/IRDAI%20(Regulatory%20Sandbox)%20Regulations2019.pdf.

20. Insurance Regulatory and Development Authority of India 2019, *Report of Committee on Regulatory Sandbox in Insurance Sector in India*, accessed 29 March 2022, www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo3726&flag=1.

21. Ministry of Electronics and Information Technology 2022, *Draft India Data Accessibility & Use Policy 2022*, accessed 29 March 2022, www.meity.gov.in/content/draft-india-data-accessibility-use-policy-2022

22. Ministry of Electronics and Information Technology 2022, *Draft India Enterprise Architecture (InDEA) Framework 2.0*, accessed 29 March 2022, www.meity.gov.in/writereaddata/files/InDEA%202_0%20Report%20Draft%20V6%2024%20Jan%2022_Rev.pdf

23. Ministry of Electronics and Information Technology 2021, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, The Gazette of India, accessed 29 March 2022, www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.

24. Ministry of Electronics and Information Technology 2021, *National Strategy on Blockchain*, accessed 29 March 2022, www.meity.gov.in/writereaddata/files/NationalStrategyBCT_%20Jan2021_final.pdf. See also the updated strategy: Ministry of Electronics and Information Technology 2021, *National Strategy on Blockchain: Towards Enabling Trusted Digital Platforms*, accessed 29 March 2022, www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf.

25. Ministry of Electronics and Information Technology 2020, *Report by the Committee of Experts on Non-Personal Data Governance Framework*, accessed 29 March 2022, https://ourgovdotin.files.wordpress.com/2020/12/revised-report-kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf.

26. Ministry of Electronics and Information Technology 2020, *Draft Data Centre Policy*, accessed 29 March 2022, www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf.

27. Ministry of Electronics and Information Technology 2020, *Strategy for National Digital Open Ecosystems (NODE) Consultation Whitepaper*, accessed 29 March 2022, https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf.

28. Ministry of Electronics and Information Technology 2020, *Notification of the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020 in light of the COVID-19 pandemic*, accessed 29 March 2022, www.meity.gov.in/writereaddata/files/Order_for_DATA_SHARING_PROTOCOL_OF_AAROGYASETU.pdf.

29. Ministry of Electronics and Information Technology 2020, *Government of India blocks 43 mobile apps from accessing by users in India: MEITY issues order for blocking apps under Section 69A of the Information Technology Act*, accessed 29 March 2022, www.pib.gov.in/PressReleasePage.aspx?PRID=1675335.

30. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna n.d., *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, Ministry of Electronics and Information Technology (MeitY), accessed 29 March 2022, www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

31. Ministry of Information and Broadcasting 2022, *Ministry of Information and Broadcasting orders blocking of Apps, website and social media accounts linked to banned organization Sikhs For Justice*, press release, accessed 29 March 2022, https://pib.gov.in/PressReleasePage.aspx?PRID=1800212.

32. Ministry of Information and Broadcasting 2021, *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules*, The Gazette of India, accessed 29 March 2022, www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.

33. National Security Council Secretariat 2020, *Cyber Security Audit Baseline Requirements*, accessed 29 March 2022, https://nciipc.gov.in/documents/CyberSecurityAuditbaseline.pdf.

34. National Critical Information Infrastructure Protection Centre 2019, *Guidelines for Identification of Critical Information Infrastructure*, accessed 29 March 2022, https://nciipc.gov.in/documents/Guidelines_for_Identification_of_CII.pdf.

35. National Health Authority 2021, *Consultation Paper on Proposed Health Data Retention Policy*, accessed 29 March 2022, accessed 29 March 2022, https://abdm.gov.in/assets/uploads/consultation_papersDocs/Consultation_Paper_on_Health_Data_Retention_Policy_21.pdf.

36. National Health Authority 2021, *Consultation Paper on Unified Health Interface*, accessed 29 March 2022, https://abdm.gov.in/assets/uploads/consultation_papersDocs/UHI_Consultation_Paper.pdf.

37. National Health Authority 2021, *Consultation Paper on Health Facility Registry*, accessed 29 March 2022, https://abdm.gov.in/assets/uploads/consultation_papersDocs/Consultation-Paper-on-Health-Facility-Registry.pdf.

38. National Health Authority 2021, *Consultation Paper on Healthcare Professionals Registry*, accessed 29 March 2022, https://abdm.gov.in/assets/uploads/consultation_papersDocs/Consultation-Paper-on-Healthcare-Professionals-Registry.pdf.

39. National Health Authority 2020, *Health Data Management Policy*, accessed 29 March 2022, https://abdm.gov.in/publications/policies_regulations/health_data_management_policy.

40. Reserve Bank of India 2021, *Action against Paytm Payments Bank Ltd under section 35 A of the Banking Regulation Act, 1949*, press release, accessed 29 March 2022, www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=53405.

41. Reserve Bank of India 2021, *Enabling Framework for Regulatory Sandbox*, accessed 29 March 2021, www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1187#C2.

42. Reserve Bank of India 2021, *Report of the Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps*, accessed 29 March 2022, www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1189.

43. Reserve Bank of India 2020, *'Technology Vision for Cyber Security' for Urban Co-operative Banks – 2020-2023*, accessed 29 March 2022, www.rbi.org.in/Scripts/PublicationVisionDocuments.aspx?Id=1159.

44. Reserve Bank of India 2018, *Report of the Working Group on FinTech and Digital Banking*, accessed 29 March 2022, https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=892.

45. Securities and Exchange Board 2021, *Consultation Paper on Algorithmic Trading by Retail Investors*, accessed 29 March 2022, www.sebi.gov.in/reports-and-statistics/reports/dec-2021/consultation-paper-on-algorithmic-trading-by-retail-investors_54515.html.

46. Securities and Exchange Board 2021, *Consultation Paper on Review of certain aspects of Public issue framework under SEBI (Issue of Capital and Disclosure Requirements) Regulations, 2018*, accessed 29 March 2022, www.sebi.gov.in/reports-and-statistics/reports/nov-2021/consultation-paper-on-review-of-certain-aspects-of-public-issue-framework-under-sebi-issue-of-capital-and-disclosure-requirements-regulations-2018_53983.html.

47. Securities and Exchange Board 2021, *Discontinuation of usage of pool accounts for transactions in units of Mutual Funds on the Stock Exchange Platforms*, accessed 29 March 2022, www.sebi.gov.in/legal/circulars/oct-2021/discontinuation-of-usage-of-pool-accounts-for-transactions-in-units-of-mutual-funds-on-the-stock-exchange-platforms_53104.html.

48. Securities and Exchange Board 2020, *Adjudication Order in respect of Neeraj Kumar Agarwal and Shruti Vishal Vora in the matter of circulation of UPSI through WhatsApp messages in the scrip of Ambuja Cements Ltd.,* accessed 29 March 2022, www.sebi.gov.in/enforcement/orders/apr-2020/adjudication-order-in-respect-of-neeraj-kumar-agarwal-and-shruti-vishal-vora-in-the-matter-of-circulation-of-upsi-through-whatsapp-messages-in-the-scrip-of-ambuja-cements-ltd-_46613.html.

49. Securities and Exchange Board 2019, *New Framework for Tech Companies to Issue DVR Shares and Undertake IPOs*, accessed 29 March 2022, www.sebi.gov.in/media/press-releases/jun-2019/sebi-board-meeting_43417.html.

50. Securities and Exchange Board 2018, *Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants*, accessed 29 March 2022, www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html.

51. Telecom Regulatory Authority of India 2021, *Recommendations on 'Enabling Unbundling of Different Layers Through Differential Licensing*, accessed 29 March 2022, www.trai.gov.in/sites/default/files/Recommendation_19082021_0.pdf.

52. Telecom Regulatory Authority of India 2021, *Consultation Paper on 'Regulatory Framework for Promoting Data Economy Through Establishment of Data Centres, Content Delivery Networks, and Interconnect Exchanges in India*, accessed 29 March 2022, www.trai.gov.in/sites/default/files/CP_16122021.pdf.

53. Telecom Regulatory Authority of India 2021, *Consultation Paper on ''Market Structure/Competition in cable TV services"*, accessed 29 March 2022, www.trai.gov.in/sites/default/files/CP_25102021.pdf.

54. Telecom Regulatory Authority of India 2020, *Recommendations on Regulatory Framework for Over-The-Top [OTT) Communication Services*, accessed 29 March 2022, https://trai.gov.in/sites/default/files/Recommendation_14092020_0.pdf.

55. Unique Identification Authority of India 2019, *Guidelines on use of Aadhaar under section 7 of the Aadhaar Act 2016 (as amended by the Aadhaar and Other Laws (Amendment) Act, 2019) by the State Governments*, accessed 29 March 2022, https://uidai.gov.in/images/UIDAI_Circular_Guidelines_on_use_of_Aadhaar_section_7_of_the_Aadhaar_Act_2016_by_the_State_Governments_25Nov_19.pdf.

56. Unique Identification Authority of India 2019, *Circular 6 of 2019 – Implementation of Virtual ID, UID Token and Limited e -KYC*, accessed 29 March 2022, https://uidai.gov.in/images/resource/Circular_No_06_of_2019_Implementation_of_VID_and_UID_Token_and_Limited_eKYC_06062019.pdf.

57. Parliamentary Standing Committee on Communications and IT 2021, *Report on 'Suspension Of Telecom Services/Internet And Its Impact'*, accessed 29 March 2022, http://164.100.47.193/lsscommittee/Communications%20and%20Information%20Technology/17_Communications_and_Information_Technology_26.pdf.

58. *The DNA Technology (Use and Application) Regulation Bill (2019),* accessed 29 March 2022, http://164.100.47.4/billstexts/lsbilltexts/asintroduced/128_%202019_LS_eng.pdf.

59. Committee of Virtual Currencies 2019, *Report of the Committee to propose specific actions to be taken in relation to Virtual Currencies (2019)*, accessed 29 March 2022, https://prsindia.org/files/bills_acts/bills_parliament/1970/Report%20of%20the%20Inter-Ministerial%20Committee%20on%20Virtual%20Currencies.pdf.

Japan

Hiroki Habuka, University of Tokyo

Consumer Affairs Authority (CAA)

Institutional Form: Administrative agency

Responsible Minister: The Minister of State for Consumer Affairs and Food Safety

Principal Instrument(s): *Act for the Protection of Consumers who use Digital Platforms (2021)*[1], *Consumer Safety Act (2009), Consumer Contract Act (2000)*

Mandate: The CAA protects and promotes consumer rights and interests by shaping consumer policy, requesting government members to take appropriate actions, and preventing deceptive and unfair business practices through law enforcement. The CAA led a review of consumer protection in business-to-consumer transactions using digital platforms. This resulted in the *Act for the Protection of Consumers who use Digital Platforms.* This act places obligations on digital platform, providers to implement measures that enable smooth communication between sellers and consumers, investigate complaints by consumers regarding transactions on the digital platform and request sellers to provide information on their identity.

Major Reports, Inquiries, and Related Initiatives:

- Outline of the Act for the Protection of Consumers who use Digital Platforms (2021): [Summary] (In Japanese)[2]
- Final report by the Study Group on Improvements of Consumer Protections Involving Digital Platforms (2021): [Report] (In Japanese)[3]

*Digital Extraordinary Administrative Advisory Committee (DEAAC)

Institutional Form: Provisional Commission

Responsible Minister: The Prime Minister

Principal Instrument(s): *Digital Principles for Structural Reform (2021)*

Mandate: The DEAAC is a special committee established under the Prime Minister to examine and implement cross-cutting agendas related to digital reform, regulatory reform, and administrative reform in an integrated manner. The DEAAC will review more than 40,000 laws, ordinances, notices, and notifications, following the Digital Principles for Structural Reform, and promote the digitalisation of more than 20,000 administrative procedures.

Major Reports, Inquiries, and Related Initiatives:

- Digital Principles for Structural Reform (2021): [Report] (In Japanese)[4]

Headquarters for Digital Market Competition (HDMC)

Institutional Form: Headquarters under the Cabinet

Responsible Minister: The Prime Minister

Principal Instrument(s): *Act on Improving Transparency and Fairness of Digital Platforms (TFDPA) (2020)*[5]

Mandate: The HDMC is composed of experts with diverse and high-level knowledge to address the issues in the digital markets, including those caused by digital platforms. It coordinates policies of various organizations in the government, including the Japan Fair Trade Commission, the Ministry of Economy, Trade and Industry, the Ministry of Internal Affairs and Communications and the Person Information Protection Commission to tackle challenges in the cross-sectional approach. The HDMC has worked on competition reviews on digital markets, especially ones of e-commerce, app store and digital advertising.

Major Reports, Inquiries, and Related Initiatives:

- Evaluation of Competition in the Digital Advertising Market - Final Report (2021): [Summary] [Report] (In Japanese)[6]
- Report on Medium-Term Vision on Competition in the Digital Market (2020): [Summary] [Report] (In Japanese)[7]

Financial Services Agency (FSA)

Institutional Form: Administrative agency

Responsible Minister: The Minister of State for Financial Services

Principal Instrument(s): *Payment Services Act (Act No. 59 of 2009), Act on Sales, etc. of Financial Instruments (Act No. 101 of 2000), Financial Instruments and Exchange Act (Act No. 25 of 1948)*

Mandate: The FSA is responsible for ensuring the stability of Japan's financial system, the protection of depositors, insurance policy holders and securities investors, and smooth finance. It delivers stability through such measures as planning and policymaking in the financial system, inspection, and supervision of private-sector financial institutions, and surveillance of securities transactions. The FSA leads the discussion on regulations governing crypto assets. The 2019 amendments to the *Payment Services Act* redefined assets previously regulated as 'virtual currency' to 'crypto assets' and reformed the regulations to include a trust requirement for deposits and an obligation to address crypto-asset leakage risks. The *Financial Instruments and Exchange Law* regarding initial coin offering was also amended in the same year.

Major Reports, Inquiries, and Related Initiatives:

- Interim Report by the Study Group on Digital and Decentralized Finance (2021): [Report] (In Japanese)[8]
- Research report on measures to promote innovative technology fields and RegTech/SupTech in the financial sector (2020): [Report] (In Japanese)[9]

Japan Fair Trade Commission (JFTC)

Institutional Form: Independent authority

Responsible Minister: The Prime Minister

Principal Instrument(s): *Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (Antimonopoly Act) (1947)*[10]

Mandate: The JFTC promotes fair and free competition and the development of a democratic national economy. JFTC's activities in digital markets include investigating digital platform companies under the *Antimonopoly Act,* reviewing mergers involving digital platforms, revising guidelines on merger review and abuse of superior bargaining position, and conducting fact-finding surveys on the app market, e-commerce markets and digital advertising markets.

Major Reports, Inquiries, and Related Initiatives:

- Final Report Regarding Digital Advertising (2021): [Press Release] [Report][11]
- Amendments of the "Guidelines to Application of the Antimonopoly Act Concerning Review of Business Combination" and the "Policies Concerning Procedures of Review of Business Combination" (2019): [Press Release] [Guidelines 1, 2][12]
- Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information (JFTC Guidelines) (2019): [Press Release] [Guidelines][13]
- Report regarding trade practices on digital platforms (Business-to-Business transactions on online retail platform and app store) (2019): [Press Release] [Report][14]

*Japan Virtual and Crypto assets Exchange Association (JVCEA)

Institutional Form: Self-regulatory body

Responsible Minister: Not applicable

Principal Instrument(s): *JVCEA's Basic guidelines for self-regulation (2018), Rules and Guidelines for the Handling of Crypto Assets (2018), Rules and Guidelines for the Management of Users' Property Pertaining to the Crypto Asset Exchange Business (2018), Rules and Guidelines for Solicitation and Advertisement of Crypto Asset Exchange Business (2018)*

Mandate: The JVCEA is a self-regulatory organization for crypto-asset exchange business and crypto-asset related derivatives trading business. The JVCEA's objectives are to ensure appropriate and smooth implementation of crypto-asset exchange business and crypto-asset related derivatives trading business conducted by its members, and to contribute to their sound development and protection of users and investors. Based on these objectives, the JVCEA establishes self-regulatory rules, conducts inspections of its members, and provides guidance, recommendations, and disciplinary actions to its members.

Major Reports, Inquiries, and Related Initiatives:

- Basic guidelines for self-regulation (2020): [Guidelines] (In Japanese)[15]
- Rules and Guidelines for the Handling of Crypto Assets (2020): [Guidelines] (In Japanese)[16]
- Rules and Guidelines for the Management of Users' Property Pertaining to the Crypto Asset Exchange Business (2020): [Guidelines] (In Japanese)[17]
- Rules and Guidelines for Solicitation and Advertisement of Crypto Asset Exchange Business (2020): [Guidelines] (In Japanese)[18]

Ministry of Economy, Trade and Industry, Digital Market Policy Office (METI-DMPO)

Institutional Form: Office in a ministry

Responsible Minister: The Minister of Economy, Trade and Industry

Principal Instrument(s): *Guidelines for Measures Taken by Specified Digital Platform Providers to Facilitate Mutual Understanding with Platform Users (2021), Act on Improving Transparency and Fairness of Digital Platforms (TFDPA) (2020)* [19]

Mandate: The METI-DMPO enforces the *TFDPA*, a regulation which requires 'specified platform providers' to disclose their terms and conditions, develop procedures and systems, and submit a report every fiscal year on the measures and businesses that they have conducted to improve the transparency and fairness between digital platforms and business users.* The METI-DMPO is responsible for reviewing the platform operations under the submitted annual report and publicising the assessment results. The METI-DMPO refers cases to the Japan Fair Trade Commission if it finds the digital platforms could be in violation of the *Antimonopoly Act*.

Major Reports, Inquiries, and Related Initiatives:

- Review on business conducts of specified digital platforms (to come in mid-2022): [METI's Webpage][20]
- Interpretative Guidelines on Electronic Commerce and Information Property Trading in March 2002 (Latest amendment was in August 2020): [Guidelines] (In Japanese)[21]

Ministry of Economy, Trade and Industry, Trade Control Department (METI-TCD)

Institutional Form: Department in a Ministry

Responsible Minister: The Minister of Economy, Trade and Industry

Principal Instrument(s): *Foreign Exchange and Foreign Trade Act (FEFTA) (1949)*

Mandate: The METI-TCD oversees security export control in Japan. It exercises export licensing and other authorities to provide development of foreign trade and maintain peace and safety in Japan, as well as in internationally based on international export control regimes. The recent revision of the *Foreign Exchange and Foreign Trade Act* clarified that even the provision of technology to a resident is subject to export control if it is considered virtually identical to the provision of technology to a non-resident (i.e., if the resident is under the strong influence of the non-resident).

Major Reports, Inquiries, and Related Initiatives: None issued

* As of 2022 March, five companies are considered "specified platform providers" are Amazon, Apple, Google, Rakuten, and Yahoo.

*Ministry of Health, Labour and Welfare (MHLW)

Institutional Form: Regulatory authority

Responsible Minister: The Minister of Health, Labour and Welfare

Principal Instrument(s): *Pharmaceutical and Medical Device Act (1960)*

Mandate: The MHLW is responsible for the administration of health, medical care, children, childcare, welfare, long-term care, employment, labour, and pensions in Japan. In relation to digital technology, the *Pharmaceutical and Medical Device Act* was amended in 2014 to make software subject to regulation as a 'medical device program'. This amendment requires companies to obtain a licence as well as approval for their programs if they manufacture or sell programs for diagnostic, therapeutic or other purposes.

Major Reports, Inquiries, and Related Initiatives:

- Guidelines on whether a device qualifies as a programmed medical device (2021): [Guidelines] (In Japanese)[22]

Ministry of Internal Affairs and Communications (MIC)

Institutional Form: Regulatory authority

Responsible Minister: The Minister of Internal Affairs and Communications

Principal Instrument(s): *Act on Regulation of Transmission of Specified Electronic Mail (2002), Telecommunications Business Act (1984), Wire Telecommunications Act (1953), The Broadcast Act (1950), Radio Act (1950)*

Mandate: The MIC provides a safe and secure internet by taking measures against the distribution of illegal and harmful information, such as child pornography and information that infringes on people's rights. This includes supporting the voluntary deletion and reporting of such information by private businesses. It also promotes protection of consumers who use telecommunication networks. For telecommunications carriers that own major networks, the MIC enforces fair competition rules, such as connection obligations, so that carriers using those networks can provide services under fair conditions.

Major Reports, Inquiries, and Related Initiatives:

- Final Report of Study Group on Governance of Telecommunications Businesses (2022): [Report] (In Japanese)[23]
- Final Report of Study Group on Platform Services (2020): [Press Release] [Report] (In Japanese)[24]

Ministry of Finance, Foreign Investment Policy and Review Office (MOF-FIPRO) and Bank of Japan, International Department (BOJ-ID)

Institutional Form: Office in a ministry / Central Bank

Responsible Minister: The Minister of Finance (MOF) and The Governor of Bank of Japan

Principal Instrument(s): *Foreign Exchange and Foreign Trade Act (FEFTA) (1949)*

Mandate: The MOF-FIPRO and the BOJ-ID are both changed with screening inward direct investment to Japan under the FEFTA. If the business in which the target company is engaged qualifies as a 'core business', the foreign investor must accept the added restrictions applicable to the acquisitions of core business by non-financial institutions. The core business includes, among others, cyber security of critical infrastructures and certain telecommunication services. In 2020, the MOF added the manufacturing of drugs for infectious diseases and the manufacturing of highly controlled medical devices to the core businesses.

Major Reports, Inquiries, and Related Initiatives:

- Update of the List of Classifications of Listed Companies regarding the Prior-notification Requirements on Inward Direct Investment (2021): [Press Release][25]
- Rules and Regulations of the Foreign Exchange and Foreign Trade Act (2020): [Outline][26]
- Factors to be considered in authorities' screening of foreign direct investment (2020): [Press Release][27]

Personal Information Protection Commission (PPC)

Institutional Form: Independent authority

Responsible Minister: The Minister of State for the PPC

Principal Instrument(s): *Act on the Protection of Personal Information (2003, amended 2020) (APPI)*

Mandate: The PPC protects the rights and interests of individuals while taking into consideration proper and effective use of personal information including 'My Number'. Based on the Act on the Protection of Personal Information, the Chairman and Commission members exercise their authority independently, including policy making, supervision, and mediation of complaints. The act is revised every three years, the latest version of which was enacted 1 April 2022.

Major Reports, Inquiries, and Related Initiatives:

- Amended Act on the Protection of Personal Information (Tentative Translation) (2022): [Act][28]
- Report on systems for the protection of personal information in foreign countries (2021): [Report] (In Japanese)[29]
- Fact-finding survey on persons responsible for handling personal data (2021): [Survey] (In Japanese)[30]
- Report on Safety Management Measures of Small and Medium-Sized Businesses (2021): [Report] (In Japanese)[31]
- Report on the Actual Conditions Concerning the Proper Handling of Personal Information (2020): [Report] (In Japanese)[32]
- Fact-finding Survey on the Appropriate Use of Personal Data (2020): [Survey] (In Japanese)[33]
- Handling of personal data for preventing the spread of Novel-Coronavirus (COVID-19) disease (2020): [Report][34]

Endnotes (Japan)

1. *Protection of Consumers who use Digital Platforms Act on Improving Transparency and Fairness of Digital Platforms 2021,* accessed 29 March 2022, www.caa.go.jp/law/bills/assets/consumer_system_cms101_210305_03.pdf (In Japanese).

2. *Outline of the Act for the Protection of Consumers who use Digital Platforms 2021, accessed 8 April 2022,* www.caa.go.jp/law/bills/assets/consumer_system_cms101_210305_03.pdf.

3. Consumer Affairs Authority 2021, *Final report by the Study Group on Improvements of Consumer Protections Involving Digital Platforms* (In Japanese), accessed 29 March 2022, www.caa.go.jp/about_us/about/plans_and_status/digital_platform/assets/consumer_system_cms101_210201_01.pdf.

4. Digital Extraordinary Administrative Advisory Committee 2021, *Digital Principles for Structural Reform* (In Japanese), accessed 29 March 2022, https://cio.go.jp/sites/default/files/uploads/documents/digital/20211222_meeting_extraordinary_administrative_research_committee_01.pdf.

5. *Act on Improving Transparency and Fairness of Digital Platforms 2020, accessed 29 March 2022,* www.meti.go.jp/policy/mono_info_service/digitalplatform/houritsu.pdf (In Japanese).

6. Headquarters for Digital Market Competition 2021, *Evaluation of Competition in the Digital Advertising Market - Final Report* (In Japanese), accessed 29 March 2022, www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai5/siryou3s.pdf. For a summary in English, see: Headquarters for Digital Market Competition 2021, *Evaluation of Competition in the Digital Advertising Market Final Report : Summary,* accessed 29 March 2022, www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_210427.pdf.

7. Headquarters for Digital Market Competition 2020, *Report on Medium-Term Vision on Competition in the Digital Market* (In Japanese), accessed 29 March 2022, https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000204145. For a summary in English, see: Headquarters for Digital Market Competition (HDMC) 2021, *Report on Medium-Term Vision on Competition in the Digital Market: Summary*, accessed 29 March 2022, www.kantei.go.jp/jp/singi/digitalmarket/pdf_e/documents_200616-2.pdf.

8. Financial Services Agency 2021, *Interim Report by the Study Group on Digital and Decentralized Finance* (In Japanese), accessed 29 March 2022, www.fsa.go.jp/news/r3/singi/20211117/seiri.pdf.

9. Financial Services Agency 2020, *Research report on measures to promote innovative technology fields and RegTech/SupTech in the financial sector* (In Japanese), accessed 29 March 2022, www.fsa.go.jp/common/about/research/200903.pdf.

10. *Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (Antimonopoly Act) (1947),* accessed 29 March 2022, www.jftc.go.jp/en/policy_enforcement/21041301.pdf.

11. Japan Fair Trade Commission 2021, *Final Report Regarding Digital Advertising*, press release, accessed 29 March 2022, www.jftc.go.jp/en/pressreleases/yearly-2021/February/211012-2.pdf. See also: Japan Fair Trade Commission 2021, *Final Report Regarding Digital Advertising*, accessed 29 March 2022, www.jftc.go.jp/en/pressreleases/yearly-2021/February/210217.html.

12. Japan Fair Trade Commission 2019, *Amendments of the "Guidelines to Application of the Antimonopoly Act Concerning Review of Business Combination" and the "Policies Concerning Procedures of Review of Business Combination"*, press release, accessed 29 March 2022, www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217.html. See also: Japan Fair Trade Commission (JFTC) 2019, *Guidelines to Application of the Antimonopoly Act Concerning Review of Business Combination*, accessed 29 March 2022, www.jftc.go.jp/en/pressreleases/yearly-2019/December/1912173GL.pdf.

13. Japan Fair Trade Commission 2019, *Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information (JFTC Guidelines)*, press release, accessed 29 March 2022, www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217_DP.html. See also: Japan Fair Trade Commission (JFTC) 2019, *Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information (JFTC Guidelines)*, accessed 29 March 2022, www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217DPconsumerGL.pdf.

14. Japan Fair Trade Commission 2019, *Report regarding trade practices on digital platforms (Business-to-Business transactions on online retail platform and app store)*, press release, accessed 29 March 2022, www.jftc.go.jp/en/pressreleases/yearly-2019/October/191031.html. See also: Japan Fair Trade Commission (JFTC) 2019, *Report regarding trade practices on digital platforms (Business-to-Business transactions on online retail platform and app store)*, accessed 29 March 2022, htwww.jftc.go.jp/en/pressreleases/yearly-2019/October/191031Report.pdf.

15. Japan Virtual and Crypto assets Exchange Association 2020, *Basic guidelines for self-regulation* (In Japanese), accessed 29 March 2022, https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/B02_jvcea202005.pdf.

16. Japan Virtual and Crypto assets Exchange Association 2020, *Rules and Guidelines for the Handling of Crypto Assets* (In Japanese), accessed 29 March 2022, https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/B03_jvcea20200925.pdf.

17. Japan Virtual and Crypto assets Exchange Association 2020, *Rules and Guidelines for the Management of Users' Property Pertaining to the Crypto Asset Exchange Business* (In Japanese), accessed 29 March 2022, https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/B08_jvcea20200925.pdf.

18. Japan Virtual and Crypto assets Exchange Association 2020, *Rules and Guidelines for Solicitation and Advertisement of Crypto Asset Exchange* (In Japanese), accessed 29 March 2022, https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/B06_jvcea20200925.pdf.

19. *Act on Improving Transparency and Fairness of Digital Platforms 2020,* accessed 29 March 2022, www.meti.go.jp/policy/mono_info_service/digitalplatform/houritsu.pdf (In Japanese).

20. Ministry of Economy, Trade and Industry, Digital Market Policy Office 2021, *Review on business conducts of specified digital platforms,* accessed 29 March 2022, www.meti.go.jp/english/policy/mono_info_service/information_economy/digital_platforms/index.html.

21. Ministry of Economy, Trade and Industry, Digital Market Policy Office 2020, *Interpretative Guidelines on Electronic Commerce and Information Property Trading in March 2002 (Latest amendment was in August 2020)* (In Japanese), accessed 29 March 2022, www.meti.go.jp/press/2020/08/20200828001/20200828001-1.pdf.

22. Ministry of Health, Labour and Welfare 2021, *Guidelines on whether a device qualifies as a programmed medical device* (In Japanese), accessed 29 March 2022, www.jaame.or.jp/mdsi/program-files/210331gideline.pdf.

23. Ministry of Internal Affairs and Communications 2022, *Final Report of Study Group on Governance of Telecommunications Businesses* (In Japanese), accessed 29 March 2022, www.soumu.go.jp/main_content/000794590.pdf.

24. Ministry of Internal Affairs and Communications 2020, *Final Report of Study Group on Platform Services* (In Japanese), accessed 29 March 2022, www.soumu.go.jp/main_content/000668595.pdf.See also: Ministry of Internal Affairs and Communications 2020, *Result of Appeal for Opinions on Draft Final Report from Study Group on Platform Services and Release of Finalized Report*, press release, accessed 29 March 2022, www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/2/07_7.html.

25. Ministry of Finance 2021, *Update of the List of Classifications of Listed Companies regarding the Prior-notification Requirements on Inward Direct Investment*, accessed 29 March 2022, www.mof.go.jp/english/policy/international_policy/fdi/20211102.html.

26. *Rules and Regulations of the Foreign Exchange and Foreign Trade Act*, accessed 29 March 2022, www.mof.go.jp/english/policy/international_policy/fdi/kanrenshiryou01_20200424.pdf.

27. Ministry of Finance 2020, *Factors to be considered in authorities' screening of foreign direct investment*, press release, accessed 29 March 2022, www.mof.go.jp/english/policy/international_policy/fdi/gaitamehou_20200508.htm.

28. *Amended Act on the Protection of Personal Information 2020,* accessed 11 April 2022, www.ppc.go.jp/files/pdf/APPI_english.pdf.

29. Personal Information Protection Commission 2021, *Report on systems for the protection of personal information in foreign countries* (In Japanese), accessed 29 March 2022, www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf.

30. Personal Information Protection Commission 2021, *Fact-finding survey on persons responsible for handling personal data* (In Japanese), accessed 29 March 2022, www.ppc.go.jp/files/pdf/dpo_report202103.pdf.

31. Personal Information Protection Commission 2021, *Report on Safety Management Measures of Small and Medium-Sized Businesses* (In Japanese), accessed 29 March 2022, www.ppc.go.jp/files/pdf/R2_chuushou_anzenkanri_report.pdf.

32. Personal Information Protection Commission 2020, *Report on the Actual Conditions Concerning the Proper Handling of Personal Information* (In Japanese), accessed 29 March 2022, www.ppc.go.jp/files/pdf/R02fchoukokusho.pdf.

33. Personal Information Protection Commission 2020, *Fact-finding Survey on the Appropriate Use of Personal Data* (In Japanese), accessed 29 March 2022, www.ppc.go.jp/files/pdf/personal_date_report2019_1.pdf.

34. Personal Information Protection Commission 2020, *Handling of personal data for preventing the spread of Novel-Coronavirus (COVID-19) disease*, accessed 29 March 2022, www.ppc.go.jp/files/pdf/information_20200515.pdf.

Republic of Ireland

Mark Williams, Matthew G. O'Neill and Caitríona Heinl (Ed.), The Azure Forum for Contemporary Security Strategy

Data Protection Commission (DPC)

Institutional Form: National supervisory authority

Responsible Minister: Not applicable

Principal Instrument(s): *EU Law Enforcement Directive (LED) (2018), and Data Protection Act (2018), EU General Data Protection Regulation Directive (GDPR) (2016), Irish ePrivacy Regulations Act (2011)*

Mandate: The DPC is responsible for upholding the fundamental right of individuals in the European Union to data privacy through the monitoring and enforcement of compliance with data protection legislation in Ireland. The DPC's powers and assigned tasks allow it to handle complaints from individuals, in addition to conducting its own investigations into more systemic areas of risk.

Major Reports, Inquiries, and Related Initiatives:

- Data Protection Commission Regulatory Strategy 2022–2027 (2021): [Strategy][1]
- Report on the topic of 'GDPR' published by Justice Committee: [Report][2]
- Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing (2020): [Consultation Draft][3]
- Irish Data Protection Act (2018): [Act][4]
  - (Section 36(2)) (Health Research (Amendment) Regulations (2021): [Regulations][5]
  - (Section 60(6)) (Central Bank of Ireland) Regulations (2020): [Regulations][6]
  - (Employer's Insolvency) Act 1984 (Transfer of Personal Data) Regulations (2020): [Regulations][7]
  - (Section 60(6)) (Central Bank of Ireland) Regulations (2019): [Regulations][8]
  - (Section 36(2)) (Health Research (Amendment) Regulations (2019): [Regulations][9]
- EU General Data Protection Regulation (GDPR) (2016): [Regulation][10]
- Law Enforcement Directive (EU) 2016/680 (2016): [Directive][11]

Commission for Communications Regulations (ComReg)

Institutional Form: State agency

Responsible Minister: The Minister of the Department for the Environment, Climate and Communications

Principal Instrument(s): *Communications Regulation (Postal Service) (Amendment) Act (2017), Communications Regulation (Premium Rate Services and Electronic Communications Infrastructure) Act (2010), Communications Regulation (Premium Rate Services and Electronic Communications Infrastructure) Act (2010), Communications Regulation Act (2002), S.I. (Statutory Instrument) No. 510 of 2002 Communications Regulation Act 2002 (Establishment Day) Order (2002)*

Mandate: The ComReg regulates the electronic communications industry (telecommunications, radio communications, broadcast transmission and premium rate services) in Ireland. It promotes competition, safeguards consumers, and stimulates innovation. It is working on the Communications Regulation (Enforcement) Bill that would establish the ComReg as the Irish competent body for enforcement of the European Electronic Communications Code, and on the Competition (Amendment) Bill 2022 to transpose European Union Directive 2019/1 (ECN+ Directive) into Irish law. This will strengthen the enforcement authorities of both the ComReg and the Competition and Consumer Protection Commission.

Major Reports, Inquiries, and Related Initiatives:

- Competition (Amendment) Bill (2022): [Bill][12]
- Communications Regulation (Enforcement) Bill (2022): [Bill][13]
- European Union (Electronic Communications Code) Regulations (2022): [Regulations][14]
- Declaration on European Digital Rights and Principles (2022): [Strategy][15]
- Joint Committee on European Union Affairs Debate – Wednesday, 1 Dec 2021. EU Cybersecurity (2021): [Discussion][16]
- Joint Committee on Transport and Communications Debate – Tuesday, 28 Sep 2021. Scrutiny of EU Legislative Proposals (2021): [Discussion][17]
- Communication on the 2030 Digital Compass (2020): [Strategy][18]
- Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018, to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (2018): [Directive][19]
- Regulation (EU) 2017/920 of the European Parliament and of the Council of 17 May 2017 (2017): [Regulations][20]

Broadcasting Authority of Ireland (BAI)

Institutional Form: State agency

Responsible Minister: The Minister of the Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media

Principal Instrument(s): *Competition and Consumer Protection Act (2014) - Part 4, Media Mergers; Broadcasting Act (2009)*

Mandate: The BAI regulates all content broadcast by Irish-licensed broadcasters for both programming and commercial content. In addition to processing broadcasting complaints, the BAI monitors broadcast content for compliance with broadcasting codes and rules. Under the *Competition and Consumer Protection Act 2014 - Part 4*, the BAI is also responsible for conducting a phase 2 review to determine if the outcome of a media merger is likely to be detrimental to the public interest in safeguarding media plurality in Ireland, as defined under the *Competition Act 2002 (as amended).* The Online Safety and Media Regulation Bill 2022 proposes the dissolution of the BAI and the transference of its staff and functions to a 'Media Commission', which will be tasked with regulating linear broadcasting and video on-demand services in Ireland as well as regulating harmful content on online platforms. An Online Safety Commissioner with responsibility for overseeing the regulatory framework for online safety will be established within the Media Commission.

Major Reports, Inquiries, and Related Initiatives:

- Online Safety and Media Regulation Bill (2022): [Bill][21]
- Revision of the Audiovisual Media Services Directive (AVMSD) (2022): [Webpage][22]
- Joint Committee on Tourism, Culture, Arts, Sport and Media- Report of the Joint Committee on the Pre-Legislative Scrutiny of the General Scheme of the Online Safety and Media Regulation Bill November (2021): [Report][23]
- Broadcasting Authority of Ireland Strategy Statement 2021 – 2023 (2021): [Strategy][24]
- Broadcasting Authority of Ireland submission to the Future of Media Commission (2021): [Report][25]
- CovidCheck: Assessing the implementation of EU Code of Practice on Disinformation in relation to COVID-19 (2021): [Report][26]
- Broadcasting (Amendment) Bill (2019): [Bill][27]

Competition and Consumer Protection Commission (CCPC)

Institutional Form: State agency

Responsible Minister: The Minister of the Department of Enterprise, Trade and Employment

Principal Instrument(s): *Competition and Consumer Protection Act (2014)*

Mandate: The CCPC promotes compliance with, and enforces, competition, product safety, and consumer protection law in Ireland. The CCPC assesses proposed mergers, acquisitions and takeovers that reach a certain financial threshold, including all media mergers. The CCPC also monitors compliance with, and enforcement of, several European Union Directives governing the sale of goods or services online to consumers in the European Union, including the Consumer Rights Directive, the Geo-Blocking Regulation, and the Platform to Business Regulations.

Major Reports, Inquiries, and Related Initiatives:

- Competition (Amendment) Bill (2022): [Bill][28]
- Geo-Blocking – What you need to know (2022): [Guide][29]
- Selling Online – What you need to know (2022): [Guide][30]
- Competition and Consumer Protection Commission Strategy Statement 2021 – 2023 (2021): [Strategy][31]
- Platform to Business Regulations (2020): [Regulations][32]

*National Advisory Council for Online Safety (NAC-OS)

Institutional Form: Government forum

Responsible Minister: The Minister of the Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media

Principal Instrument(s): *The Action Plan for Online Safety (2018–19)*

Mandate: The NAC-OS was established as part of the Action Plan for Online Safety. It is composed of 20 members and a chairperson, which are representatives from children's and parents' organisations, major internet platforms, and online safety specialists. The role of the NAC-OS is to advise the government about online safety issues, identify emerging issues that may require government intervention, assist to develop clear and easily understandable online safety guidance materials for all internet users, and conduct national and international research and communicate findings to the government, stakeholders, and the public.

Major Reports, Inquiries, and Related Initiatives:

- Joint Committee on Tourism, Culture, Arts, Sport and Media- Report of the Joint Committee on the Pre-Legislative Scrutiny of the General Scheme of the Online Safety and Media Regulation Bill (2021): [Report][33]
- Report of a National Survey of Children, their Parents and Adults regarding Online Safety (2021): [Report][34]
- National Advisory Council for Online Safety: Annual Report (2019): [Report][35]
- National Advisory Council for Online Safety: Progress Report (2019): [Report][36]
- Action Plan for Online Safety 2018 – 2019 (2018): [Strategy][37]

Central Bank of Ireland (CBI)

Institutional Form: Central Bank (European System of Central Banks (ESCB))

Responsible Minister: Independent authority – Central Bank Commission

Principal Instrument(s): *The Central Bank Reform Act (2010), Central Bank Act (1942)*

Mandate: The CBI is the financial services regulator and is responsible for authorising and supervising providers of regulated financial services. The CBI is responsible for prudential supervision and consumer protection of regulated entities that it has authorised. Ireland does not currently have a specific regulatory framework for FinTech businesses; however, the CBI has regulatory authority over the provision of services or the undertaking of activities that fall within the regulator's purview. Regulated activities are governed by European Union directives and each of the reports listed below includes a passporting provision that allows a provider authorised in one member state to provide services in another member state, subject to notification requirements to the home and host state competent authorities. A Markets in Crypto-Asset Regulation (MiCA) is being developed at the European Union level, and this legislative proposal will build a more appropriate regulatory framework for virtual asset service providers across Europe, including passporting rights for those enterprises.

Major Reports, Inquiries, and Related Initiatives:

- Securities Markets Risk Outlook Report (2022): [Report][38]
- Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act (2021) (transposed the EU's Fifth Anti-Money Laundering ("MLD5") Directive into Irish law): [Act][39]
- Central Bank of Ireland Strategic Plan 2022–2024 (2021): [Strategy][40]
- Crowdfunding Marketing Requirements (2021): [Report][41]
- The future of payments in Ireland and Europe (2021): [Speech][42]
- Regulation (EU) 2020/1503 (the 'Crowdfunding Regulation') and Directive (EU) 2020/1504 (the 'MiFID II Amending Directive') (2020): [Regulations][43]
- The European Union (Payment Services) Regulations (2018) transposed Directive (EU) 2015/2366 ('PSD II') into Irish legislation and regulates the supply of payment services: [Regulations][44]
- The European Union (Markets in Financial Instruments) Regulations (2017) (the 'Irish MiFID II Regulations') transposed Directive 2014/65/EU ('MiFID II') into Irish law: [Regulations][45]
- The European Communities (Electronic Money) Regulations (2011), which regulate the issue and redemption of electronic money, were transposed into Irish law by Directive 2009/110/EC ("EMD"): [Regulations][46]

The Intellectual Property Office of Ireland (IPOI)

Institutional Form: State agency

Responsible Minister: The Minister for Enterprise, Trade and Employment

Principal Instrument(s): *Copyright and Other Intellectual Property Law Provisions Act (2019), Industrial Designs Act (2001), Copyright and Related Rights Act (2000), Intellectual Property (Miscellaneous Provisions) Act (1998), Trademarks Act (1996), European Communities (Supplementary Protection Certificate) Regulations (1993), Patents Act (1992)*

Mandate: The IPOI is responsible for intellectual property rights including patents, designs, trade marks, and copyright.

Major Reports, Inquiries, and Related Initiatives:

- SI No 567 of 2021 European Union (Copyright and Related Rights in the Digital Single Market) Regulations (2021): [Regulation][47]
- EU Directive 2019/790: Copyright and Related Rights in the Digital Single Market - Information Note (2021): [Report][48]
- IPOI Strategic Plan 2020–2022 (2020): [Strategy][49]
- Review of the Administration of Civil Justice Report (2020)*: [Report][50]

Trade Licensing and Control Unit (TLCU)

Institutional Form: Unit within a Government Department

Responsible Minister: The Minister for Enterprise, Trade and Employment

Principal Instrument(s): *S.I. No. 207/2021 - Control of Exports (Brokering Activities, Goods and Technology) Regulations (2021), Control of Exports (Dual-Use Items) (Amendment) Order 2019, EU Commission Delegated Regulation 2018/1922 (2018), Control of Exports (Goods and Technology) Order (2012), Council Regulation (EC) No. 1236/2005 (2005)*

Mandate: The TLCU is responsible for managing controls on exports of dual-use items and technology, military items, and items destined for countries to which trade sanctions apply. Dual-use items include products and components, (i.e., software and technology) that can be used for both civil and military purposes.

Major Reports, Inquiries, and Related Initiatives:

- EU Dual-use Regulation and Ireland (2021): [Regulation][51]
- Report under the Control of Exports Act 2008 covering the period 1 January - 31 December 2020 (2021): [Report][52]

* Recommended the establishment of a separate list within the Commercial Court dedicated to intellectual property disputes and disputes concerning technology.

Department for Enterprise, Trade and Employment (DETE)

Institutional Form: Government Department

Responsible Minister: The Minister for Enterprise, Trade and Employment

Principal Instrument(s): *Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union (2019)*

Mandate: The DETE advises and implements policies that stimulate the productive capacity of the economy and creates employment sustainability. The DETE also promotes fair competition in the marketplace, protects consumers, and safeguards workers. Investment screening is a procedure allowing the DETE to assess, investigate, authorise, condition, prohibit, or unwind foreign direct investments based on security and public-order criteria. This includes effects on critical infrastructure, technologies, and inputs that are essential for security or the maintenance of public order. Effects of foreign direct investment relating to access to sensitive information (including personal data) or the ability to control this information, or the freedom and pluralism of the media may also be considered. Industries affected include remote sensing systems, artificial intelligence, autonomous driving or flying, industrial robots, semiconductors, cybersecurity, aeronautical/aerospace, nuclear technology, quantum technology, biotechnology, additive manufacturing (3D printing), network technologies, smart metre gateways, and information and communication technology.

Major Reports, Inquiries, and Related Initiatives:

- Public Consultation on EU Proposal for a Foreign Subsidies Regulation (2021): [Report][53]
- Public Consultation on Investment Screening (2020): [Inquiry Webpage] [Report][54]
- The Investment Screening Bill 2020 will give full effect to EU Regulation 2019/452 (2020): [Discussion Record][55]

DETE, Digital Single Market Unit (DSU)

Institutional Form: Unit within a Government Department

Responsible Minister: The Minister for Enterprise, Trade and Employment

Principal Instrument(s): *Regulation COM/2020/842 final, regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act (2020)), Regulation COM/2020/825 final, regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act (2020)) and amending Directive 2000/31/EC*

Mandate: The DSU provides a whole-of-government approach and a cross-government coordination of the digital single market in Ireland. It has a lead role in the National Digital Strategy to develop a digital ecosystem for small-to-medium enterprises and to increase Ireland's digital competitiveness.

Major Reports, Inquiries, and Related Initiatives:

- Harnessing Digital - The Digital Ireland Framework (2022): [Strategy][56]
- Virtual Roundtable Discussion on the EU Digital package of the Digital Markets Act and Digital Services Act (2021): [Discussion Record][57]
- National submission to the EU consultation on the Digital Services Act package (2020): [Report][58]

Ombudsman for Children's Office (OCO)

Institutional Form: Independent public body

Responsible Minister: Not applicable

Principal Instrument(s): *Ombudsman for Children Act (2002)*

Mandate: The OCO is a human rights institution that promotes the rights and welfare of young people under 18 years of age living in Ireland, including their rights online.

Major Reports, Inquiries, and Related Initiatives:

- Public consultation on the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation (2019): [Report][59]
- Consultation on Data protection safeguards for children ('digital age of consent') (2016): [Report][60]

Office of the Revenue Commissioners (ORCs)

Institutional Form: Government agency

Responsible Minister: The Minister for Finance

Principal Instrument(s): *Revenue Commissioners was established by Government Order in (1923)*

Mandate: The ORC is responsible for the assessment and collection of taxes and duties. ORC's mission is derived from statutory and administrative requirements, as well as from Ireland's membership in the European Union.

Major Reports, Inquiries, and Related Initiatives:

- Public consultation Data Sharing Agreement (2022): [Webpage][61]
- Data Sharing Agreement for Immigration Investor Data (2022): [Webpage][62]
- Data Sharing and Governance Act (2019): [Act][63]
- Regulation (EU) 2016/679 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 (2016)): [Regulation][64]
- Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016): [Directive][65]

Ongoing Parliamentary Committees, Inquiries, or Legislative Proposals (not previously referred to):

- AI - Here for Good: National Artificial Intelligence Strategy for Ireland (2021): [Report][66]
- Commission for Regulation of Utilities - Direction to the System Operators related to Data Centre grid connection processing (2021): [Report][67]
- Inter-Departmental Working Group on Future Licensing and Regulation of Gambling (2019): [Report][68]
- The Broadcasting (Amendment) Bill (2019): [Bill][69]
- National Cyber Security Strategy 2019 – 2024 (2019): [Strategy][70]
- NIS Compliance Guidelines for Operators of Essential Service (OES) (2019): [Report][71]
- S.I. No. 360/2018 – European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations (2018): [Regulation][72]

Endnotes (Republic of Ireland)

1. Data Protection Commission (DPC) 2021, *Data Protection Commission Regulatory Strategy 2022 – 2027*, accessed 1 April 2022, www.dataprotection.ie/en/news-media/latest-news/dpc-publishes-regulatory-strategy-2022-2027.

2. Houses of the Oireachtas Joint Committee on Justice 2021, *Report on the topic of 'GDPR' published by Justice Committee*, accessed 1 April 2022, www.oireachtas.ie/en/press-centre/press-releases/20210722-report-on-the-topic-of-gdpr-published-by-justice-committee/.

3. Data Protection Commission 2020, *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*, www.dataprotection.ie/index.php/en/news-media/consultations/children-front-and-centre-fundamentals-child-oriented-approach-data-processing.

4. *Irish Data Protection Act (2018),* accessed 1 April 2022, www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html.

5. *Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2021,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2021/si/18/made/en/print.

6. *Data Protection Act 2018 (section 60(6)) (Central Bank of Ireland) Regulations 2020,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2020/si/534/made/en/print.

7. *Protection of Employees (Employers' Insolvency) Act 1984 (Transfer of Personal Data) Regulations 2020,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2020/si/730/made/en/print.

8. *Data Protection Act 2018 (Section 60(6)) (Central Bank of Ireland) Regulations 2019,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2019/si/537/made/en/print.

9. *Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2019*, accessed 1 April 2022, www.irishstatutebook.ie/eli/2019/si/188/made/en/print.

10. *Consolidated text: 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) (Text with EEA relevance),* EUR-Lex, accessed 1 April 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504.

11. *Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA,* accessed 1 April 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680.

12. *Competition (Amendment) Bill 2022,* accessed 1 April 2022, https://data.oireachtas.ie/ie/oireachtas/bill/2022/12/eng/initiated/b1222d.pdf.

13. *Communications Regulation (Enforcement) Bill (2022),* accessed 1 April 2022, https://assets.gov.ie/212053/f6cd7fdc-72b0-45be-bbde-5eb2158b57d1.pdf.

14. *European Union (Electronic Communications Code) Regulations (2022),* accessed 1 April 2022, https://assets.gov.ie/212062/b320ab75-300e-4a19-9a5e-a3a4d66d1db7.pdf.

15. European Commission 2022, *European Declaration on Digital Rights and Principles for the Digital Decade*, accessed 1 April 2022, https://ec.europa.eu/newsroom/dae/redirection/document/82703.

16. Houses of the Oireachtas 2021, *Joint Committee on European Union Affairs debate - Wednesday, 1 Dec 2021 – EU Cybersecurity: Discussion (Resumed)*, accessed 1 April 2022, www.oireachtas.ie/en/debates/debate/joint_committee_on_european_union_affairs/2021-12-01/2/?highlight%5B0%5D=digital&highlight%5B1%5D=europe&highlight%5B2%5D=digitally.

17. Houses of the Oireachtas 2021, *Joint Committee on Transport and Communications debate - Tuesday, 28 Sep 2021*, accessed 1 April 2022, www.oireachtas.ie/en/debates/debate/joint_committee_on_transport_and_communications/2021-09-28/2/?highlight%5B0%5D=digital&highlight%5B1%5D=digital&highlight%5B2%5D=europe&highlight%5B3%5D=digital&highlight%5B4%5D=digital.

18. European Commission 2021, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - 2030 Digital Compass: the European way for the Digital Decade*, accessed 1 April 2021, https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02/DOC_1&format=PDF.

19. *Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018, to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market*, Official Journal of the European Union, accessed 1 April 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0001&from=EN.

20. *Regulation (EU) 2017/920 of the European Parliament and of the Council of 17 May 2017*, accessed 1 April 2022, www.comreg.ie/media/2016/02/2015-2017-Roaming-Regs-Consolidated.pdf.

21. *Online Safety and Media Regulation Bill,* accessed 1 April 2022, www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/.

22. Eurovision Commission 2022, *Revision of the Audiovisual Media Services Directive (AVMSD)*, accessed 1 April 2022, https://digital-strategy.ec.europa.eu/en/policies/revision-avmsd.

23. Houses of the Oireachtas 2021, *Joint Committee on Tourism, Culture, Arts, Sport and Media- Report of the Joint Committee on the Pre-Legislative Scrutiny of the General Scheme of the Online Safety and Media Regulation Bill November*, 1 April 2022, https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_tourism_culture_arts_sport_and_media/reports/2021/2021-11-02_report-of-the-joint-committee-on-the-pre-legislative-scrutiny-of-the-general-scheme-of-the-online-safety-and-media-regulation-bill_en.pdf.

24. Broadcasting Authority of Ireland 2021, *Strategy Statement 2021-2023*, https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_tourism_culture_arts_sport_and_media/reports/2021/2021-11-02_report-of-the-joint-committee-on-the-pre-legislative-scrutiny-of-the-general-scheme-of-the-online-safety-and-media-regulation-bill_en.pdf.

25. Broadcasting Authority of Ireland 2021, *Broadcasting Authority of Ireland: Submission to the Future of Media Commission*, accessed 1 April 2022, https://futureofmediacommission.ie/wp-content/uploads/258.-BAI-Submission.pdf.

26. Culloty, E, Park, K, Feenane, T, Papaevangelou, C, Conroy, A & Suiter, J 2021, *CovidCheck: Assessing the implementation of EU Code of Practice on Disinformation in relation to COVID-19*, accessed 1 April 2022, www.bai.ie/en/download/136478/.

27. *Broadcasting (Amendment) Bill 2019,* accessed 1 April 2022, www.gov.ie/pdf/?file=https://assets.gov.ie/136690/4e5a8b35-d394-4334-90fe-4cfe132c7ca1.pdf#page=null.

28. *Competition (Amendment) Bill,* accessed 1 April 2022, www.oireachtas.ie/en/bills/bill/2022/12/.

29. Competition and Consumer Protection Commission 2018, *Geo-blocking: What you need to know*, accessed 1 April 2022, www.ccpc.ie/business/wp-content/uploads/sites/3/2018/12/Geo-blocking-Guide.pdf.

30. Competition and Consumer Protection Commission 2021, *Selling Online: What you need to know*, 1 April 2022, www.ccpc.ie/business/wp-content/uploads/sites/3/2018/12/Geo-blocking-Guide.pdf.

31. Competition and Consumer Protection Commission 2021, *Competition and Consumer Protection Commission Strategy Statement 2021 – 2023*, accessed 1 April 2022, www.ccpc.ie/business/wp-content/uploads/sites/3/2020/12/CCPC-Strategy-Statement-2021-2023.pdf.

32. *European Union (Promoting Fairness and Transparency For Business Users of Online Intermediation Services) Regulations 2020,* accessed 1 April 2022, www.ccpc.ie/business/wp-content/uploads/sites/3/2020/11/S.I.-No.-256-of-2020-P2B-Regulations.pdf.

33. House of the Oireachtas 2021, *Joint Committee on Tourism, Culture, Arts, Sport and Media- Report of the Joint Committee on the Pre-Legislative Scrutiny of the General Scheme of the Online Safety and Media Regulation Bill*, accessed 1 April 2022, https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_tourism_culture_arts_sport_and_media/reports/2021/2021-11-02_report-of-the-joint-committee-on-the-pre-legislative-scrutiny-of-the-general-scheme-of-the-online-safety-and-media-regulation-bill_en.pdf.

34. National Advisory Council for Online Safety 2021*, Report of a National Survey of Children, their Parents and Adults regarding Online Safety*, https://assets.gov.ie/204409/b9ab5dbd-8fdc-4f97-abfc-a88afb2f6e6f.pdf.

35. National Advisory Council for Online Safety 2019, *National Advisory Council for Online Safety: Annual Report*, accessed 1 April 2022, https://assets.gov.ie/76744/6446ed60-6998-4eee-b010-29fb-f1acf872.pdf.

36. National Advisory Council for Online Safety 2019, *National Advisory Council for Online Safety: Progress Report*, 1 April 2022, https://assets.gov.ie/76743/ab7813dd-366b-4e8b-a0f1-e1310fa3c6a3.pdf.

37. National Advisory Council for Online Safety 2018*, Action Plan for Online Safety 2018 – 2019*, accessed 1 April 2022, https://assets.gov.ie/27511/0b1dcff060c64be2867350deea28549a.pdf.

38. Central Bank of Ireland 2022, *Securities Markets Risk Outlook Report: A Changing Landscape*, accessed 1 April 2022, www.centralbank.ie/docs/default-source/regulation/industry-market-sectors/securities-markets/risk-outlook-reports/securities-markets-risk-outlook-report-2022.pdf?sfvrsn=4.

39. *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2021/act/3/enacted/en/pdf. See also: *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance)*, accessed 1 April 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843.

40. Central Bank of Ireland 2021, *Our Strategy: September 2021,* accessed 1 April 2022, www.centralbank.ie/docs/default-source/publications/corporate-reports/strategic-plan/our-strategy/central-bank-of-ireland-our-strategy.pdf?sfvrsn=4.

41. Central Bank of Ireland 2021, *Crowdfunding Marketing Requirements,* accessed 1 April 2022, www.centralbank.ie/docs/default-source/publications/consultation-papers/cp141/cp141-crowdfunding-marketing-requirements.pdf?sfvrsn=4.

42. Donnery, S 2021, 'Opening remarks by Deputy Governor Sharon Donnery - "The Future of Payments in Ireland and Europe"', transcript, accessed 1 April 2022, www.bis.org/review/r210429a.pdf.

43. *Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (Text with EEA relevance)*, EUR-Lex, accessed 1 April 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1503. See also: European Parliament and the Council of the European Union 2020, *Directive (EU) 2020/1504 of the European Parliament and of the Council of 7 October 2020 amending Directive 2014/65/EU on markets in financial instruments (Text with EEA relevance)*, EUR-Lex, 1 April 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020L1504.

44. *European Union (Payment Services) Regulations 2018,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2018/si/6/made/en/print.

45. *European Union (Markets in Financial Instruments) Regulations 2017,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2017/si/375/made/en/print.

46. *European Communities (Electronic Money) Regulations 2011,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2011/si/183/made/en/print.

47. *European Union (Copyright and Related Rights in the Digital Single Market) Regulations 2021,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2021/si/567/made/en/print.

48. Department of Enterprise, Trade and Employment 2021, *Transposition of EU Directive on Copyright and related rights in the Digital Single Market (EU) 2019/790*, accessed 1 April 2022, www.irishstatutebook.ie/eli/2021/si/567/made/en/print.

49. Intellectual Property Office of Ireland 2020, *Strategy Statement 2020 – 2022*, 1 March 2022, https://ipoi.gov.ie/en/about-us/ipoi-publications/strategy-statement/ipoi-raiteas-straiteise-strategy-statement-2020-2022.pdf.

50. Department of Justice 2020, *Review of the Administration of Civil Justice*, accessed 1 April 2022, www.justice.ie/en/JELR/Review_of_the_Administration_of_Civil_Justice_-_Review_Group_Report.pdf/Files/Review_of_the_Administration_of_Civil_Justice_-_Review_Group_Report.pdf.

51. *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast),* EUR-Lex, 1 April 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0821&from=EN.

52. Department of Enterprise, Trade and Employment 2020, *Report under the Control of Exports Act 2008: Covering the Period 1st January 2020 – 31st December 2020*, https://assets.gov.ie/212121/5a22576d-3641-4b55-aa80-a4a7ad843405.pdf.

53. Department of Enterprise, Trade and Employment 2021, *Public Consultation on EU Proposal for a Foreign Subsidies Regulation*, 1 April 2022, https://assets.gov.ie/204711/181292a8-429c-4267-ab4b-4b95f4264ee7.docx.

54. Department of Business, Enterprise, and Innovation 2020, *Public Consultation on Investment Screening: Transposition of the EU Regulation Establishing a Framework for Screening of Foreign Direct Investments into the EU*, accessed 1 April 2022, https://enterprise.gov.ie/en/Consultations/Consultations-files/Public-Consultation-Investment-Screening.pdf.

55. Department of Enterprise, Trade and Employment 2020, *Government agrees EU Regulation to screen Foreign Direct Investment*, accessed 1 April 2022, https://enterprise.gov.ie/en/News-And-Events/Department-News/2020/September/20200913.html.

56. Department of the Taoiseach 2022, *Harnessing Digital - The Digital Ireland Framework*, accessed 1 April 2022, https://assets.gov.ie/214584/fa3161da-aa9d-4b11-b160-9cac3a6f6148.pdf.

57. Department of Business, Enterprise, and Innovation 2020, *A virtual Roundtable on the EU Digital package – the Digital Markets Act and Digital Services Act*, accessed 1 April 2022, https://enterprise.gov.ie/en/Publications/Publication-files/Virtual-Roundtable-on-the-EU-Digital-package.pdf.

58. Department of Business, Enterprise, and Innovation 2020, *The Irish position on the EU Commission's proposed Digital Services Act package - Submission to the Public Consultation*, accessed 1 April 2022, https://enterprise.gov.ie/en/Publications/Publication-files/Virtual-Roundtable-on-the-EU-Digital-package.pdf.

59. Data Protection Commission 2019, *Public consultation on the processing of children's personal data and the rights of children as data subjects under the General Data Protection Regulation*, accessed 1 April 2022, www.dataprotection.ie/sites/default/files/uploads/2018-12/DPC_ChildrensRights_2019_English.pdf.

60. Ombudsman for Children's Office 2016, *Consultation on Data protection safeguards for children ('digital age of consent') – OCO Submission on the Age of Digital Consent*, accessed 1 April 2022, www.justice.ie/en/JELR/Office_of_the_Ombudsman_for_Children.pdf/Files/Office_of_the_Ombudsman_for_Children.pdf.

61. Office of the Revenue Commissioners 2022, *Proposed Data Sharing Agreement between the Department of Justice and Revenue (DSA for Immigration Investor Data),* accessed 1 April 2022, www.gov.ie/en/consultation/b809f-proposed-data-sharing-agreement-between-the-department-of-justice-and-the-revenue-dsa-for-immigration-investor-data/.

62. Office of the Revenue Commissioners 2022, *Proposed Data Sharing Agreement between the Department of Justice and the Department of Foreign Affairs (DSA for citizenship data)*, accessed 1 April 2022, www.gov.ie/en/consultation/d0e2c-proposed-data-sharing-agreement-between-the-department-of-justice-and-the-department-of-foreign-affairs-dsa-for-citizenship-data/.

63. *Data Sharing and Governance Act 2019,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2019/act/5/enacted/en/html.

64. *Regulation (EU) 2016/679 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*, EUR-Lex, accessed 1 April 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&rid=1#page=30.

65. *Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, accessed 1 April 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&rid=1.

66. Department of Enterprise, Trade and Employment 2021, *AI - Here for Good: A National Artificial Intelligence Strategy for Ireland*, 1 April 2022, https://enterprise.gov.ie/en/Publications/Publication-files/National-AI-Strategy.pdf.

67. Commission for the Regulation of Utilities 2021, *CRU Direction to the System Operators related to Data Centre grid connection processing Decision*, www.cru.ie/wp-content/uploads/2021/11/CRU21124-CRU-Direction-to-the-System-Operators-related-to-Data-Centre-grid-connection-processing.pdf.

68. Department of Justice 2019, *Inter-Departmental Working Group on Future Licensing and Regulation of Gambling*, accessed 1 April 2022, www.justice.ie/en/JELR/Inter-Departmental_Working_Group_on_Future_Licensing_and_Regulation_of_Gambling.pdf/Files/Inter-Departmental_Working_Group_on_Future_Licensing_and_Regulation_of_Gambling.pdf.

69. *Broadcasting (Amendment) Bill 2019,* accessed 1 April 2022, https://data.oireachtas.ie/ie/oireachtas/bill/2019/64/eng/initiated/b6419d.pdf.

70. Government of Ireland 2019, *National Cyber Security Strategy, 2019-2024*, accessed 1 April 2022, https://assets.gov.ie/76728/567c89b8-47f6-4e13-8782-409cff8b5b94.pdf.

71. Department of Communications, Climate Action and Environment 2019, *NIS Compliance Guidelines for Operators of Essential Services*, accessed 1 April 2022, https://assets.gov.ie/76729/ea0bcd3b-0161-41d2-8c51-df00e558689c.pdf.

72. *European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018,* accessed 1 April 2022, www.irishstatutebook.ie/eli/2018/si/360/made/en.

Republic of Korea*

Dr Yong Lim, Dr Sangchul Park, Dr Haksoo Ko, Jonggu Jeong, Eunjung Cho and Haesung Lee, Seoul National University

*Ministry of Culture, Sports and Tourism (MOCST)

Institutional Form: Department (Executive Ministry)

Responsible Minister: The Minister of Culture, Sports and Tourism

Principal Instrument(s): *Game Industry Promotion Act (2006), Content Industry Promotion Act (2002)*

Mandate: The MOCST administers duties concerning culture, arts, video, advertising, publishing, sports, tourism, and publicity. To promote K-content as part of the Korean New Deal, the MOCST has plans to reinforce cultural technology, research, and development capabilities, and strengthen the competitiveness of over-the-top video services and metaverse content. The MOCST develops and implements policies that protect the intellectual property rights of game products to create a healthy gaming culture. It also pursues policies that prevent adverse effects of gaming, such as excessive immersion in games or the encouragement of speculation, violence, and lasciviousness.

Major Reports, Inquiries, and Related Initiatives:

- Cultural Data Creation and Utilization Promotion Act (proposed) (2021): [Proposal] (In Korean)[1]

Game Rating and Administration Committee (GRAC)

Institutional Form: Public organisation (established by law)

Responsible Minister: The Chairperson of GRAC

Principal Instrument(s): *Game Industry Promotion Act (2006)*

Mandate: The GRAC is a video game content rating board that has responsibility for rating games manufactured and distributed in South Korea. Pursuant to the *Game Industry Promotion Act,* games sold in Korea must be rated by the GRAC prior to sale. In 2022, the GRAC warned that it may decline to provide ratings to games, especially those featuring tradable non fungible tokens or cryptocurrencies, including 'play-to-earn' games. This is based on concerns that such games could fuel gambling addiction, particularly among teenagers.

Major Reports, Inquiries, and Related Initiatives:

- GRAC Yearbook 2020 on Rating Classification and Post Management of Game (2020): [Final Report][2]

* Note: Korea's tech regulatory structure may undergo changes during 2022 following the results of the presidential election.

Korea Copyright Commission (KCOPC)

Institutional Form: Public organisation (established by law)

Responsible Minister: The Chairperson of KCOPC

Principal Instrument(s): *Copyright Act (1957)*

Mandate: The KCOPC administers the copyright-related affairs, promotes the legitimate use of works, and develops the copyright sector. Its roles include deliberating copyright-related issues, mediating copyright disputes, researching policies and legislation on copyright, providing copyright education and public awareness programs, and serving as a copyright registration agency. The KCOPC is reviewing the current Korean copyright laws especially regarding the metaverse, short-form content, non-fungible tokens, and what future copyright institutions should look like.

Major Reports, Inquiries, and Related Initiatives:

- Analysis on the implementation of the copyright directive on Digital Single Market Directive in European Union (2022): [Final Report] (In Korean)[3]
- A study to prepare exemptions notice draft for the prohibition on circumvention of technological protection measures (2020): [Final Report] (In Korean)[4]

*Ministry of Economy and Finance (MOEF)

Institutional Form: Department (Executive Ministry)

Responsible Minister: The Minister of Economy and Finance

Principal Instrument(s): *National Finance Act (2007), Framework Act on National Taxes (1975), Restriction of Special Taxation Act (1966)*

Mandate: The MOEF administers the formulation, execution, and performance management of budgets and funds, currency, foreign exchange, government accounting, internal tax system, customs, international finance, and management of public institutions as well as the National Treasury. The MOEF moved to amend the law to provide tax reductions for producing over-the-top video content to support the relevant industries.

Major Reports, Inquiries, and Related Initiatives:

- Amendment of Restriction of Special Taxation Act (2021): [Press Release] (In Korean)[5]

National Tax Service (NTS)

Institutional Form: Government agency (established under MOEF)

Responsible Minister: The Commissioner of NTS

Principal Instrument(s): *Framework Act on National Taxes (1975), National Tax Collection Act (1949)*

Mandate: The NTS administers duties concerning the imposition, reduction and collection of internal taxes and exemption. The NTS provides guides and helps taxpayers to fulfil their obligations in accordance with the taxation laws.

Major Reports, Inquiries, and Related Initiatives: None issued

Ministry of the Interior and Safety (MOIS)

Institutional Form: Department (Executive Ministry)

Responsible Minister: The Minister of the Interior and Safety

Principal Instrument(s): *Act on Facilitation of Data-Driven Administration (2020), Act on Promotion of the Provision and Use of Public Data (2013) ("Public Data Act"), Electronic Government Act (2001)*

Mandate: The MOIS is responsible for conducting the public affairs of the State Council and for implementing policies related to safety and disaster management. The MOIS enforces laws and regulations, usually in the form of compliance investigations, rulings, and approvals. This includes data and digital services.

Major Reports and Inquiries, and Related Initiatives:

- Electronic Government Act Explained (2022): [Final Report] (In Korean)[6]
- Public Data Management Manual (2021): [Final Report] (In Korean)[7]
- Amendment to the Public Data Act (2021): [Proposal] (In Korean)[8]

*Ministry of Land, Infrastructure and Transport (MOLIT)

Institutional Form: Department (Executive Ministry)

Responsible Minister: The Minister of Land, Infrastructure and Transport

Principal Instrument(s): *Act on the Promotion of and Support for Commercialization of Autonomous Driving Motor Vehicles ("Self-Driving Vehicle Act") (2020), Act on Promotion of Utilization of Drones and Creation of Infrastructure Therefor (2019), Act on the Promotion of Smart City Development and Industry (2008) ("Smart City Act"), Motor Vehicle Management Act (1987)*

Mandate: The MOLIT formulates and coordinates comprehensive plans for national land, including the construction of cities, roads and houses, coastlines, rivers, land reclamation, overland transportation, railroads, and aviation. As part of the Korean New Deal, the MOLIT is focused on building smart cities and hydrogen cities to embrace connecting technologies of the Fourth Industrial Revolution (ICT, Big Data) with urban infrastructures for transport, safety, and energy.

Major Reports, Inquiries, and Related Initiatives:

- Amendment to the Self-Driving Vehicle Act (proposed) (2021): [Proposal] (In Korean)[9]
- Amendment to the Smart City Act (proposed) (2021): [Proposal] (In Korean)[10]
- Ethical Guidelines for Autonomous Vehicles (2020): [Final Report] (In Korean)[11]
- Act on Mobility Activation and Support (proposed) (2020): [Proposal] (In Korean)[12]

Ministry of Science and ICT (MOSICT)

Institutional Form: Department (Executive Ministry)

Responsible Minister: The Minister of Science and ICT

Principal Instrument(s): *Framework Act on Promotion of Data Industry and Data Utilization (2021), Framework Act on Intelligent Informatization (2020), Framework Act on Broadcasting Communications Development (2010), Information and Communications Technology Industry Promotion Act (2009), Communications Secrecy Act (1993), Act on Promotion of Information and Communications Network Utilization and Information Protection (1987), Broadcasting Act (1987), Telecommunications Business Act (1983), Radio Wave Act (1962)*

Mandate: The MOSICT develops, controls, coordinates, and evaluates policies on science and technology, including the protection of information and the convergence and promotion of broadcasting and communications. It also regulates radio airwaves and the information and communications sectors. As part of the Korean New Deal, the MOSICT has been involved with the 'Data Dam Project' to assemble and allow access to high-quality big data that is essential for artificial intelligence applications.

Major Reports, Inquiries, and Related Initiatives:

- Strategy for Realizing Trustworthy Artificial Intelligence in Pursuit of Human-Centred Artificial Intelligence (2021): [Final Report] (In Korean)[13]
- Data Platform Development Strategy Based on Public-Private Partnership (2021): [Final Report] (In Korean)[14]
- Understanding Network Neutrality Policy – Guidelines for Network Neutrality and Internet Traffic Management (2021): [Final Report] (In Korean)[15]
- Blockchain Industry Promotion Act (proposed) (2021): [Proposal] (In Korean)[16]
- Artificial Intelligence Ethics Guideline (2020): [Final Report] (In Korean)[17]
- National Strategy on Artificial Intelligence (2019): [Final Report] (In Korean)[18]
- AI related legislations (proposed) (2021):† [Proposal] (In Korean)[19]

Ministry of SMEs and Startups (MOSS)

Institutional Form: Department (Executive Ministry)

Responsible Minister: The Minister of SMEs and Startups

Principal Instrument(s): *Act on The Fostering of Self-employed Creative Enterprises (2011), Act on Special Measures for The Promotion of Venture Businesses (1997), Framework Act on Small and Medium Enterprises (1966)*

Mandate: The MOSS administers the planning and consolidation of small and medium enterprise (SME) policies to protect and promote SMEs, support start-ups, encourage cooperation between large and small businesses, and protect and support small commercial and industrial entrepreneurs. The MOSS may designate certain markets (sectors) as being an "SME-suitable Industry", which restricts the market entry and activities of non-SMEs in that market. This is a cross-sectional authority that includes the tech industry and related markets and has implications for tech innovation in the digital economy. The MOSS also enforces regulations that sanction and remedy infringement of technology held by SMEs (by larger companies that could include big tech) via the SME Technical Dispute Mediation/Arbitration Committee. To help SMEs develop and commercialise new technologies for the fourth industrial revolution, the MOSS has a research and development support system tailored to the different stages of an SMEs' growth (from start-up to middle-standing companies).

Major Reports, Inquiries, and Related Initiatives: None issued

† Major proposals include, among others, (Proposal) Algorithm and AI Act, (Proposal) AI Industry Promotion Act, (Proposal) Framework Act on the Promotion Of R&D, Industry and Ethical responsibility of AI.

Ministry of Trade, Industry and Energy (MOTIE)

Institutional Form: Department (Executive Ministry)

Responsible Minister: The Minister of Trade, Industry and Energy

Principal Instrument(s): *Intelligent Robot Development and Distribution Promotion Act (2020) (Intelligent Robot Act), Industrial Convergence Promotion Act (2011), Industrial Technology Innovation Promotion Act (1995), Foreign Trade Act (1987)*

Mandate: The MOTIE administers commerce, trade, foreign investment, policies on the research and development of industrial technology and energy and underground resources. It enforces export controls of strategic items in partnership with Defence Acquisition Program Administration and the Nuclear Safety and Security Commission. The MOTIE has established the Industrial Digital Transformation Task Force to promote the digital transformation of key industries and to initiate digital transition across industry. The MOTIE also deliberates regulatory exemptions and temporary permission requests for new, high-tech business models.

Major Reports, Inquiries, and Related Initiatives:

- Introduction to Digital Commerce - Case Studies (2021): [Final Report] (In Korean)[20]
- Amendment to the Intelligent Robot Act (proposed) (2021): [Proposal] (In Korean)[21]

Ministry of Trade, Industry and Energy (MOTIE), Korean Intellectual Property Office (KIPO)

Institutional Form: Governmental agency

Responsible Minister: The Chairperson of KIPO

Principal Instrument(s): *Patent Act (1952*)

Mandate: The KIPO administers duties concerning patents, utility models, designs, and trade marks, and examinations and trials related to such duties to strengthen national competitiveness by establishing new markets.

Major Reports, Inquiries, and Related Initiatives: None issued

National Intelligence Service (NIS)

Institutional Form: Government agency

Responsible Minister: The Director of the NIS

Principal Instrument(s): *National Intelligence Service Act (1961)*

Mandate: The NIS is the executive intelligence agency for the Republic of Korea and reports directly to the President. It provides intelligence, maintains, and monitors national security and cyber security, and conducts criminal investigations. The NIS works with the Korea Internet and Security Agency to enforce compliance with cybersecurity policies.

Major Reports, Inquiries, and Related Initiatives:

- National Cybersecurity White Paper (2021): [Final Report][22]

Korea Internet and Security Agency (KISA)

Institutional Form: Public organisation (established by law)

Responsible Minister: The President of KISA

Principal Instrument(s): *Act on Promotion of Information and Communications Network Utilization and Information Protection (1987)*

Mandate: The KISA is tasked with upgrading information and communications networks, encouraging the safe use of these networks, and promoting international cooperation and advancement into overseas markets in relation to broadcasting and communications. The KISA performs the survey and research of laws, policies, and systems for the use and protection of information and telecommunications networks, It also analyses the negative effects arising from the use of information and telecommunications networks, and identifies countermeasures. The KISA coordinates with government agencies such as the Personal Information Protection Commission, the Ministry of Science and ICT, and National Intelligence Service to implement and enforce compliance with cyber security policies. Cyber security policy for the financial sector is enforced by the Financial Supervisory Service, Financial Services Commission, and Financial Security Agency.

Major Reports, Inquiries, and Related Initiatives:

- Research on the technology of Ethereum 2.0 (2022): [Final Report] (In Korean)[23]
- A study on revision of guidelines for handling pseudonymous information by demonstrating the level of pseudonymization (2022): [Final Report] (In Korean)[24]
- Blockchain-driven Innovative Finance Ecosystem Research (2021): [Final Report] (In Korean)[25]

Financial Services Commission (FSC)

Institutional Form: Independent statutory authority

Responsible Minister: The Chairperson of the FSC

Principal Instrument(s): *Act on Online Investment-linked Financial Business and the Protection of Users (2020), Act on Special Cases Concerning Establishment and Operation of Internet-only Banks (2019), Electronic Financial Transactions Act (2007), Act on Reporting and Using Specified Financial Transaction Information (2001), Act on the Establishment of Financial Services Commission (1998), Credit Information Use and Protection Act (1995)*

Mandate: The FSC formulates financial policies, supervises financial institutions and financial markets, protects consumers, and advances Korea's financial industry. In March 2021, it announced a proposal to amend Korea's anti-money laundering-related law – the *Act on Reporting and Using Specified Financial Transaction Information* – requiring virtual asset service providers to register with the Korea Financial Intelligence Unit and comply with various anti-money laundering obligations.

Major Reports, Inquiries, and Related Initiatives:

- Guideline (Model Rules) on Artificial Intelligence in the Financial Sector (2021): [Final Report] (In Korean)[26]
- Virtual asset related legislation (proposed) (2021): [Proposal] (In Korean)[27]
- Plan for Comprehensive Innovation of Digital Finance (2020): [Final Report] (In Korean)[28]
- Guideline on Pseudonymization and Anonymization in the Financial Sector (2020): [Final Report] (In Korean)[29]
- Amendment to the Electronic Financial Transactions Act (proposed) (2020): [Proposal] (In Korean)[30]

Financial Supervisory Service (FSS)

Institutional Form: Public organisation (established by law)

Responsible Minister: The Governor of FSS

Principal Instrument(s): *Act on the Establishment of Financial Supervisory Organizations (1997)*

Mandate: The FSS conducts supervision of banks, non-bank financial companies, financial investment services providers and insurance companies to ensure they comply with certain safety and soundness guidelines, standards, requirements, and safeguards. The FSS performs capital market supervision, consumer protection, and other supervision and enforcement activities as delegated or charged by the Financial Services Commission. It's Digital Finance Innovation Department is responsible for tasks related to digital technologies, including conducting research on digital assets (e.g., virtual assets), tasks related to FinTech, RegTech and supervising electronic financial services.

Major Reports, Inquiries, and Related Initiatives:

- Global Fintech Trends and Supervisory Policies (2020): [Final Report] (In Korean)[31]
- FSS Annual Report (2020): [Final Report][32]

Korea Communications Commission (KCOMC)

Institutional Form: Independent statutory authority

Responsible Minister: The Chairperson of KCOMC

Principal Instrument(s): *Framework Act on Broadcasting Communications Development (2010), Internet Multimedia Broadcast Services Act (2008), Act on the Protection, Use, etc. of Location Information (2005), Act on Promotion of Information and Communications Network Utilization and Information Protection (1987), Broadcasting Act (1987), Telecommunications Business Act (1983)*

Mandate: The KCOMC regulates the broadcast and communications sector and maintains the independence of broadcast services. The KCOMC develops and implements policies for terrestrial broadcasting, general-service, and news-only program providers. It investigates and imposes sanctions for violations, develops and implements measures that protect users and personal information, and prevents the circulation of illegal or harmful information. It also administers policies on programming, evaluation, and media diversification as well as the arrangement of broadcasting commercials. The KCOMC is amending the *Telecommunications Business Act* to prohibit the forced use of certain in-app payment methods.

Major Reports, Inquiries, and Related Initiatives:

- Amendment to Enforcement Decree of The Telecommunications Business Act (related to in-app payment methods) (2021): [Enforcement Decree] (In Korean)[33]
- Report by the 3rd Committee for the Win-Win Development of the Internet (2020): [Final Report] (In Korean)[34]
- Act on Digital Platform Development and User Protection (proposed) (2020): [Proposal] (In Korean)[35]

Korea Fair Trade Commission (KFTC)

Institutional Form: Independent statutory authority

Responsible Minister: The Chairperson of the KFTC

Principal Instrument(s): *Monopoly Regulation and Fair Trade Act (1980) (MRFTA)*

Mandate: The KFTC regulates competition policy and investigates, deliberates, decides antitrust cases as a quasi-judicial body, and protects consumer rights under the MRFTA. The KFTC has increased its focus on competition in the digital economy and the tech industry, producing legislative proposals and guidelines.

Major Reports, Inquiries, and Related Initiatives:

- Guidelines for Reviewing Abuse of Dominance and Unfair Trade Practices by Online Platforms (proposed) (2022): [Proposal] (in Korean)[36]
- Act on Fairness in Intermediation Transactions by Online Platforms (proposed) (2021): [Proposal] (In Korean)[37]

National Human Rights Commission of Korea (NHRCK)

Institutional Form: Independent statutory authority

Responsible Minister: The Chairperson of the Commission

Principal Instrument(s): *National Human Rights Commission of Korea Act (2001)*

Mandate: The NHRCK protects, advocates, and promotes human rights as an independent authority regarding all human rights issues in Korea. The NHRCK has set human rights standards for an information society through numerous rounds of expert meetings, debates, and symposiums. Focusing on issues of ICTs and Human Rights, such as the right of information privacy, freedom of expression on the internet, right of access to information, and right to enjoy information and culture, the NHRCK has provided recommendations for improving administrative policies and actions to protect and ensure such rights.

Major Reports, Inquiries, and Related Initiatives:

- Report on Countering Hate Speech (2021): [Final Report][38]
- Methods to improve personal data protection laws and regulations in alignment with the EU GDPR and other international human rights standards (2021): [Final Report][39]

Personal Information Protection Commission (PIPC)

Institutional Form: Independent statutory authority

Responsible Minister: The Chairperson of the PIPC

Principal Instrument(s): *Personal Information Protection Act (2011, amended 2020)*

Mandate: The PIPC is responsible for the protection and supervision of personal information. It promotes and improves laws and regulations and establishes and implements policies, systems, and plans. It cooperates with international organisations and data-protection authorities, conducts research, supports and disseminates technology development, and fosters personal information protections. The PIPC also investigates violations of privacy rights and manages complaints and mediation of disputes. Following amendments to the *Personal Information Protection Act* in 2020, the PIPC has been transformed into a central administrative agency.

Major Reports, Inquiries, and Related Initiatives:

- Amendment to the Personal Information Protection Act (proposed) (2022): [Proposal] (In Korean)[40]
- AI Personal Information Protection Self-Checklist (2021): [Final Report][41]
- Personal Information Protection Guidelines for Smart Cities (2021): [Final Report][42]
- Guidelines for Processing Pseudonymized Data (2021): [Final Report][43]

Presidential Committee on the Fourth Industrial Revolution (PCFIR)

Institutional Form: Presidential committee

Responsible Minister: Chairperson of the PCFIR

Principal instrument(s): *Presidential Decree on the Establishment and Operation of the Fourth Industrial Revolution Committee (2021)*

Mandate: The PCFIR develops policy directions, strategies, and action plans across government to support the Fourth Industrial Revolution. It deliberates and coordinates important policy issues related to new technologies, including artificial intelligence and data-related technologies, as well as new industries and services necessary for adapting to the Fourth Industrial Revolution. The PCFIR also runs relevant events to engage with various stakeholders and the public, including the Regulatory and Institutional Reform Hackathon, a public debate hackathon where participants are invited to discuss issues related to the Fourth Industrial Revolution.

Major Reports, Inquiries, and Related Initiatives:

- Korea Data 119 Project (2021): [Final Report][44]
- 4th industrial revolution government recommendations (2019): [Final Report][45]

Endnotes (Republic of Korea)

1. *Cultural Data Creation and Utilization Promotion Act (proposed)* (In Korean), accessed 29 March 2022, https://opinion.lawmaking.go.kr/gcom/nsmLmSts/out/2113494/detailRP.

2. Game Rating and Administration Committee 2020, *GRAC Yearbook 2020 on Rating Classification & Post Management of Game*, accessed 29 March 2022, https://www.grac.or.kr/download/FileDown.aspx?fileName=GRAC+Yearbook+2020+E.pdf.

3. Korea Copyright Commission (KCOPC) 2022, *Analysis on the implementation of the copyright directive on Digital Single Market Directive in European Union* (In Korean), accessed 29 March 2022, www.copyright.or.kr/information-materials/publication/research-report/view.do?brdctsno=50496&pageIndex=1&brdctsstatecode=&brdclasscode=&searchTarget=ALL&nationcode=&brdno=34&noticeYn=&etc1=&searchText=&portalcode=04&servicecode=06&searchkeyword=&portalcode04=.

4. Korea Copyright Commission 2020, *A study to prepare exemptions notice draft for the prohibition on circumvention of technological protection measures* (In Korean), accessed 29 March 2022, www.copyright.or.kr/information-materials/publication/research-report/view.do?brdctsno=47747&pageIndex=2&brdctsstatecode=&brdclasscode=&searchTarget=ALL&nationcode=&brdno=34&noticeYn=&etc1=&searchText=&portalcode=04&servicecode=06&searchkeyword=&portalcode04=.

5. *Amendment of Restriction of Special Taxation Act 2021* (In Korean), press release, accessed 29 March 2022, www.moef.go.kr/nw/nes/detailNesDtaView.do?menuNo=4010100&searchNttId1=MOSF_000000000055951&searchBbsId1=MOSFBBS_000000000028.

6. Ministry of the Interior and Safety 2022, *Electronic Government Act Explained* (In Korean), accessed 29 March 2022, www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000012&nttId=90258.

7. Ministry of the Interior and Safety 2021, *Public Data Management Manual* (In Korean), accessed 29 March 2022, www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000012&nttId=87981.

8. *Amendment to the Public Data Act 2021* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_V2Y1K0B3O1U9Q1T7R1D0C1N3K5A5W1.

9. *Amendment to the Self-Driving Vehicle Act 2021* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_B2A1O0D4T0O6B1J0W2R2P3I9U1R4P3.

10. *Amendment to the Smart City Act 2021* (In Korean), accessed 8 April 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=ARC_D2N1G1Q1F1H9X1V6F0Q3U1J8K4Y0O6.

11. Ministry of Land, Infrastructure and Transport 2020, *Ethical Guidelines for Autonomous Vehicles* (In Korean), accessed 29 March 2022, www.molit.go.kr/USR/policyData/m_34681/dtl.jsp?id=4508.

12. *Act on Mobility Activation and Support 2020* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_Z2L0F0Z9G1U8Y1L7Z5M6T5X8G9S5H4.

13. Ministry of Science and ICT 2021, *Strategy for Realizing Trustworthy Artificial Intelligence in Pursuit of Human-Centered Artificial Intelligence* (In Korean), accessed 29 March 2022, www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&pageIndex=&bbsSeqNo=94&nttSeqNo=3180239&searchOpt=ALL&searchTxt=.

14. *AI related legislations 2021*, accessed 8 April 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_A2J1R1B1R1J0S1V6W3K9B0K6N6Q0Z9. Note: This link relates to one (the most recent) of the 9 bills proposed (and which have not yet lapsed).

15. Ministry of Science and ICT 2021, *Data Platform Development Strategy Based on Public-Private Partnership* (In Korean), accessed 29 March 2022, www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&pageIndex=&bbsSeqNo=94&nttSeqNo=3180352&searchOpt=ALL&searchTxt=.

16. Ministry of Science and ICT 2021, *Understanding Network Neutrality Policy – Guidelines for Network Neutrality and Internet Traffic Management* (In Korean), accessed 29 March 2022, www.msit.go.kr/bbs/view.do?sCode=user&mId=102&mPid=100&pageIndex=&bbsSeqNo=81&nttSeqNo=3148950&searchOpt=ALL&searchTxt=.

17. *Blockchain Industry Promotion Act (proposed)* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_B2U1F0P8T0U5G0Y9Z2S1F4A5P5T7T8.

18. Ministry of Science and ICT 2020, *Artificial Intelligence Ethics Guideline* (In Korean), accessed 29 March 2022, www.msit.go.kr/bbs/view.do?sCode=user&mPid=112&mId=113&bbsSeqNo=94&nttSeqNo=3179742.

19. Ministry of Science and ICT 2019, *National Strategy on Artificial Intelligence* (In Korean), accessed 29 March 2022, www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&pageIndex=1&bbsSeqNo=94&nttSeqNo=2405727&searchOpt=ALL&searchTxt=%EA%B5%AD%EA%B0%80%EC%A0%84%EB%9E%B5.

20. Ministry of Trade, Industry and Energy 2021, *Introduction to Digital Commerce - Case Studies* (In Korean), accessed 29 March 2022, https://motie.go.kr/motie/py/gh/Publication/bbs/bbsView.do?bbs_seq_n=632&bbs_cd_n=30&currentPage=1&search_key_n=&cate_n=&dept_v=&search_val_v=.

21. *Amendment to the Intelligent Robot Act 2021* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_X2H1Y0P2A2B5I0K9P4I7X1I4F0Y1U5.

22. National Intelligence Service 2021, *National Cybersecurity White Paper*, accessed 29 March 2022, www.nis.go.kr:4016/AF/1_7_7_1.do?currentPage=1.

23. Korea Internet and Security Agency 2022, *Research on the technology of Ethereum 2.0* (In Korean), accessed 29 March 2022, www.kisa.or.kr/201/form?postSeq=12037&page=1.

24. Korea Internet and Security Agency 2022, *A study on revision of guidelines for handling pseudonymous information by demonstrating the level of pseudonymization* (In Korean), accessed 29 March 2022, www.kisa.or.kr/201/form?postSeq=12034&page=1.

25. Korea Internet and Security Agency 2021, *Blockchain-driven Innovative Finance Ecosystem Research* (In Korean), accessed 29 March 2022, www.kisa.or.kr/201/form?postSeq=0224&page=1.

26. Financial Services Commission 2021, *Guideline (Model Rules) on Artificial Intelligence in the Financial Sector* (In Korean), accessed 29 March 2022, www.fsc.go.kr/no010101/76206.

27. Financial Services Commission 2021, *Virtual asset related legislation (proposed)* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_K2T1V0H6U0L9M0X9A4W8A3G0W7Q6H1.

28. Financial Services Commission 2020, *Plan for Comprehensive Innovation of Digital Finance* (In Korean), accessed 29 March 2022, www.korea.kr/news/pressReleaseView.do?newsId=156402911#sitemap-layer.

29. Financial Services Commission 2020, *Guideline on Pseudonymization and Anonymization in the Financial Sector* (In Korean), accessed 29 March 2022, www.fsc.go.kr/no010101/74483.

30. *Amendment to the Electronic Financial Transactions Act (proposed)* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_R2Y0P1Y1P2W7K1W7I5D8X0O7Q2R3T3.

31. Financial Supervisory Service 2020, *Global Fintech Trends and Supervisory Policies* (In Korean), accessed 29 March 2022, www.fss.or.kr/fss/bbs/B0000080/view.do?nttId=35597&menuNo=200395&pageIndex=1.

32. Financial Supervisory Service 2020, *FSS Annual Report*, accessed 29 March 2022, www.fss.or.kr/eng/bbs/B0000215/view.do?nttId=42385&menuNo=400011&pageIndex=1.

33. *Amendment to Enforcement Decree of The Telecommunications Business Act (related to in-app payment methods)* (In Korean), accessed 29 March 2022, https://kcc.go.kr/user.do?mode=view&page=E04010000&dc=E04010000&boardId=1058&cp=1&boardSeq=52182.

34. Korea Communications Commission 2020, *Report by the 3rd Committee for the Win-Win Development of the Internet* (In Korean), accessed 29 March 2022, https://kcc.go.kr/user.do?mode=view&page=A02050200&dc=K02050200&boardId=1025&cp=2&boardSeq=50593.

35. Korea Communications Commission 2020, *Act on Digital Platform Development and User Protection (proposed)* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_F2L0A1F1D2T7J1W6Y5I1A0V1R6U9T2.

36. Korean Fair Trade Commission 2022, *Guidelines for Reviewing Abuse of Dominance and Unfair Trade Practices by Online Platforms*, accessed 8 April 2022, www.ftc.go.kr/www/selectReportUserView.do?key=10&rpttype=1&report_data_no=9432.

37. *Act on Fairness in Intermediation Transactions by Online Platforms 2021* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_T2M1G1P1T2N2F1S5K5N2M3Z2W4N5Q9.

38. National Human Rights Commission of Korea 2021, *Report on Countering Hate Speech(2019-2020)*, accessed 29 March 2022, www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003002&pagesize=10&boardtypeid=7019&boardid=7606214.

39. National Human Rights Commission of Korea 2021, *Methods to improve personal data protection laws and regulations in alignment with the EU GDPR and other international human rights standards* (In Korean), accessed 29 March 2022, www.humanrights.go.kr/site/program/board/basicboard/view?menuid=001003001004001&pagesize=10&boardtypeid=16&boardid=7606166.

40. Personal Information Protection Commission 2022, *Amendment to the Personal Information Protection Act (proposed)* (In Korean), accessed 29 March 2022, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_A2G1C1Q2M2L8P1Q4P5C7S3C8O3E5W6.

41. Personal Information Protection Commission 2021, *AI Personal Information Protection Self-Checklist*, accessed 29 March 2022, www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do.

42. Personal Information Protection Commission 2021, *Personal Information Protection Guidelines for Smart Cities*, accessed 29 March 2022, www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=7777.

43. Personal Information Protection Commission 2021, *Guidelines for Processing Pseudonymized Data*, accessed 29 March 2022, www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=7622.

44. Presidential Committee on the 4th Industrial Revolution 2021, *Korea Data 119 Project*, accessed 29 March 2022, www.4th-ir.go.kr/article/detail/1221?boardName=internalData&category=relation.

45. Presidential Committee on the Fourth Industrial Revolution 2019, *4th industrial revolution government recommendations*, accessed 29 March 2022, www.4th-ir.go.kr/source/recommendation.pdf.

Singapore

Benjamin Ang and Sithuraj Ponraj, Nanyang Technological University

Competition and Consumer Commission of Singapore (CCCS)

Institutional Form: Statutory board

Responsible Minister: The Minister for Trade and Industry

Principal Instrument(s): *Competition Act (2004), Consumer Protection (Fair Trading) Act (2003)*

Mandate: The CCCS is Singapore's competition regulator. It investigates and enforces against practices that have an adverse effect on competition and protects consumers against unfair trade practices in Singapore. The CCCS also advises the government and other public authorities on national needs and policies related to competition matters. The CCCS represents Singapore with respect to competition matters in the international arena.

Major Reports, Inquiries, and Related Initiatives:

- Competition Act (2004): [Act][1]
- Consumer Protection (Fair Trading) Act (2003): [Act][2]

Cyber Security Agency of Singapore (CSA)

Institutional Form: Government department

Responsible Minister: The Minister for Communications and Information and the Minister-in-charge of Smart Nation and Cybersecurity

Principal Instrument(s): *Cybersecurity Act (2018)*

Mandate: The CSA is responsible for cyber security strategy, operations, education, outreach, and ecosystem development. The CSA administers the *Cybersecurity Act* and its chief executive serves as the Commissioner of Cybersecurity. Recent initiatives launched by the CSA as part of its mandate include the *Singapore's Operational Technology Cybersecurity Masterplan 2019,* the Cybersecurity Code of Practice for Critical Information Infrastructure, and three certification schemes for providing security assurance for cyber security products, including the Cybersecurity Labelling Scheme for consumer smart devices.

Major Reports, Inquiries, and Related Initiatives:

- Cybersecurity Certification Guide (2021): [Guidance][3]
- Singapore Cybersecurity Strategy (2021): [Strategy][4]
- Singapore's Operational Technology Cybersecurity Masterplan (2019): [Guidance][5]
- Cybersecurity Code of Practice for Critical Information Infrastructure (2019): [Code of Practice][6]

Intellectual Property Office of Singapore (IPOS)

Institutional Form: Statutory board

Responsible Minister: The Minister for Law

Principal Instrument(s): *Intellectual Property (Amendment) Act (2022), Copyright Act (2021)*

Mandate: The IPOS administers intellectual property rights in Singapore. Recent amendments to the *Intellectual Property (Amendment) Act* improved the intellectual property registration process. Specific to technology, the IPOS introduced the SG IP Fast Track Programme in 2020 to accelerate patent applications across technology fields within 6 months from filing.

Major Reports, Inquiries, and Related Initiatives:

- Intellectual Property (Amendment) Act (2022): [Act][7]
- Copyright Act (2021): [Act][8]

Infocomm Media Development Authority (IMDA)

Institutional Form: Statutory board

Responsible Minister: The Minister for Communications and Information and the Minister-in-charge of Smart Nation and Cybersecurity

Principal Instrument(s): *Protection from Online Falsehoods and Manipulation Act (2019), Info-Communications Media Development Authority Act (2016, amended 2020), Personal Data Protection Act (2012), Electronic Transactions Act (2010), Telecommunications Act (1999)*

Mandate: The IMDA develops and regulates the infocomm and media sectors in a holistic way, through an emphasis on talent, research, innovation, and enterprise. As a statutory board in the Singapore government, it seeks to deepen regulatory capabilities for a converged infocomm media. As part of its mandate, IMDA enforces the *Telecommunications Act* that regulates the licensing of telecom systems and services and grant of spectrum rights, among other matters. It also enforces the *Electronic Transactions Act (amended in 2021)* that covers matters such as electronic records, signatures, and contracts. As part of its broader remit, the IMDA issued an updated Model Artificial Intelligence Governance Framework that provides guidance to private-sector organisations on ethical and governance issues when deploying artificial intelligence solutions. An Advisory Council on the Ethical Use of AI and Data was set up in 2018 to advise the Government on issues arising from commercial deployment of artificial intelligence that may require policy or regulatory intervention. Members comprise international industry leaders in artificial intelligence, advocates of social and consumer interests, and leaders of local companies who are keen to make use of artificial intelligence.

Major Reports, Inquiries, and Related Initiatives:

- Electronic Transactions Act (2021): [Act][9]
- Model Artificial Intelligence Governance Framework (2020): [Framework][10]
- Digital Economy Framework for Action (2018): [Strategy][11]
- Services and Digital Economy Technology Roadmap (2018): [Roadmap][12]

Infocomm Media Development Authority, Personal Data Protection Commission (PDPC)

Institutional Form: Commission within a statutory board

Responsible Minister: The Minister for Communications and Information and the Minister-in-charge of Smart Nation and Cybersecurity

Principal Instrument(s): *Info-Communications Media Development Authority Act (2016, amended 2020), Personal Data Protection Act (2012, amended 2020)*

Mandate: The PDPC regulates the collection, use, disclosure, and protection of personal data used by organisations, including online personal data.

Major Reports, Inquiries, and Related Initiatives:

- Personal Data Protection Act (2012): [Act][13]

Infocomm Media Development Authority, Protection from Online Falsehoods and Manipulation Act Office (POFMA)

Institutional Form: Office within a statutory board

Responsible Minister: The Minister for Communications and Information and Minister-in-charge of Smart Nation and Cybersecurity

Principal Instrument(s): *Protection from Online Falsehoods and Manipulation Act (2019)*

Mandate: The POFMA is part of Singapore's whole-of-government approach to counter the proliferation of online falsehoods. The POFMA issued codes of practices to provide guidance to internet intermediaries and digital advertising intermediaries about systems and processes to prevent and counter the misuse of online accounts. The POFMA works to improve the transparency of political advertising and 'de-prioritise' online falsehoods by providing a list of prescribed intermediaries subject to the codes of practice.

Major Reports, Inquiries, and Related Initiatives:

- Code of Practice for Giving Prominence to Credible Online Sources of Information (2019): [Code of Practice][14]
- Code of Practice for Transparency of Online Political Advertisements (2019): [Code of Practice][15]
- Code of Practice for Preventing and Countering Abuse of Online Accounts (2019): [Code of Practice][16]
- Protection from Online Falsehoods and Manipulation Act (2019): [Act][17]

Monetary Authority of Singapore (MAS)

Institutional Form: Statutory board

Responsible Minister: The Prime Minister

Principal Instrument(s): *Monetary Authority of Singapore Act (1970)*

Mandate: The MAS is Singapore's central bank and integrated financial regulator. The MAS develops guidance on digital banking, digital and crypto currencies, and banking cyber security. The MAS issued an Internet Banking Framework in 2000, and an Eligibility Criteria and Requirements for Digital Banks in 2019. In 2016, the MAS launched a FinTech Regulatory Sandbox framework to encourage and enable experimentation of technology innovation to deliver financial products and services. The Regulatory Sandbox was enhanced with Sandbox Express in 2019 to provide firms with a faster option for market testing in predefined environments. The MAS announced a Sandbox Plus that took effect on 1 January 2022. The MAS has also announced initiatives including the 2021 Project Orchid, which builds the foundational digital infrastructure for central-bank-issued digital currency (CBDCs) and blueprint for a future digital currency-ready platform. The MAS also issued policy research papers on CBDCs. In 2021, the MAS revised the *Technology Risk Management Guidelines* to keep pace with emerging technologies and shifts in the cyber-threat landscape. The MAS also issued a set of legally binding *Notice of Cyber Hygiene* that sets out that financial institutions have to comply with to mitigate the risk of cyber threats.

Major Reports, Inquiries, and Related Initiatives:

- FAQs on MAS FinTech Regulatory Sandbox Framework (2021): [Overview][18]
- The Future of Money, Finance and the Internet – Speech by Mr Ravi Menon, Managing Director, Monetary Authority of Singapore, at Singapore FinTech Festival on 9 November 2021: [Speech][19]
- A Retail Central Bank Digital Currency: Economic Considerations in the Singapore Context (2021): [Policy Paper][20]
- Revised Technology Risk Management Guidelines (2021): [Guidelines][21]
- Eligibility Criteria and Requirements for Digital Banks in 2019: [Criteria and Requirements][22]

Singapore Customs

Institutional Form: Government department

Responsible Minister: The Minister for Finance

Principal Instrument(s): *Strategic Goods Control Act (2002)*

Mandate: Singapore Customs is responsible for trade facilitation and revenue enforcement. It regulates and controls the transfer and brokering of strategic goods, strategic goods technology, and goods and technology that could be used to develop, produce, operate, stockpile or acquire weapons capable of causing mass destruction as well as missiles capable of delivering such weapons. The *Strategic Goods Control Regulations* support the implementation of the act including permit procedures for legitimate activities and the conditions for approval, revocation, or suspension of permits.

Major Reports, Inquiries, and Related Initiatives:

- Strategic Goods (Control) Order (2021): [Subsidiary Legislation][23]
- Strategic Goods (Control) Regulations (2006): [Subsidiary Legislation][24]
- Strategic Goods (Control) Act (2002) (Revised Edition) (2020): [Act][25]

Singapore Police Force (SPF)

Institutional Form: Government department

Responsible Minister: The Minister for Home Affairs

Principal Instrument(s): *Foreign Interference (Countermeasures) Act (2021), Protection from Harassment (Amendment) Act (2019), Penal Code; Computer Misuse and Cybersecurity Act (1993, amended 2017)*

Mandate: The SPF oversees Singapore's public law and order and law enforcement functions. It enforces relevant provisions of the Penal Code and the *Computer Misuse Act*, which criminalises unauthorised access or modification of computer material as well as other computer crimes. The SPF enforces the *Protection from Harassment (Amendment) Act*, which criminalises, among other things, cyber bullying, unlawful stalking and harassment within and outside of the workplace, and doxing. It also provides measures to address the spread of online falsehoods affecting people and established the POHA court. The SPF also enforces the *Foreign Interference (Countermeasures) Act* to prevent, detect, and disrupt the use of hostile information campaigns and local proxies by foreign entities that interfere in domestic politics, including using online technologies.

Major Reports, Inquiries, and Related Initiatives:

- Foreign Interference (Countermeasures) Act (2021) (2020 Revised Edition): [Act][26]
- Protection from Harassment (Amendment) Act (2014) (2020 Revised Edition): [Act][27]
- Computer Misuse and Cybersecurity Act (2017): [Act][28]

Endnotes (Singapore)

1. *Competition Act (2004)*, accessed 30 March 2022, https://sso.agc.gov.sg/Act/CA2004.

2. *Consumer Protection (Fair Trading) Act (2003)*, accessed 30 March 2022, https://sso.agc.gov.sg/Act/CPFTA2003.

3. Cyber Security Agency of Singapore 2021, *Cybersecurity Certification Guide*, accessed 30 March 2022, www.csa.gov.sg/-/media/Csa/Documents/CLS/CSA-Cybersecurity-Certification-Guide.pdf.

4. Cyber Security Agency of Singapore 2021, *Singapore Cybersecurity Strategy*, accessed 30 March 2022, www.csa.gov.sg/-/media/Csa/Documents/Publications/The-Singapore-Cybersecurity-Strategy-2021.pdf.

5. Cyber Security Agency of Singapore 2019, *Operational Technology (OT) Cybersecurity Masterplan*, accessed 30 March 2022, www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan.

6. Cyber Security Agency of Singapore 2019, *Cybersecurity Code of Practice for Critical Information Infrastructure*, accessed 30 March 2022, www.csa.gov.sg/-/media/Csa/Documents/Legislation_COP/cybersecurity-code-of-practice-cii-dec-2019.pdf.

7. *Intellectual Property (Amendment) Bill 2021*, accessed 29 March 2022, https://sso.agc.gov.sg/Bills-Supp/39-2021/Published/20211101?DocDate=20211101.

8. *Copyright Act (2021)*, accessed 30 March 2022, https://sso.agc.gov.sg/Acts-Supp/22-2021/Published/.

9. *Electronic Transactions Act (2010) (2020 Revised Edition)*, accessed 30 March 2022, https://sso.agc.gov.sg/Act/ETA2010.

10. Infocomm Media Development Authority and Personal Data Protection Commission 2020, *Model Artificial Intelligence Governance Framework*, accessed 30 March 2022, https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.ashx.

11. Infocomm Media Development Authority 2018, *Digital Economy Framework for Action*, accessed 30 March 2022, www.imda.gov.sg/-/media/Imda/Files/SG-Digital/SGD-Framework-For-Action.pdf.

12. Infocomm Media Development Authority 2018, *The Future of Services: Service and Digital Economy Technology Roadmap*, accessed 30 March 2022, www.imda.gov.sg/-/media/Imda/Files/Industry-Development/Infrastructure/Technology/Technology-Roadmap/SDE-TRM-Main-Report.pdf.

13. *Personal Data Protection Act (2012) (2020 Revised Edition)*, accessed 30 March 2022, https://sso.agc.gov.sg/Act/PDPA2012.

14. Protection from Online Falsehoods and Manipulation Act Office 2019, *Code of Practice for Giving Prominence to Credible Online Sources of Information*, accessed 30 March 2022, www.pofmaoffice.gov.sg/documents/Prominence Code.pdf.

15. Protection from Online Falsehoods and Manipulation Act Office 2019, *Code of Practice for Transparency of Online Political Advertisements*, accessed 30 March 2022, www.pofmaoffice.gov.sg/documents/Political%20Advertisements%20Code%20and%20Annex.pdf.

16. Protection from Online Falsehoods and Manipulation Act Office 2019, *Code of Practice for Preventing and Countering Abuse of Online Accounts*, accessed 30 March 2022, www.pofmaoffice.gov.sg/documents/Online%20Accounts%20Code%20and%20Annex.pdf.

17. *Protection from Online Falsehoods and Manipulation Act (2019)*, accessed 30 March 2022, https://sso.agc.gov.sg/Act/POFMA2019?TransactionDate=20191001235959.

18. Monetary Authority of Singapore 2021, *FAQs on MAS FinTech Regulatory Sandbox Framework*, accessed 30 March 2022, www.mas.gov.sg/-/media/MAS-Media-Library/development/Regulatory-Sandbox/FAQsNov2021.pdf?la=en&hash=075D18DC2B19BD6BCB5A98D1B974666736F87553.

19. Menon, R 2021, 'The Future of Money, Finance and the Internet', transcript, *Singapore FinTech Festival* on 9 November, speech, 9 November 2021, accessed 30 March 2022, www.mas.gov.sg/news/speeches/2021/the-future-of-money-finance-and-the-internet.

20. Monetary Authority of Singapore 2021, *A Retail Central Bank Digital Currency: Economic Considerations in the Singapore Context*, accessed 30 March 2022, www.mas.gov.sg/-/media/MAS/EPG/Monographs-or-Information-Paper/A-retail-CBDC---Economic-Considerations-in-the-Singapore-Context.pdf.

21. Monetary Authority of Singapore 2021, *Technology Risk Management Guidelines*, accessed 30 March 2022, www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf?la=en&hash=607D03D8FD460EBDA89FC2634E25C09B5D0ADDA3.

22. Monetary Authority of Singapore 2019, *Eligibility Criteria and Requirements for Digital Banks in 2019*, accessed 30 March 2022, www.mas.gov.sg/-/media/Digital-Bank-Licence/Eligibility-Criteria-and-Requirements-for-Digital-Banks.pdf?la=en&hash=57410B76A3359791816B0A0BD592DF8EF2D37B33.

23. *Strategic Goods (Control) Order (2021)*, accessed 30 March 2022, https://sso.agc.gov.sg/SL-Supp/S564-2021/Published/20210802?DocDate=20210802.

24. *Strategic Goods (Control) Regulations (2021)*, accessed 30 March 2022, https://sso.agc.gov.sg/SL/SGCA2002-RG1?DocDate=20180904#legis.

25. *Strategic Goods (Control) Act (2002) (Revised Edition) (2020)*, accessed 30 March 2022, https://sso.agc.gov.sg/Act/SGCA2002.

26. *Foreign Interference (Countermeasures) Act (2021) (2020 Revised Edition)*, accessed 30 March 2022, https://sso.agc.gov.sg/Acts-Supp/28-2021/Published/20211125?DocDate=20211125.

27. *Protection from Harassment (Amendment) Act (2014) (2020 Revised Edition)*, accessed 30 March 2022, https://sso.agc.gov.sg/Act/PHA2014.

28. *Computer Misuse and Cybersecurity Act (2017)*, accessed 30 March 2022, https://sso.agc.gov.sg/Acts-Supp/22-2017/Published/20170511170000?DocDate=20170511170000.

United Kingdom*

Dr Jose Tomas Llanos, University College London

Bank of England (BoE)

Institutional Form: Independent statutory authority

Responsible Minister: The Chancellor of the Exchequer

Principal Instrument(s): *Financial Services Act (2012), Banking Act (2009), Financial Services and Markets Act (2000), Charter (1998); Bank of England Act (1998)*

Mandate: The BoE is the central bank in the United Kingdom. It implements monetary policy, maintains financial stability, and provides a safe environment for the use of money. Through its subsidiary, the Prudential Regulation Authority (PRA), the BoE enforces prudential regulation and exerts oversight over banks, building societies, credit unions, insurers, and other financial services. Together with the Financial Conduct Authority (FCA), the PRA reduced barriers to entry that arise from capital requirements, thereby allowing for the authorisation of banks with highly innovative business models.† Given emerging digital technologies' potentially beneficial and harmful effects on financial stability, the BoE has been actively involved in fintech innovation, launching important initiatives such as the Fintech Accelerator Programme. Also, to improve its supervisory functions and ensure financial resiliency, the BoE has been piloting new data-driven approaches in areas such as natural language processing, machine learning, and artificial intelligence.

Major Reports, Inquiries, and Related Initiatives:

- New forms of digital money (2021): [Discussion Paper][1]
- The impact of machine learning and big data on credit markets (2021): [Staff Working Paper][2]
- Central Bank Digital Currency: Opportunities, challenges and design (2020): [Discussion Paper][3]
- The Impact of Covid on machine learning and data science in UK banking (2020): [Bulletin][4]
- Open data for SME finance: what we proposed and what we have learnt (2020): [Final Report][5]
- Machine Learning in UK financial services (2019): [Final Report][6]

* This overview includes regulators with competence over the United Kingdom. Regulators that are specific to the Wales, Scotland and Northern Ireland (e.g., the Scottish Information Commissioner) are not included.

† For example, Atom Bank, an app-only bank where customers can only access services via smartphones and not through internet or telephone banking. Also, Tandem Bank, a digital-only retail bank that operates a personal finance guide that compares financial products offered by Tandem and its competitors. www.gov.uk/government/publications/data-ethics-framework

*Biometrics and Surveillance Camera Commissioner (BSCC)

Institutional Form: Independent statutory authority

Responsible Minister: The Secretary of State for the Home Department

Principal Instrument(s): *Data Protection Act (2018), UK GDPR (2016), Protection of the Freedoms Act (2012), Police and Criminal Evidence Act (1984)*

Mandate: The BSCC keeps under review the retention and use by the police of DNA samples, DNA profiles and fingerprints, decides applications by the police to retain DNA profiles, fingerprints, and reviews national security determinations (NSD)‡ that are made or renewed by the police in connection with the retention of DNA profiles and fingerprints. The BSCC has no enforcement or inspection powers regarding surveillance cameras. Rather, its role in this area is limited to encouraging compliance with the Surveillance Camera Code of Practice, dealing with technical standards, liaising with academia and industry, and delivering certification schemes.

Major Reports, Inquiries, and Related Initiatives:

- Update to Surveillance Camera Code of Practice (2022): [Guidance][7]
- Consultation: Surveillance camera code of practice (2021): [Consultation Webpage][8]
- Secure by default: self-certification of video surveillance systems (2021): [Form and Guidance Webpage][9]
- Surveillance camera code of practice: third-party certification scheme (2021): [Guidance Webpage][10]
- National surveillance camera strategy for England and Wales (2020): [Webpage][11]

Competition and Markets Authority (CMA)

Institutional Form: Non-ministerial government department

Responsible Minister: Not applicable

Principal Instrument(s): *Enterprise and Regulatory Reform Act (2013), Enterprise Act (2002), Competition Act (1998)*

Mandate: The CMA enforces the *Competition Act* and a range of consumer protection legislation, investigating mergers that may lead to a substantial lessening of competition and potential violations of competition law (e.g., abuse of dominance, cartels), and promoting stronger competition in regulated industries (e.g., gas, electricity, water, aviation, rail, communications, and health). Government proposals for a new pro-competition regime for digital markets contemplate the creation of the Digital Markets Unit, which for now (i.e., until the enabling legislation is enacted) has been established within the CMA on a non-statutory basis in order to focus on operationalising and preparing for the new regime (e.g., gathering evidence on digital markets and carrying out preparatory work to implement the upcoming regime). The CMA updated its Digital Markets Strategy and completed a broad inquiry into online platforms and digital advertising, assessing the effectiveness of competition in these markets, including the role of advertising revenue in the business model of Google and Facebook. The CMA concluded that competition is not healthy within these markets. The CMA has recommended that government pass law to establish a new pro-competition regime.

Major Reports, Inquiries, and Related Initiatives:

- Mobile ecosystem market study (ongoing): [Interim Report][12]
- Algorithms: How they can reduce competition and harm consumers (2021): [Final Report][13]
- Final report of market study into online platforms and digital advertising (2020): [Final Report][14]
- Advice of the Digital Markets Taskforce (2020): [Final Report][15]

‡ Made by chief police officers, NSDs are highly exceptional measures that are used to retain the biometric material of individuals who, while never having been convicted of any offences, are nonetheless believed to present such a threat to our national security that retention of their biometrics is deemed necessary by the police and the Security Service.

*Data Standards Authority (DSA)

Institutional Form: Department agency

Responsible Minister: The Prime Minister

Principal Instrument(s): *Data Protection Act (2018), Digital Economy Act (2017), UK GDPR (2016)*

Mandate: The DSA improves how the public sector manages data. Its establishment in 2020 was in line with the United Kingdom's *National Data Strategy*, which describes the potential of government data and recognises the government's need to change the way that data is used, reused, and shared. Thus, the DSA sets cross-government data standards by identifying which areas benefit most from standardisation, develops standards for wider adoption, sets direction and best practice for data standards in government. The aim of the standards is to produce data that can be easily found, accessed, shared responsibly, and combined as a means for improving public services through stronger policies, analysis, and insights.

Major Reports, Inquiries, and Related Initiatives:

- Catalogue of data standards endorsed by the DSA (ongoing): [Webpage][16]
- Draft Access and record address data using the UPRN standard and AddressBase (ongoing): [Guidance Webpage][17]
- API Standards (ongoing): [Guidance Webpage][18]
- Draft Using GraphQL for your API (ongoing): [Guidance Webpage][19]
- Publish reference data for use across government (2021): [Guidance Webpage][20]
- Develop your data and APIs using a reference architecture (2021): [Guidance Webpage][21]
- Technology Code of Practice point 10 – Make better use of data (2021): [Guidance Webpage][22]
- Data Standards Authority Strategy 2020 to 2023 (2021): [Guidance Webpage][23]

Department for Business, Energy and Industrial Strategy (BEIS)

Institutional Form: Ministerial department

Responsible Minister: The Secretary of State for BEIS

Principal Instrument(s): *National Security and Investment Act (2021)*

Mandate: The BEIS is responsible for business, industrial strategy, science, research and innovation, energy and clean growth, and climate change. It has powers of oversight of, and intervention in, investments for the purposes of protecting national security. In particular, the Secretary of State for BEIS is called upon to assess - and block if applicable - acquisitions of assets across 17 sensitive areas of the economy, including artificial intelligence, computing hardware, cryptographic authentication, data infrastructure, and quantum technologies. Notifiable acquisitions must be approved by the Secretary of State before their completion. A notifiable acquisition that is completed without prior approval is void and of no legal effect.

Major Reports, Inquiries, and Related Initiatives:

- National Security and Investment Act: guidance on notifiable acquisitions (2022): [Guidance][24]
- The National Security and Investment Act alongside regulatory requirements (2022): [Guidance][25]
- How the National Security and Investment Act could affect people or acquisitions outside the UK (2022): [Guidance][26]
- National Security and Investment Act (2021): [Act][27]

Department for International Trade (DIT) and Her Majesty's Revenue and Customs (HRMC)

Institutional Form: Ministerial department (DIT), non-ministerial department (HRMC)

Responsible Minister: The Secretary of State for DIT (DIT), First Permanent Secretary and Chief Executive (HMRC)

Principal Instrument(s): *Export Control Order (2008), Commissioners for Revenue and Customs Act (2005), Export Control Act (2002)*

Mandate: The DIT has responsibility for the statutory and regulatory framework of export controls, and for decisions to grant or refuse an export licence. Licence applications related to military and dual-use items, including computers, software, and technology (i.e., any information necessary for the development, production, or use of controlled goods) must be made through the SPIRE system, which is managed by the Export Control Joint Unit (ECJU), one of the DIT's branches. Inspectors from the ECJU conduct compliance audits to find irregularities, which are then acted upon by HMRC, the entity responsible for the enforcement of strategic export controls.

Major Reports, Inquiries, and Related Initiatives:

- Strategic export controls: licensing data (2022): [Guidance Webpage][28]
- Open general export licences for overseas access to software and technology for military goods (2021): [Guidance Webpage][29]
- Using SPIRE to get an export licence (2021): [Guidance Webpage][30]
- Open Banking – TPP Customer Survey 2021 (2021): [Report][31]
- Export controls: military goods, software and technology (2021): [Guidance Webpage][32]

*Digital Economy Council

Institutional Form: Non-statutory committee

Responsible Minister: The Secretary of State for Digital, Culture, Media and Sports (DCMS)

Principal Instrument(s): Not applicable

Mandate: The Digital Economy Council is an advisory committee of independent members set up to provide advice to the government on digital and tech-policy, including relevant strategies. It is intended to harness the expertise of industry and the wider tech community to identify the priorities, opportunities, and challenges for the United Kingdom's tech sector as a means for implementing the Digital Strategy.[33] The Digital Economy Council provides a forum for open dialogue and the exchange of ideas between industry, academia, and government.

Major Reports, Inquiries, and Related Initiatives: None issued

Digital Regulation Cooperation Forum (DRCF)

Institutional Form: Forum comprised of the CMA, the ICO, Ofcom and the FCA

Responsible Minister: Not applicable

Principal Instrument(s): Not applicable

Mandate: The DRCF was established to ensure a greater level of cooperation among its members given the unique challenges posed by regulation of online platforms. Its objectives are to advance a coherent regulatory approach, inform regulatory policymaking, enhance regulatory capabilities, anticipate future developments, promote innovation, and strengthen international engagement. In the DRCF workplace for 2021–22, the DRCF set out a roadmap for how its members will increase the scope and scale of their cooperation on online regulatory matters of mutual importance.

Major Reports, Inquiries, and Related Initiatives:

- Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022 (2021): [Policy Paper][34]
- Embedding coherence and cooperation in the fabric of digital regulators (2021): [Document][35]
- Digital Regulation Cooperation Forum workplan 2021/22 (2021): [Workplan][36]
- Joining up on future technologies (2021): [Policy Paper][37]
- Digital Regulation Cooperation Forum launch document (2020): [Launch Document][38]

Equality and Human Rights Commission (EHRC)

Institutional Form: Independent statutory authority

Responsible Minister: The Prime Minister

Principal Instrument(s): *Equality Act (2010) (Specific Duties) Regulations (2011), Equality Act (2006), Equality Act (2010), Human Rights Act 1998*

Mandate: The EHRC safeguards and enforces people's rights to fairness, dignity, and respect, including in digital environments. It protects equality across nine areas of age, disability, sex, race, religion and belief, pregnancy and maternity, marriage and civil partnership, sexual orientation, and gender reassignment. In the context of digital technologies, the EHRC has called for the suspension of the use of automated facial recognition and predictive algorithms in policing in England and Wales until their impact has been independently scrutinised, and laws are improved.

Major Reports, Inquiries, and Related Initiatives:

- Civil and political rights in Great Britain: submission to the UN (2020): [Final Report][39]

Financial Conduct Authority (FCA)

Institutional Form: Independent statutory authority

Responsible Minister: The Chancellor of the Exchequer

Principal Instrument(s): *Payment Services Regulations (2017), Financial Services Act (2012), Electronic Money Regulations (2011), Financial Services and Markets Act (2000)*

Mandate: The FCA is the conduct regulator of financial services firms and financial markets in the United Kingdom. Its operational objectives include securing an appropriate degree of protection for consumers, protecting, and enhancing the integrity of the United Kingdom's financial system, and promoting effective competition in the interests of consumers. The Payment Systems Regulator, a subsidiary of the FCA, is the independent economic regulator for the payment systems industry in the United Kingdom, including online payment systems. Through initiatives implemented within the context of its Project Innovate – such as the Regulatory Sandbox – the FCA encourages innovation in the interest of consumers, particularly in the areas of FinTech and RegTech.

Major Reports, Inquiries, and Related Initiatives:

- Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money – Our Approach' and the Perimeter Guidance Manual (2021): [Consultation Paper][40]
- Using online experiments for behaviourally informed consumer policy (2020): [Webpage][41] [Occasional Paper][42]
- Fostering innovation through collaboration: The evolution of the FCA TechSprint Approach (2020): [Final Report][43]
- Crypto-asset consumer research (2020): [Research Note][44]
- Understanding consumer financial wellbeing though banking data (2020): [Occasional Paper][45]
- The impact and effectiveness of Innovate (2019): [Final Report][46]
- Machine learning in UK Financial services (2019): [Research Note][47]
- Cyber security – industry insights (2019): [Final Report][48]

Information Commissioner's Office (ICO)

Institutional Form: Independent statutory authority

Responsible Minister: The Secretary of State for Digital, Culture Media and Sport (DCMS)

Principal Instrument(s): *Data Protection Act (2018), UK GDPR (2016), Investigatory Powers Act (2016), Privacy and Electronics Communications (EC Directive) Regulations (2003) (as amended), Network and Information Systems Regulations (2018), Freedom of Information Act (2000)*

Mandate: The ICO is the regulator for data protection and freedom of information. Its mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO conducts investigations, handles complaints and data breach reports, imposes fines and other sanctions in cases of data protection infringements, and provides guidance on data protection matters. Through the Innovation Hub, the ICO helps innovators build privacy-by-design into their new products, tailoring the support it gives to each partner and project.

Major Reports, Inquiries, and Related Initiatives:

- Investigation into data protection compliance in the direct marketing data broking sector (2021): [Report][49]
- COVID-19 and information rights: reflections and lessons learnt from the Information Commissioner (2021): [Report][50]
- Global Privacy Enforcement Network (GPEN) report - Resetting Privacy (2021): [Report][51]
- ICO Innovation Hub project report (2020): [Report][52]
- Update report into adtech and real time bidding (2019): [Update Report][53]

Intellectual Property Office (IPO)

Institutional Form: Executive agency of the Department for BIES

Responsible Minister: The Minister of State for Energy and Intellectual Property

Principal Instrument(s): *Trade Marks Act (1994), Copyright, Designs and Patents Act (1988), Patents Act (1977), Registered Designs Act (1949), Patents and Designs Act (1907)*

Mandate: The IPO is responsible for intellectual property rights including patents, designs, trade marks, and copyright. It is responsible for intellectual property policy, educating businesses and consumers about rights and responsibilities, supporting enforcement and granting patents, trade marks, and design rights. As technological developments have an impact on the intellectual property framework[§], including intellectual property enforcement, the IPO launched the Futures Group, a body that engages with stakeholders and experts in a range of emerging technologies. The work of the Futures Group is intended to map out long-term intellectual property operational and policy effects, which serves as a basis for future strategies. In 2020, the IPO launched a Call for Views to help understand the questions that must be addressed to ensure the intellectual property framework incentivises the development and adoption of artificial intelligence technologies. The government response to this Call for Views was published in March 2021, setting out 11 actions to provide an intellectual property system better equipped to meet the government's ambitions on artificial intelligence.

Major Reports, Inquiries, and Related Initiatives:

- IP Counter-infringement Strategy 2022 to 2027 (2022): [Report][54]
- Artificial intelligence and intellectual property: call for views (2021): [Call for Views and Responses][55]
- Social media influencers and counterfeit goods (2021): [Report][56]
- Music creators' earnings in the digital era (2021): [Report][57]
- Artificial intelligence: a worldwide overview of AI patents (2019): [Report][58]

§ For example, IP criminals have been able to use the Internet to reach consumers using legitimate platforms to advertise illicit counterfeit goods.

*National Data Guardian (NDG)

Institutional Form: Independent statutory authority

Responsible Minister: The Department of Health and Social Care

Principal Instrument(s): *Health and Social Care (National Data Guardian) Act (2018), Data Protection Act (2018), UK GDPR (2016)*

Mandate: The NDG is an independent champion for patients and the public when it comes to matters of their confidential health and care information. It encourages the building and maintenance of trustworthy systems and practices by providing advice, guidance, and challenge on the use of health and adult social care data, including for the provision of innovative services. Emphasising the importance of keeping people's information safe and confidential, but also of sharing it when appropriate to achieve better outcomes for patients and service users, the NDG advises on matters such as confidentiality, security, effective use of data, communicating with the public and individual choice. The NDG's functions are advisory only. Public bodies such as hospitals, general practices, care homes, planners, commissioners of services, and private organisations delivering services for the National Health Service must take note of the NDG's official guidance that is relevant to them.

Major Reports, Inquiries, and Related Initiatives:

- Putting good into practice: a public dialogue on making public benefit assessments when using health and care data (2021): [Final Report][59]
- Data sharing during this public health emergency (2020): [Authored Article][60]
- NDG report on barriers to information sharing to support direct care (2020): [Final Report][61]
- Caldicott Principles: a consultation about revising, expanding and upholding the principles (2020): [Webpage] [Consultation Outcome][62]
- The Caldicott Principles (2020): [Guidance Webpage][63]
- National Data Guardian for Health and Care: consultation response (2019): [Final Report][64]
- NDG poll findings: public attitudes to organisations innovating with NHS data (2019): [Press Release][65]

** In 2016, the CMA published a report on investigations into competition and innovation in the retail banking industry finding that big banks dominated the market. Consumers and small businesses would benefit from increased competition. To remedy this, the CMA and the government mandated 9 of the largest banks to implement common standards for open banking. This would ensure that there were standard application programming interfaces that allow customers to securely share their financial data or safely initiate transactions. Trusted companies could use these APIs to offer new innovative services to customers and SMEs increasing competition. In a nutshell, open banking enables Account Servicing Payment Service Providers (ASPSPs), including banks and building societies, to allow their personal and small business customers to share their account data securely with Third Party Providers (TTPs). This enables those third parties to provide customers with services related to account information such as product comparison or payment initiation or confirmation of funds.

Office of Communications (Ofcom)

Institutional Form: Independent statutory authority

Responsible Minister: The Secretary of State for the Department of Culture, Media and Sport (DCMS)

Principal Instrument(s): *Digital Economy Act (2017), Communications Act (2003)*

Mandate: The Ofcom is the regulator and competition authority for communications industries in the United Kingdom. It regulates the television and radio sectors, fixed-line telecoms, mobiles, postal services, plus the airwaves over which wireless devices operate. It has a statutory duty to represent the interests of citizens and consumers by promoting competition and protecting the public from harmful or offensive material. The *Draft Online Safety Bill* was published in May 2021 to protect people from illegal or harmful online content by making digital platform operators (Regulated Providers) responsible for swiftly removing such content. Compliance with the *OSB* will be overseen by the Ofcom, which will classify online companies as Category 1, 2A or 2B services (based on thresholds set by the Secretary of State) to help determine the obligations they are under.

Major Reports, Inquiries, and Related Initiatives:

- The future of media plurality in the UK (ongoing): [Consultation] [Statement Webpage] [Statement][66]
- Net neutrality review (ongoing): [Call for Evidence Webpage] [Call for Evidence][67]
- Promoting competition and investment in fibre networks: Wholesale Fixed Telecoms Market Review 2021–2026 (2021): [Consultation and Statement Webpage] [Final Report][68]
- Guidance for video-sharing platform providers on measures to protect users from harmful material (2021): [Consultation and Statement Webpage] [Guidance][69]
- Call for evidence: Video-sharing platform regulation (2020): [Call for Evidence Webpage] [Call for Evidence][70]

*Open Banking Implementation Entity (OBIE)

Institutional Form: Independent non-statutory authority

Responsible Minister: The Trustee of the OBIE, appointed by the CMA

Principal Instrument(s): *CMA's Retail Banking Investigation Order (2017), Payment Services Regulations (2017) (PSRs), Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication (RTS-SCA), UK regulatory technical standards for strong customer authentication and secure communication (UK-RTS)*

Mandate: The OBIE supervises the implementation efforts of the largest financial institutions that participate in the open banking ecosystem,** shapes and champions the open banking ecosystem, and provides critical services and infrastructure to that ecosystem. The OBIE publishes and maintains the Open Banking Standards, which include Technical API (Application Programming Interface) Specifications (the security and messaging standards necessary for the transfer of sensitive financial data between regulated participants), the Customer Experience Guidelines (the user journey standards that allow customers to provide informed consent in an intuitive manner), and Operational Guidelines (the performance standards required of the technical infrastructure). Also, it provides tangible technical assistance to all ecosystem participants, including financial institutions, prepaid and credit card providers, and third-party service (i.e., FinTech) providers from certification and on-boarding through to business-as-usual support.

Major Reports, Inquiries, and Related Initiatives:

- Enrolling onto the OBIE Directory: How to Guide (2021): [Guide][71]
- Managing your Access to the OBIE Directory: How to Guide (2021): [Guide][72]
- Viewing and Requesting Updates to your Entity: How to Guide (2021): [Guide][73]
- Open Banking Customer Experience Guidelines (2019): [Guidelines][74]

Single Source Regulations Office (SSRO)

Institutional Form: Executive non-departmental public body

Responsible Minister: The Secretary of State for Defence

Principal Instrument(s): *Defence Reform Act (2014), Single Source Contract Regulations (2014)*

Mandate: The SSRO supports the operation of the regulatory framework for single-source defence contracts, which places controls on the prices of qualifying defence contracts. In addition to reviewing the regulatory framework, recommending appropriate changes to it, and receiving statutory reports from defence contractors, the SSRO gives opinions and makes determinations on questions referred by the Ministry of Defence and defence contractors. In doing so, it clarifies how the regime applies to qualifying contracts, including contracts for the provision of IT services and resolves disagreements. In 2021, the SSRO launched a consultation to create a separate activity – IT services – for the purposes of qualifying defence contracts. The government's final response is expected in Spring 2022.

Major Reports, Inquiries, and Related Initiatives:

- Consultation: Developing an information technology services activity group (2021): [Consultation Webpage][75]
- Consultation: Review of the single source regulatory framework 2020 (2020): [Consultation Webpage][76]

Ongoing Parliamentary Committees, Inquiries, or Legislative proposals (not previously referred to):

- Delivering a UK science and technology strategy, House of Lords Science and Technology Committee (ongoing): [Inquiry Webpage] [Call for Evidence][77]
- Online Safety and online harms, House of Commons DCMS Sub-Committee on Online Harms and Disinformation (ongoing): [Inquiry Webpage] [Report][78]
- National Law Enforcement Data Programme, House of Commons Public Accounts Committee (ongoing): [Inquiry Webpage] [Report][79]
- NHS (Prohibition of Data Transfer) Bill, House of Commons Session 2021–2022: [Webpage][80]

Endnotes (United Kingdom)

1. Bank of England 2021, *New forms of digital money*, accessed 31 March 2022, www.bankofengland.co.uk/paper/2021/new-forms-of-digital-money.

2. Eccles, P, Grout, P, Siciliani, P & Zalewska, A 2021, *The impact of machine learning and big data on credit markets*, Bank of England, accessed 31 March 2022, www.bankofengland.co.uk/-/media/boe/files/working-paper/2021/the-impact-of-machine-learning-and-big-data-on-credit-markets.pdf?la=en&hash=E24C0793C1E755C20DAD193C8902485CC13709B7.

3. Bank of England 2020, *Central Bank Digital Currency: Opportunities, challenges and design*, accessed 31 March 2022, www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593.

4. Bank of England 2020, *The impact of Covid on machine learning and data science in UK banking*, *Quarterly* Bulletin 2020 Q4, accessed 31 March 2022, www.bankofengland.co.uk/quarterly-bulletin/2020/2020-q4/the-impact-of-covid-on-machine-learning-and-data-science-in-uk-banking.

5. Bank of England 2020, *Open data for SME finance: What we proposed and what we have learnt*, accessed 31 March 2022, www.bankofengland.co.uk/-/media/boe/files/fintech/open-data-for-sme-finance.pdf?la=en&hash=FD4BC43BBD61EDEC5F8460C6BB7488EFDE647581.

6. Financial Conduct Authority 2019, *Machine learning in UK financial services,* accessed on 31 March 2022, www.bankofengland.co.uk/-/media/boe/files/report/2019/machine-learning-in-uk-financial-services.pdf?la=en&hash=F8CA6EE7A5A9E0CB182F5D568E033F0EB2D21246.

7. Biometrics and Surveillance Camera Commissioner 2022, *Update to Surveillance Camera Code of Practice*, accessed 1 April 2022, www.gov.uk/government/publications/update-to-surveillance-camera-code.

8. Biometrics and Surveillance Camera Commissioner 2021, *Surveillance camera code of practice*, accessed 1 April 2022, www.gov.uk/government/consultations/surveillance-camera-code-of-practice.

9. Biometrics and Surveillance Camera Commissioner 2022, *Secure by default: self-certification of video surveillance systems*, accessed 1 April 2022, www.gov.uk/government/publications/secure-by-default-self-certification-of-video-surveillance-systems.

10. Biometrics and Surveillance Camera Commissioner 2022, *Surveillance camera code of practice: third party certification scheme*, accessed 1 April 2022, www.gov.uk/government/publications/surveillance-camera-code-of-practice-third-party-certification-scheme.

11. Biometrics and Surveillance Camera Commissioner 2020, *National surveillance camera strategy for England and Wales*, accessed 1 April 2022, www.gov.uk/government/publications/national-surveillance-camera-strategy-for-england-and-wales.

12. Competition and Markets Authority 2021, *Mobile ecosystems: Market study interim report*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1048746/MobileEcosystems_InterimReport.pdf.

13. Competition and Markets Authority 2021, *Algorithms: How they can reduce competition and harm consumers*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/954331/Algorithms_++.pdf.

14. Competition and Markets Authority 2020, *Online platforms and digital advertising*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

15. Competition and Markets Authority 2020*, A new pro-competition regime for digital markets: Advice of the Digital Markets Taskforce*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital_Taskforce_-_Advice.pdf.

16. Data Standards Authority 2022, *Data Standards*, accessed 1 April 2022, https://alphagov.github.io/data-standards-authority/standards/.

17. Data Standards Authority n.d., *DRAFT Access and record address data using the UPRN standard and AddressBase DRAFT*, accessed 1 April 2022, https://alphagov.github.io/data-standards-authority/guidance/addressbase/.

18. Data Standards Authority n.d., *DRAFT - API Standards*, accessed 1 April 2022, https://alphagov.github.io/data-standards-authority/guidance/apistandardsv3/.

19. Data Standards Authority 2022, *DRAFT - Using GraphQL for your API*, accessed 1 April 2022, https://alphagov.github.io/data-standards-authority/guidance/graphql/.

20. Central Digital and Data Office 2021, *Publish reference data for use across government*, accessed 1 April 2022, www.gov.uk/guidance/publish-reference-data-for-use-across-government.

21. Central Digital and Data Office 2021, *Develop your data and APIs using a reference architecture*, accessed 1 April 2022, www.gov.uk/guidance/develop-your-data-and-apis-using-a-reference-architecture.

22. Data Standards Authority 2021, *Make better use of data*, accessed 1 April 2022, https://alphagov.github.io/data-standards-authority/guidance/tcop10/.

23. Central Digital and Data Office 2021, *Data Standards Authority Strategy 2020 to 2023*,accessed 1 April 2022, www.gov.uk/guidance/data-standards-authority-strategy-2020-to-2023.

24. Department for Business, Energy and Industrial Strategy 2022, *National Security and Investment Act: guidance on notifiable acquisitions*, accessed 1 April 2022, www.gov.uk/government/publications/national-security-and-investment-act-guidance-on-notifiable-acquisitions.

25. Department of Business, Energy and Industrial Strategy 2022, *The National Security and Investment Act alongside regulatory requirements*, GOV.UK, accessed 1 April 2022, www.gov.uk/government/publications/the-national-security-and-investment-act-alongside-regulatory-requirements.

26. Department of Business, Energy and Industrial Strategy 2022, *How the National Security and Investment Act could affect people or acquisitions outside the UK*, accessed 1 April 2022, www.gov.uk/government/publications/check-if-an-acquisition-outside-the-uk-will-be-in-scope-of-the-national-security-and-investment-act.

27. *National Security and Investment Act 2021*, accessed 1 April 2022, www.legislation.gov.uk/ukpga/2021/25/contents/enacted.

28. Export Control Joint Unit and Department for International Trade 2022, *Strategic export controls: licensing data*, accessed 1 April 2022, www.gov.uk/guidance/strategic-export-controls-licensing-data.

29. Export Control Joint Unit and Department for International Trade 2021, *Open general export licences for overseas access to software and technology for military goods (individual use only)*, accessed 1 April 2022, www.gov.uk/government/publications/open-general-export-licence-access-overseas-to-software-and-technology-for-military-goods-individual-use-only.

30. Export Control Joint Unit and Department for International Trade 2021, *Using SPIRE to get an export licence*, accessed 1 April 2022, www.gov.uk/government/publications/spire-online-export-licensing-guidance/using-spire-to-get-an-export-licence.

31. Marketing Means 2021, *Open Banking - TPP Customer Survey 2021: Report on survey results collected by post, telephone and online*, accessed 1 April 2022, www.openbanking.org.uk/wp-content/uploads/Open-Banking-third-party-provider-customer-survey-Nov-2021-Marketing-Means-v1.pdf.

32. Export Control Joint Unit and Department for International Trade 2021, *Export controls: military goods, software and technology*, accessed 1 April 2022, www.gov.uk/guidance/export-controls-military-goods-software-and-technology.

33. GOV.UK n.d., *Digital Economy Council*, accessed 1 April 2022, https://www.gov.uk/government/groups/digital-economy-council.

34. Competition and Markets Authority 2021, *Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022*, accessed 1 April 2022, www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022.

35. Digital Regulation Cooperation Forum 2021, *Digital Regulation Cooperation Forum: Embedding coherence and cooperation in the fabric of digital regulators*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/982898/DRCF_response_to_DCMS__PDF.pdf.

36. Competition and Markets Authority 2021, *Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022*, accessed 1 April 2022, www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022.

37. Digital Regulation Cooperation Forum 2021, *Joining up on future technologies*, accessed 1 April 2022, www.gov.uk/government/publications/joining-up-on-future-technologies-digital-regulation-cooperation-forum-technology-horizon-scanning-programme/joining-up-on-future-technologies.

38. Digital Regulation Cooperation Forum 2020, *Digital Regulation Cooperation Forum*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896827/Digital_Regulation_Cooperation_Forum.pdf.

39. See in particular: Equality and Human Rights Commission 2020, 'Chapter 10 on the Rights to privacy and freedom of expression', *Civil and political rights in Great Britain*, accessed 1 April 2022, www.equalityhumanrights.com/sites/default/files/civil_and_political_rights_in_great_britain_2020.pdf.

40. Financial Conduct Authority 2021, *Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money – Our Approach' and the Perimeter Guidance Manual*, accessed 1 April 2022, www.fca.org.uk/publication/consultation/cp21-3.pdf.

41. Financial Conduct Authority 2020, *Occasional Paper No. 51: Using online experiments for behaviourally informed consumer policy*, accessed 1 April 2022, www.fca.org.uk/publications/occasional-papers/occasional-paper-no-51-using-online-experiments-behaviourally-informed-consumer-policy.

42. Financial Conduct Authority 2020, *Occasional Paper No. 51: Using online experiments for behaviourally informed consumer policy*, accessed 1 April 2022, www.fca.org.uk/publication/occasional-papers/occasional-paper-51.pdf.

43. Financial Conduct Authority 2020, *Fostering innovation through collaboration: The evolution of the FCA TechSprint Approach*, accessed 1 April 2022, www.fca.org.uk/publication/research/fostering-innovation-through-collaboration-evolution-techsprint-approach.pdf.

44. Financial Conduct Authority 2020, *Research Note: Cryptoasset consumer research 2020*, accessed 1 April 2022, www.fca.org.uk/publication/research/research-note-cryptoasset-consumer-research-2020.pdf.

45. Financial Conduct Authority 2020, *Occasional Paper No. 58: Understanding consumer financial wellbeing through banking data*, accessed 1 April 2022, www.fca.org.uk/publication/occasional-papers/occasional-paper-58.pdf.

46. Financial Conduct Authority 2019, *The Impact and Effectiveness of Innovate*, accessed 1 April 2022, www.fca.org.uk/publication/research/the-impact-and-effectiveness-of-innovate.pdf.

47. Financial Conduct Authority 2019, *Machine learning in UK financial services*, accessed 1 April 2022, www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf.

48. Financial Conduct Authority 2019, *Cyber security - industry insights*, accessed 1 April 2022, www.gov.uk/government/publications/joining-up-on-future-technologies-digital-regulation-co-operation-forum-technology-horizon-scanning-programme/joining-up-on-future-technologies.

49. Information Commissioner's Office 2020, *Investigation into data protection compliance in the direct marketing data broking sector*, accessed 1 April 2022, https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf.

50. Information Commissioner's Office 2021, *COVID-19 and information rights: reflections and lessons learnt from the Information Commissioner*, accessed 1 April 2022, https://ico.org.uk/media/about-the-ico/documents/4019157/covid-19-report.pdf.

51. Global Privacy Enforcement Network 2021, *GPEN Report 'Resetting privacy'*, Information Commissioner's Office, accessed 1 April 2022, https://ico.org.uk/media/about-the-ico/documents/2620173/gpen-resetting-privacy-20210617.pdf.

52. Innovation Commissioner's Office 2020, *ICO Innovation Hub Project Report*, accessed 1 April 2022, https://ico.org.uk/media/about-the-ico/documents/2618205/ih-report-20200828-grayscale.pdf.

53. Information Commissioner's Office 2019, *Update report into adtech and real time bidding*, accessed 1 April 2022, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

54. Intellectual Property Office 2022, *Intellectual Property Counter-Infringement Strategy 2022 to 2027*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1051908/IP-Counter-Infringement-Strategy-2022-2027.pdf.

55. Intellectual Property Office 2021, *Artificial intelligence and intellectual property: call for views*, accessed 1 April 2022, www.gov.uk/government/consultations/artificial-intelligence-and-intellectual-property-call-for-views.

56. Intellectual Property Office 2021, *Influencer Report: The impact of complicit social media influences on the consumption of counterfeit goods in the UK*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1035304/Social-media-Influencer.pdf.

57. Hesmondhalgh, D, Osborne, R, Sun, H & Barr, K 2021, *Music Creators' Earnings in the Digital Era*, Intellectual Property Office, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020133/music-creators-earnings-report.pdf.

58. Intellectual Property Office 2019, *Artificial Intelligence: A worldwide overview of AI patents*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817610/Artificial_Intelligence_-_A_worldwide_overview_of_AI_patents.pdf.

59. National Data Guardian 2021, Hopkins Van Mil 2021, *Putting Good into Practice: A public dialogue on making public benefit assessments when using health and care data*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/977737/PGiP_Report_FINAL_1304.pdf.

60. National Data Guardian and Caldicott, Dame F 2020, *Data sharing during this public health emergency*, GOV.UK, accessed 1 April 2022, www.gov.uk/government/speeches/data-sharing-during-this-public-health-emergency.

61. National Data Guardian 2020, *Survey report: Information sharing to support direct care*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906788/NDG_survey_report_v1.4.pdf.

62. National Data Guardian 2020, *Caldicott Principles: a consultation about revising, expanding, and upholding the principles*, accessed 11 April 2022, www.gov.uk/government/consultations/caldicott-principles-a-consultation-about-revising-expanding-and-upholding-the-principles. See also: National Data Guardian 2020, *The National Data Guardian's response to the consultation on the Caldicott Principles and Caldicott Guidelines*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/941865/NDG_CP_and_CG_consultation_response_FINAL_08.12.20.pdf.

63. National Data Guardian 2020, *The Caldicott Principles*, accessed 1 April 2022, www.gov.uk/government/publications/the-caldicott-principles.

64. National Data Guardian 2019, *National Data Guardian for Health and Care: consultation response*, accessed 1 April 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/815950/1037_-_NDG_consultation_response_10.07.19_FINAL_TO_PUBLISH.pdf.

65. National Data Guardian 2019, *NDG poll findings: public attitudes to organisations innovating with NHS data*, accessed 1 April 2022, www.gov.uk/government/news/ndg-poll-findings-public-attitudes-to-organisations-innovating-with-nhs-data.

66. Office of Communications 2022, *The Future of Media Plurality in the UK: Including Ofcom's consultation on the Media Ownership Rules Review*, accessed 1 April 2022, www.ofcom.org.uk/__data/assets/pdf_file/0012/220710/media-plurality-in-the-uk-condoc.pdf. See also: Office of Communications 2021, *Statement: the future of media plurality in the UK*, accessed 1 April 2022, www.ofcom.org.uk/consultations-and-statements/category-2/future-media-plurality-uk.

67. Office of Communications 2021, *Call for evidence: Net neutrality review*, accessed 1 April 2022, www.ofcom.org.uk/consultations-and-statements/category-2/call-for-evidence-net-neutrality-review. See also: Office of Communications 2021, *Call for evidence: Net neutrality review*, accessed 1 April 2022, www.ofcom.org.uk/__data/assets/pdf_file/0015/224142/call-for-evidence-net-neutrality-review.pdf.

68. Office of Communications 2021, *Statement: Promoting investment and competition in fibre networks –Wholesale Fixed Telecoms Market Review 2021-26*, accessed 1 April 2022, www.ofcom.org.uk/consultations-and-statements/category-1/2021-26-wholesale-fixed-telecoms-market-review. See also: Office of Communications 2021, *Promoting competition and investment in fibre networks: Wholesale Fixed Telecoms Market Review 2021-26*, accessed 1 April 2022, www.ofcom.org.uk/__data/assets/pdf_file/0022/216085/wftmr-statement-volume-1-overview.pdf.

69. Office of Communications 2021, *Video-sharing platform guidance: Guidance for providers on measures to protect users from harmful material*, accessed 1 April 2022, www.ofcom.org.uk/consultations-and-statements/category-1/guidance-vsp-harmful-material-measures. See also: Office of Communications 2021, *Guidance for providers on measures to protect users from harmful material*, accessed 1 April 2022, www.ofcom.org.uk/__data/assets/pdf_file/0015/226302/vsp-harms-guidance.pdf.

70. Office of Communications 2020, *Call for evidence: Video-sharing platform regulation*, accessed 1 April 2022, www.ofcom.org.uk/consultations-and-statements/category-1/video-sharing-platform-regulation. See also: Office of Communications 2020, *Call for evidence: Video-sharing platform regulation*, accessed 1 April 2022, www.ofcom.org.uk/__data/assets/pdf_file/0030/198327/call-for-evidence-vsp-regulation.pdf.

71. Open Banking 2021, *Enrolling onto the OBIE Directory: How to Guide*, accessed 1 April 2022, www.openbanking.org.uk/wp-content/uploads/Enrolling-Onto-Open-Banking-Guide.pdf.

72. Open Banking 2021, *Managing your Access to the OBIE Directory: How to Guide*, accessed 1 April 2022, www.openbanking.org.uk/wp-content/uploads/Managing-Your-Access-To-The-Open-Banking-Directory.pdf.

73. Open Banking 2021, *Viewing and Requesting Updates to your Entity: How to Guide*, accessed 1 April 2022, www.openbanking.org.uk/wp-content/uploads/Viewing-And-Requesting-Updates-To-Your-Enrolled-Entity-Guide.pdf.

74. Open Banking 2019, *Open Banking Customer Experience Guidelines*, accessed 1 April 2022, www.openbanking.org.uk/wp-content/uploads/2021/04/Customer-Experience-Guidelines-V3.1.3-web.pdf.

75. Single Source Regulations Office 2021, *Developing an information technology services activity group*, accessed 1 April 2022, www.gov.uk/government/consultations/developing-an-information-technology-services-activity-group.

76. Single Source Regulations Office 2020, *Review of the single source regulatory framework 2020: Consultation*, www.openbanking.org.uk/wp-content/uploads/2021/04/Customer-Experience-Guidelines-V3.1.3-web.pdf.

77. UK Parliament 2022, *Delivering a UK science and technology strategy*, accessed 1 April 2022, https://committees.parliament.uk/work/6522/delivering-a-uk-science-and-technology-strategy/. See also: UK Parliament, *Call for Evidence*, accessed 1 April 2022, https://committees.parliament.uk/call-for-evidence/722/.

78. UK Parliament 2021, *Online safety and online harms*, accessed 1 April 2022, https://committees.parliament.uk/work/1432/online-safety-and-online-harms/. See also: House of Commons 2022, *The Draft Online Safety Bill and the legal but harmful debate*, accessed 1 April, https://committees.parliament.uk/publications/8608/documents/86960/default/.

79. UK Parliament 2021, *National Law Enforcement Data Programme*, accessed 1 April 2022, https://committees.parliament.uk/work/1460/national-law-enforcement-data-programme/. See also: UK Parliament 2021, *The National Law Enforcement Data Programme*, accessed 1 April 2022, https://committees.parliament.uk/publications/8125/documents/83326/default/.

80. *NHS (Prohibition of Data Transfer) Bill*, accessed 1 April 2022, https://bills.parliament.uk/bills/2983.

United States of America (California)

Dr Diana Bowman, Nicholas Davis and Walter G. Johnson, Arizona State University

California Department of Consumer Affairs (DCA)

Institutional Form: Executive agency

Responsible Minister: Secretary of the Business, Consumer Services and Housing Agency

Principal Instrument(s): *California Business and Professions Code*

Mandate: The DCA is a consumer protection agency that primarily licenses professionals and enforces professional standards (through 38 boards, bureaus, and programs) across a wide range of services including in accounting, construction, medicine, and health care. The DCA oversees professionals who may use various technologies in their practices. For example, health care professionals prescribing medical products or providing services over telemedicine.

Major Reports, Inquiries, and Related Initiatives:

- Order Waiving Restrictions on Telemedicine and Extending Time to Refill Prescriptions (2020): [Order][1]

California Department of Tax and Fee Administration (CDTFA)

Institutional Form: Executive agency

Responsible Minister: Secretary of the Government Operations Agency

Principal Instrument(s): *California Revenue and Taxation Code*

Mandate: The CDTFA administers California's sales and use of fuel, tobacco, alcohol, and cannabis taxes, as well as a variety of other taxes and fees that fund specific state programs. California does not recognise 'virtual currencies' as legal tender but considers the sale and use of virtual currencies as the equivalent of bartering or exchanging foreign currencies for tax purposes.[2]

Major Reports, Inquiries, and Related Initiatives:

- Discussion Paper on proposed amended Regulation 1684.5. Marketplace Sales (2022): [Discussion Paper][3]
- Crypto Sale and Use Tax by State (2021): [News Media][4]

California Privacy Protection Agency (CPPA)

Institutional Form: Independent statutory authority

Responsible Minister: CPPA Board (x5 Members, 1 as Chair)

Principal Instrument(s): *California Privacy Rights Act (2020), California Consumer Privacy Act (2018)*

Mandate: The CPPA is a recently created agency that enforces two main data privacy and security statutes in California, which create consumer rights for California residents and impose obligations on businesses that collect or sell data of those consumers. These instruments focus on notice and disclosure to consumers, and create consumer rights including to request collected data be deleted or corrected, opt-out of the sale or automated processing of data, and limit the use of sensitive data. The CPPA inherited a rulemaking authority and an initial set of rules implementing the *California Consumer Privacy Act* from the Office of the Attorney-General and the Agency and Office of the Attorney-General must coordinate their enforcement activities under the *California Privacy Rights Act*. While the *California Consumer Privacy Act* went into effect in 2020, many provisions will not go into effect until 2023.

Major Reports, Inquiries, and Related Initiatives:

- Invitation for Preliminary Comments on Proposed Rulemaking Under the California Privacy Rights Act of 2020 (Proceeding No. 01–21) (2021): [Invitation for Comment][5]
- California Consumer Privacy Act Regulations (2021): [Codified Regulations][6]

California Public Utilities Commission (CPUC)

Institutional Form: Independent statutory agency

Responsible Minister: CPUC Commissioners (x5 Commissioners, 1 as President)

Principal Instrument(s): *California Public Utilities Code*

Mandate: The CPUC regulates public utilities (owned by private entities) and the public services they provide to protect consumers, ranging from water and energy to telecommunications and common carriers. The CPUC's broad mandate empowers it to license or oversee public utilities' use of technology in these sectors including renewable energy technologies, 5G infrastructure and ridesharing services, including Transportation Network Companies (TNC) such as Uber and Lyft. The CPUC coordinates with other agencies to manage some of these technologies, including its work with the California Division of Motor Vehicles on licensing autonomous vehicle testing.

Major Reports, Inquiries, and Related Initiatives:

- Renewables Portfolio Standard (RPS) Program (ongoing): [Initiative Webpage][7]
- Transportation Network Company Permits Issued (ongoing): [Database Webpage][8]
- California Solar Consumer Protection Guide (2022): [Report][9]
- In the Matter of the Joint Application of Sprint and T-Mobile (2021): [Ruling][10]
- Basic Information for Transportation Network Companies and Applicants (2019): [Guidance][11]
- CPUC Authorizes Passenger Carriers to Provide Free Test Rides in Autonomous Vehicles with Valid CPUC and DMV Permits (2018): [Press Release] [Decision][12]

*California Department of Fair Employment and Housing (DFEH)

Institutional Form: Executive agency

Responsible Minister: Secretary of the Business, Consumer Services and Housing Agency

Principal Instrument(s): *California Family Rights Act (1993), California Fair Employment and Housing Act (1959)*

Mandate: The DFEH is California's primary civil rights regulator that focuses on anti-discrimination in housing and workplace settings. The DFEH has recently held hearings on employment discrimination by artificial intelligence technologies and continues to enforce civil rights law on technology companies.

Major Reports, Inquiries, and Related Initiatives:

- Tesla Says California Plans to Sue Over Alleged Discrimination, Harassment (2022): [Media Coverage][13]
- Civil Rights Hearing on Algorithms and Bias (2021): [Hearing Summary][14]

California Department of Financial Protection and Innovation (DFPI), Office of Financial Technology Innovation (OFTI)

Institutional Form: Office within executive agency

Responsible Minister: Secretary of the Business, Consumer Services and Housing Agency

Principal Instrument(s): *California Financial Code; California Consumer Financial Protection Law (CCFPL), Cal. Fin. Code Sec. 90006(d)(1) (Mandating the creation of OFTI)*

Mandate: The DFPI provides consumer protection services to businesses engaged in financial transactions and oversees state-licensed financial businesses and institutions, including but not limited to banks, credit unions, premium finance companies, and securities brokers and dealers. In 2020, the California legislature mandated DFPI to create the Office of Financial Technology Innovation (OFTI) (officially established in 2021) to monitor and engage with fintech and cryptocurrency/asset businesses. OFTI is expected to play a critical role in helping DFPI develop new rules for FinTech and cryptocurrencies/assets. In 2021, DFPI issued an alert warning for consumers to 'exercise extreme caution before engaging with any solicitation offering investment or financial services related to crypto-currency.' [15]

Major Reports, Inquiries, and Related Initiatives:

- Official OFTI Webpage (ongoing): [Webpage][16]
- Cryptocurrency and Digital Assets (ongoing): [Webpage][17]
- What You Should Know About Virtual Currencies (2019)*: [Consumer Advisory][18]

* The Department of Business Oversight was the previous name of the DFPI prior to September 2020.

*California Department of Insurance (CDI)

Institutional Form: Independent statutory authority

Responsible Minister: California Insurance Commissioner

Principal Instrument(s): *California Insurance Code*

Mandate: The CDI is a consumer protection agency that oversees insurance products and licenses actors in the insurance industry across various classes of insurance. It also investigates and enforces insurance fraud crimes. The CDI oversees insurance products and actors that use or are affected by new technologies and the Rate Specialist Bureau indicates it tracks developments in new technologies, such as InsurTech. Since 2021, the CDI has begun approving insurance products that use artificial intelligence.

Major Reports, Inquiries, and Related Initiatives:

- Commissioner Jones Approves First Insurtech Title Insurer (2018): [Press Release][19]
- Public Hearing on Autonomous Vehicle Insurance Issues Background Paper (2014): [Working Paper][20]

*California Department of Motor Vehicles (CA DMV)

Institutional Form: Executive agency

Responsible Minister: Secretary of the State Transportation Agency

Principal Instrument(s): *California Vehicle Code (CVC), CVC Section 38750 (requiring the DMV to adopt regulations governing the testing and public use of AVs in CA), Title 13, Division 1, Chapter 1, Article 3.7 (Testing of Autonomous Vehicles)*

Mandate: The CA DMV registers motor vehicles, trailers, and vessels within California, along with issuing driver licenses and identification cards. The CA DMV also has regulatory oversight of commercial vehicles used for interstate and intrastate commerce, private driving, traffic schools and new car dealers. The CA DMV oversees California's Autonomous Vehicle (AV) Testing Program that includes permitting manufacturers to deploy autonomous vehicles onto public roads within the state. The current program includes permits for testing with a driver, and driverless testing and deployment. The CA DMV sits within the California State Transportation Agency.

Major Reports, Inquiries, and Related Initiatives:

- Autonomous Vehicles Program (ongoing): [Initiative Webpage][21]
- 2021 Disengagement Reports for the Autonomous Vehicle Program (2021): [Reports] [22]
- Automated Vehicle Principles for Healthy and Sustainable Communities (created by the California Multi-agency Workgroup on AVs (automated vehicles), comprised of staff representatives from CalEPA, CalSTA, Caltrans, CARB, CDPH, CEC, DGS, DMV, Go-Biz, OPR, and SGC): [Report][23]

*California Department of Transportation (Caltrans)

Institutional Form: Executive agency

Responsible Minister: Secretary of the State Transportation Agency

Principal Instrument(s): *California Streets and Highways Code; California Vehicle Code*

Mandate: Caltrans manages California's highway system, supports its public transportation systems, and permits public-use airports and special-use hospital heliports. The agency identified managing the adoption of connected and autonomous vehicles as a top priority in its California Transportation Plan for 2050 (2021). To date, Caltrans has completed multiple autonomous vehicle safety and traffic impact assessments to plan for future regulations and is one of several agencies that partnered with the California Office of Planning and Research to develop the Automated Vehicle Principles for Healthy and Sustainable Communities. The Caltrans Division of Aeronautics also has some regulatory jurisdiction over unmanned aircraft systems (drones), namely the oversight of permits for operating unmanned aircraft systems over state highways.

Major Reports, Inquiries, and Related Initiatives:

- Unmanned Aircraft Systems (ongoing): [Initiative Webpage][24]
- California Transportation Plan 2050, "Manage the Adoption of Connected and Autonomous Vehicles" at pg. 120. (2021): [Report][25]
- Connected Autonomous Vehicles: Safety During Merging and Lane Change and Impact on Traffic Flow (2020): [Report][26]
- Evaluation of Autonomous Vehicles and Smart Technologies for Their Impact on Traffic Safety and Traffic Congestion (2020): [Report][27]
- Automated Vehicle Principles for Healthy and Sustainable Communities (created by the California Multi-agency Workgroup on AVs (automated vehicles), comprised of staff representatives from CalEPA, CalSTA, Caltrans, CARB, CDPH, CEC, DGS, DMV, Go-Biz, OPR, and SGC) (2018): [Report][28]

Office of the Attorney-General (OAG), California Department of Justice (CA DOJ)

Institutional Form: Independent department

Responsible Minister: Attorney-General of California

Principal Instrument(s): *California Privacy Rights Act (2020), California Consumer Privacy Act (2018), California Civil Code; California Penal Code*

Mandate: The OAG brings civil suits and criminal prosecutions to enforce Californian law as well as providing technical and legal assistance to public officials. The OAG enforces a range of internet-related and intellectual-property-related civil and criminal law. This includes hacking, identity theft, trade secret theft and data-security breach reporting. While the Attorney-General retains enforcement authority for California privacy legislation, the OAG must coordinate enforcement activities with the California Privacy Protection Agency. The OAG also functions as a competition regulator, enforcing state antitrust civil and criminal law.

Major Reports, Inquiries, and Related Initiatives:

- Privacy and Data Security (ongoing): [Initiative Webpage][29]
- Data Security Breaches List (ongoing): [Database Webpage][30]
- eCrime Investigations & Prosecutions Guidelines (ongoing): [Guidance Webpage][31]

Endnotes (United States of America (California))

1. Department of Consumer Affairs 2020, *Order Waiving Restrictions on Telemedicine and Extending Time to Refill Prescriptions,* State of California, accessed 29 March 2022, www.dca.ca.gov/licensees/dca_20_21.pdf.

2. *Regulation 1684.5. Marketplace Sales*, State of California, accessed 29 March 2022, https://www.cdtfa.ca.gov/lawguides/vol1/sutr/sales-and-use-tax-regulations-art17-all.html.

3. *Certification of Emergency Regulation 1684.5, Marketplace Sales,* State of California, accessed 29 March 2022, www.cdtfa.ca.gov/taxes-and-fees/Combined1684-5.pdf.

4. Bloomberg Tax 2021, *Cryptocurrency Sales and Use Tax by State*, accessed 29 March 2022, https://pro.bloombergtax.com/brief/cryptocurrency-tax-laws-by-state/.

5. California Privacy Protection Agency 2021, *Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020,* State of California, accessed 29 March 2022, https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf.

6. California Office of Administrative Law 2022, *Chapter 20. California Consumer Privacy Act Regulations,* Thomson Reuters, accessed 29 March 2022, https://govt.westlaw.com/calregs/Browse/Home/California/CaliforniaCodeofRegulations?guid=I3B774FCEACB54B9E98ED95E1ECAEB407&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default).

7. California Public Utilities Commission 2021, *Renewables Portfolio Standard (RPS) Program*, accessed 29 March 2022, www.cpuc.ca.gov/industries-and-topics/electrical-energy/electric-power-procurement/rps.

8. California Public Utilities Commission 2021, *Transportation Network Company Permits Issued*, accessed 29 March 2022, www.cpuc.ca.gov/regulatory-services/licensing/transportation-licensing-and-analysis-branch/transportation-network-companies/tnc-permits-issued.

9. California Public Utilities Commission 2022, *California Solar Consumer Protection Guide,* www.cpuc.ca.gov/-/media/cpuc-website/divisions/energy-division/documents/solar-guide/solar-guide22_011922.pdf.

10. California Public Utilities Commission 2021, *Assigned commissioner and assigned administrative law judge's ruling directing T-Mobile USA, INC. To show cause why it should not be sanctioned by the commission for violation of rule 1.1 of the commission's rules of practice and procedure,* State of California, accessed 29 March 2022, https://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M398/K955/398955746.PDF.

11. Transportation License Section 2019, *Basic Information for Transportation Network Companies and Applicants*, California Public Utilities Commission, accessed 29 March 2022, www.cpuc.ca.gov/-/media/cpuc-website/files/uploadedfiles/cpuc_public_website/content/licensing/transportation_network_companies/basicinformation-fortncs.pdf.

12. California Public Utilities Commission 2018, *CPUC Authorizes Passenger Carriers to Provide Free Test Rides in Autonomous Vehicles with Valid CPUC and DMV Permits,* media release, https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M215/K467/215467801.PDF. See also: California Public Utilities Commission 2018, *Decision authorizing a pilot test program for autonomous vehicle passenger service with drivers and addressing in part issues raised in the petitions for modification of general motors, LLC/UATC, LLC for purposes of a pilot test program for driverless autonomous vehicle passenger services,* accessed 29 March 2022, https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M215/K279/215279920.PDF.

13. Reuters 2022, *Tesla says California plans to sue over alleged discrimination harassment*, *Reuters,* 10 February, accessed 29 March 2022, www.reuters.com/business/tesla-says-california-dfeh-sue-company-over-alleged-discrimination-2022-02-09.

14. Department of Fair Employment and Housing 2022, *DFEH Holds Civil Rights Hearing on Algorithms and Bias*, accessed 29 March 2022, www.dfeh.ca.gov/wp-content/uploads/sites/32/2021/05/Algorithms-Hearing-Press-Release.pdf.

15. Department of Financial Protection and Innovation 2022, *Cryptocurrency and Digital Assets*, accessed 29 March 2022, https://dfpi.ca.gov/2021/10/22/cryptocurrency/?#consumeralerts%3E.

16. Department of Financial Protection and Innovation 2021, *Office of Financial Technology Innovation*, accessed 29 March 2022, https://dfpi.ca.gov/office-of-financial-technology-innovation/.

17. Department of Financial Protection and Innovation 2022, *Cryptocurrency and Digital Assets*, accessed 29 March 2022, https://dfpi.ca.gov/2021/10/22/cryptocurrency/?#consumeralerts%3E.

18. Department of Business Oversight 2014, *What You Should Know about Virtual Currencies,* accessed 29 March 2022, https://dfpi.ca.gov/wp-content/uploads/sites/337/2019/02/Virtual_Currencies_0414.pdf.

19. California Department of Insurance 2018, *Commissioner Jones approves first insuretech title insurer*, accessed 29 March 2022, www.insurance.ca.gov/0400-news/0100-press-releases/2018/release094-18.cfm.

20. California Department of Insurance 2014, *Public hearing on Autonomous Vehicle Insurance Issues,* accessed 29 March 2022, www.insurance.ca.gov/0400-news/multimedia/0030VideoHearings/upload/AVHEARINGBCKGRNDFNL.pdf.

21. Department of Motor Vehicles 2022, *Autonomous Vehicles,* State of California, accessed 29 March 2022, www.dmv.ca.gov/portal/vehicle-industry-services/autonomous-vehicles/.

22. Department of Motor Vehicles 2022, *Disengagement Reports,* State of California, accessed 29 March 2022, www.dmv.ca.gov/portal/vehicle-industry-services/autonomous-vehicles/disengagement-reports/.

23. Governor's Office of Planning and Research 2018, *Automated Vehicle Principles for Healthy and Sustainable Communities*, accessed 29 March 2022, https://opr.ca.gov/docs/20181115-California_Automated_Vehicle_Principles_for_Healthy_and_Sustainable_Communities.pdf.

24. Caltrans 2022, *Unmanned Aircraft Systems (Drones)*, State of California, accessed 29 March 2022, https://dot.ca.gov/programs/aeronautics/unmanned-aircraft-systems.

25. Miles, J, & Strybel, T 2020, *Evaluation of Autonomous Vehicles and Smart Technologies for Their Impact on Traffic Safety and Traffic Congestion,* California state university, accessed 29 March 2022, https://dot.ca.gov/-/media/dot-media/programs/research-innovation-system-information/documents/final-reports/ca20-3406-final-report-a11y.pdf .

26. Ioannow, P, & Monteiro, FV 2020, *Connected Autonomous Vehicles: Safety During Merging and Lane Change and Impact on Traffic Flow*, University of Southern California, accessed 29 March 2022, https://dot.ca.gov/-/media/dot-media/programs/research-innovation-system-information/documents/final-reports/ca20-3405-final-report-a11y.pdf.

27. Miles, J, & Strybel, T 2020, *Evaluation of Autonomous Vehicles and Smart Technologies for Their Impact on Traffic Safety and Traffic Congestion,* California state university, accessed 29 March 2022, https://dot.ca.gov/-/media/dot-media/programs/research-innovation-system-information/documents/final-reports/ca20-3406-final-report-a11y.pdf.

28. Governor's Office of Planning and Research 2018, *Automated Vehicle Principles for Healthy and Sustainable Communities*, accessed 29 March 2022, https://opr.ca.gov/docs/20181115-California_Automated_Vehicle_Principles_for_Healthy_and_Sustainable_Communities.pdf.

29. Office of the Attorney General 2022, *Privacy and Data Security*, California Department of Justice, accessed 29 March 2022, https://oag.ca.gov/privacy.

30. Office of the Attorney General 2022, *Search Data Security Breaches*, State of California Department of Justice, accessed 29 March 2022, https://oag.ca.gov/privacy/databreach/list.

31. Office of the Attorney General 2022, *Investigations & Prosecutions Guidelines*, State of California Department of Justice, accessed 29 March 2022, https://oag.ca.gov/ecrime/guidelines.

United States of America (Federal)

Dr Diana Bowman, Nicholas Davis and Walter G. Johnson, Arizona State University

Bureau of Industry and Security (BIS)

Institutional Form: Executive agency

Responsible Minister: The Secretary of Commerce

Principal Instrument(s): *Export Control Reform Act (2018), Export Administration Act (1979)*

Mandate: The BIS administers export control regulations for non-defense-related items in service of national security, economic and foreign policy objectives. It oversees the Export Administration Regulations and licensing, which place controls on commodities, software and technologies of interest and pays special interest to items with dual-use potential. The State Department administers export control regulations for defense-related items, while the Committee on Foreign Investment in the United States aggregates representatives from multiple departments to regulate foreign investment.

Major Reports, Inquiries, and Related Initiatives:

- Promoting Human Rights and Democracy (ongoing): [Initiative Webpage][1]
- Information Security Controls: Cybersecurity Items (2021): [Interim Final Rule][2]
- Review of Controls for Certain Emerging Technologies (2018): [Proposed Rule][3]

Commodity Futures Trading Commission (CFTC)

Institutional Form: Independent statutory authority

Responsible Minister: CFTC Commissioners (x5 Commissioners, 1 as Chair)

Principal Instrument(s): *Dodd-Frank Wall Street Reform and Consumer Protection Act (2010), Commodity Futures Trading Commission Act (1974), Commodity Exchange Act (1936)*

Mandate: The CFTC is a financial regulator that administers and enforces law on derivatives products to promote derivatives market integrity, including markets that involve FinTech. These most prominently involve digital assets, which include cryptocurrencies. The CFTC works with the Securities Exchange Council and several financial institution regulators to manage financial markets in the United States.

Major Reports, Inquiries, and Related Initiatives:

- Electronic Trading Risk Principles (2021): [Final Rule][4]
- Digital Assets Primer (2020): [Report][5]
- Customer Advisory: Use Caution When Buying Digital Coins or Tokens (2018): [Consumer Advisory][6]
- Memorandum of Understanding Between the U.S. Securities And Exchange Commission and the U.S. Commodity Futures Trading Commission Regarding Coordination in Areas of Common Regulatory Interest and Information Sharing (2018): [Memorandum of Understanding][7]

Consumer Product Safety Commission (CPSC)

Institutional Form: Independent statutory agency

Responsible Minister: CPSC Commissioners (x5 Commissioners, 1 as Chair)

Principal Instrument(s): *Consumer Product Safety Act (1972), Federal Hazardous Substances Act (1960)*

Mandate: The CPSC regulates consumer products (not regulated by another agency) to protect consumers from unreasonable risks of death, injury, or property damage; including setting mandatory standards, investigating harm reports, and recalling products. The CPSC regulates new technologies with potential implications on consumer product safety, including nanomaterials and artificial intelligence, in part by recognising existing voluntary standards from other standard-setting bodies.

Major Reports, Inquiries, and Related Initiatives:

- Artificial Intelligence and Machine Learning In Consumer Products (2021): [Report][8]
- Voluntary Standards Activities Fiscal Year 2021 Annual Report (2021): [Report][9]
- Status Report on the Internet of Things (IoT) and Consumer Product Safety (2019): [Report][10]

Cybersecurity and Infrastructure Security Agency (CISA)

Institutional Form: Executive agency

Responsible Minister: The Secretary of Homeland Security

Principal Instrument(s): *Cybersecurity and Infrastructure Security Agency Act (2018), Protecting and Securing Chemical Facilities from Terrorist Attacks Act (2014), Federal Information Security Modernization Act (2014), Homeland Security Act (2002)*

Mandate: The CISA has multiple policy responsibilities. It monitors security for critical cyber and physical infrastructure, including infrastructure operated by both public and private actors, and builds capacity in infrastructure operators. The CISA also administers and enforces risk-based performance standards for chemical facilities deemed at high-risk from terrorist attack, including holding a standard on cyber security for these facilities. Civilian federal agencies must report security incidents to the CISA, although private actors can voluntarily submit incident reports.

Major Reports, Inquiries, and Related Initiatives:

- Security Guidance for 5G Cloud Infrastructures: Prevent and Detect Lateral Movement (2021): [Guidance][11]
- Cybersecurity Incident & Vulnerability Response Playbooks (2021): [Report][12]
- US-CERT Federal Incident Notification Guidelines (2017): [Guidance][13]
- Chemical Facility Anti-Terrorism Standards: Guidance for the Expedited Approval Program (2015): [Guidance][14]

*Department of Education

Institutional Form: Department

Responsible Minister: The Secretary of Education

Principal instrument(s): *Protection of Pupil Rights Amendment (1978), Family Educational Rights and Privacy Act (FERPA) (1974)*

Mandate: The Department of Education protects the privacy of students regarding educational records and related data. This gives parents of students (and then students once they reach the age of 18) rights to access, request corrections to and consent to disclose education records, as well as to notice and consent before sensitive categories of student data is collected for purposes such as research or marketing.

Major Reports and Inquiries:

- A Parent Guide to the Family Educational Rights and Privacy Act (FERPA) (2021): [Guidance][15]
- Protection of Pupil Rights Amendment (PPRA) General Guidance (2021): [Guidance][16]

Department of Justice (DOJ), Antitrust Division

Institutional Form: Division within department

Responsible Minister: The Attorney-General

Principal Instrument(s): *Economic Espionage Act (1996), Computer Fraud and Abuse Act (1986), Electronic Communications Privacy Act (1986), Trademark Counterfeiting Act (1984), Sherman Act (1890)*

Mandate: The DOJ brings civil suits and criminal prosecutions to enforce United States federal law and provides technical and legal assistance. The DOJ enforces a wide range of intellectual property and internet-related civil and criminal law, which includes behavior such as hacking, harassment, and digital financial crimes. The DOJ Antitrust Division enforces anticompetition law and is currently coordinating with the Federal Trade Commission on antitrust enforcement for big technology companies in the United States. The DOJ is currently investigating Google and Apple, and the Federal Trade Commission is investigating Facebook and Amazon.

Major Reports, Inquiries, and Related Initiatives:

- EU-U.S. Joint Technology Competition Policy Dialogue Inaugural Joint Statement between the European Commission, the United States Department of Justice Antitrust Division and the United States Federal Trade Commission (2021): [Joint Statement][17]
- U.S. and Plaintiff States v. Google LLC (2020, ongoing): [Enforcement Action][18]
- Attorney-General's Cyber-Digital Task Force Cryptocurrency Enforcement Framework (2020): [Report][19]
- Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources (2020): [White Paper][20]

Department of State, Directorate of Defense Trade Controls

Institutional Form: Department

Responsible Minister: The Secretary of State

Principal Instrument(s): *Arms Export Control Act (1976)*

Mandate: The State Department oversees export control regulations for military and defense-related items through the Directorate of Defense Trade Controls within the Department's Bureau of Political-Military Affairs. The International Traffic in Arms Regulations controls and licensing regimes cover 'defense articles' and 'defense services', which involves an array of technologies. The Bureau of Industry and Security administers export control regulations for non-defense-related items, while the Committee on Foreign Investment in the United States brings together representatives from multiple departments to regulate foreign investment.

Major Reports, Inquiries, and Related Initiatives:

- International Traffic in Arms Regulations (ITAR): Continued Temporary Modification of Category XI of the United States Munitions List {regarding 'intelligence-analytics software'} (2021): [Final Rule][21]

Federal Communications Commission (FCC)

Institutional Form: Independent statutory authority

Responsible Minister: FCC Commissioners (x5 Commissioners, 1 as Chair)

Principal Instrument(s): *Telecommunications Act (1996), Communications Act (1934)*

Mandate: The FCC regulates telecommunication and broadband services, facilities and infrastructure involving radio, television, cable, wire, and satellite, to promote equal access, competition, and innovation. The FCC licenses the use of satellites and the electromagnetic spectrum for commercial and non-commercial uses, including 5G-spectrum bands.

Major Reports, Inquiries, and Related Initiatives:

- Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs (2021): [Final Rule][22]
- Potential Impacts on Communications from IPv4 Exhaustion & IPv6 Transition (2021): [Working Paper][23]
- The Digital Divide in U.S. Mobile Technology and Speeds (2020): [Working Paper][24]

Federal Reserve System

Institutional Form: Independent statutory authority

Responsible Minister: Board of Governors of the Federal Reserve System (x7 Governors, 1 as Chair)

Principal Instrument(s): *Dodd-Frank Wall Street Reform and Consumer Protection Act (2010), Depository Institutions Deregulation and Monetary Control Act (1980), Federal Reserve Act (1913)*

Mandate: The Federal Reserve is the central bank of the United States and administers monetary policy, regulates and supervises financial institutions such as banks, and strives to maintain the stability of the financial system and contain systemic financial risk. These mandates place the Federal Reserve in a position to regulate and supervise financial institutions' use of technologies such as artificial intelligence and blockchain, along with several other agencies with similar mandates. These include the Consumer Financial Protection Bureau, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency.

Major Reports, Inquiries, and Related Initiatives:

- Community Bank Access to Innovation through Partnerships (2021): [Report][25]
- Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning (2021): [Request for Information and Comment][26]
- Supporting Responsible Use of AI and Equitable Outcomes in Financial Services (2021): [Public Symposium][27]

Federal Trade Commission (FTC)

Institutional Form: Independent statutory authority

Responsible Minister: FTC Commissioners (x5 Commissioners, 1 as Chair)

Principal Instrument(s): *Federal Trade Commission Act (1914), Clayton Act (1914)*

Mandate: The FTC is a consumer protection and competition regulatory agency responsible for preventing and responding to anti-competitive, unfair, or deceptive business practices across sectors. The FTC has become the United States' de facto data protection regulator through its piecemeal enforcement of instruments including the 'unfair or deceptive acts or practices' standard and the *Children's Online Privacy Protection Act*. The FTC, alongside the DOJ, has been investigating big technology companies in the United States for alleged anti-competitive practices. In 2020 and 2021, the FTC expressed interest in taking steps towards regulating artificial intelligence or algorithmic bias.

Major Reports, Inquiries, and Related Initiatives:

- Past Acquisitions by Large Technology Companies (2020-ongoing): [Inquiry Webpage][28]
- Non-HSR Reported Acquisitions by Select Technology Platforms, 2010–2019: An FTC Study (2021): [Report][29]
- The Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics (2018): [Hearing][30]
- Big Data: A Tool for Inclusion or Exclusion? (2016): [Commission Report][31]

Internal Revenue Service (IRS)

Institutional Form: Executive agency

Responsible Minister: The Secretary of Treasury

Principal Instrument(s): *Internal Revenue Code (26 U.S.C.)*

Mandate: The IRS administers the federal tax program in the United States and enforces tax laws against fraud. Since 2014, the IRS has paid particular attention to cryptocurrencies or virtual currency.

Major Reports, Inquiries, and Related Initiatives:

- IRS has begun sending letters to virtual currency owners advising them to pay back taxes, file amended returns; part of agency's larger efforts (2019): [Press Release][32]
- Notice 2014–21: IRS Virtual Currency Guidance (2014): [Guidance][33]

Nuclear Regulatory Commission (NRC)

Institutional Form: Independent statutory authority

Responsible Minister: NRC Commissioners (x5 Commissioners, 1 as Chair)

Principal Instrument(s): *Energy Reorganization Act (1974), Atomic Energy Act (1954)*

Mandate: The NRC regulates commercial uses of nuclear materials, most prominently involving oversight of nuclear power plants, but also extending to nuclear material use in other sectors such as medicine. The NRC licenses nuclear power facilities and approves their cyber security plans as a component of licensing and oversight, including inspection and enforcement, largely through its Cyber Security Branch.

Major Reports, Inquiries, and Related Initiatives:

- Audit of NRC's Cyber Security Inspections at Nuclear Power Plants OIG-19-A-13 (2019): [Report][34]
- Update to the U.S. Nuclear Regulatory Commission Cyber Security Roadmap (SECY-17-0034) (2017): [Policy Paper][35]
- Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities (2010): [Guidance][36]

Securities and Exchange Commission (SEC)

Institutional Form: Independent statutory authority

Responsible Minister: SEC Commissioners (x5 Commissioners, 1 as Chair)

Principal Instrument(s): *Dodd-Frank Wall Street Reform and Consumer Protection Act (2010), Sarbanes–Oxley Act (2002), Securities Exchange Act (1934), Securities Act (1933),*

Mandate: The SEC oversees securities exchanges, credit rating agencies, and various types of financial market participants to protect investors, maintain financial market integrity, and facilitate capital formation. The SEC's oversight of financial products and markets arises from multiple statutes and grants. It holds authority over technologies used in these settings (FinTech). This includes technologies such as artificial intelligence, automated investment advice, and distributed ledger technology. Established in 2018, the Strategic Hub for Innovation and Financial Technology (FinHub) is the SEC's primary office for fintech regulatory activities. The SEC works with the Commodity Futures Trading Commission and several financial institution regulators in overseeing financial markets in the United States.

Major Reports, Inquiries, and Related Initiatives:

- Strategic Hub for Innovation and Financial Technology (FinHub) (ongoing): [Initiative Webpage][37]
- President's Working Group on Financial Markets: Report on Stablecoins (including the SEC Chair) (2021): [Report][38]
- Memorandum of Understanding Between the U.S. Securities And Exchange Commission and the U.S. Commodity Futures Trading Commission Regarding Coordination in Areas of Common Regulatory Interest and Information Sharing (2018): [Memorandum of Understanding][39]
- Investor Bulletin: Initial Coin Offerings (2017): [Consumer Advisory][40]
- Guidance Update: Robo-Advisors (2017): [Guidance][41]

United States Patent and Trademark Office (USPTO)

Institutional Form: Executive agency

Responsible Minister: The Secretary of Commerce

Principal Instrument(s): *Patent Act (35 U.S.C.), Trademark Act (1946)*

Mandate: The USPTO issues patents and registers trade marks. The USPTO issues patents on various types of technologies and has released several publications on artificial intelligence in the last several years.

Major Reports, Inquiries, and Related Initiatives:

- Identifying Artificial Intelligence (AI) Invention: A Novel AI Patent Dataset (2021): [Working Paper][42]
- Software Piracy and IP Management Practices: Strategic Responses to Product-Market Imitation (2021): [Working Paper][43]
- Inventing AI Tracing the diffusion of artificial intelligence with U.S. patents (2020): [Report][44]
- International Collaboration and Ownership on Patents Issued to Chinese Inventors (2018): [Report][45]

Ongoing Parliamentary Committees, Inquiries, or Legislative Proposals (not previously referred to):

- American Innovation and Choice Online Act: [S.2992] [H.R.3816][46]
- Senate Subcommittee on Privacy, Technology and the Law (ongoing): [Committee Webpage][47]
- House Subcommittee on Communications and Technology (ongoing): [Committee Webpage][48]
- House Subcommittee on Consumer Protection and Commerce (ongoing): [Committee Webpage][49]
- House Subcommittee on Health (ongoing): [Committee Webpage][50]

Endnotes (United States of America (Federal))

1. US Bureau of industry and security 2022, *Promoting human rights and democracy,* U.S. Department of Commerce, accessed 30 March 2022, www.bis.doc.gov/index.php/policy-guidance/promoting-human-rights-and-democracy.

2. National Archives 2021, *Information security controls: Cybersecurity items,* Industry and Security Bureau, accessed 29 March 2022, www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items.

3. National Archives 2022, *Review of controls for certain emerging* technologies, Industry and Security Bureau, accessed 29 March 2022, www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

4. National Archives 2021, *Electronic Trading Risk Principles,* Commodity Futures Trading Commission, accessed 30 March 2022, www.federalregister.gov/documents/2021/01/11/2020-27622/electronic-trading-risk-principles.

5. Commodity Futures Trading Commission 2020, *Digital Assets Primer*, accessed 30 March 2022, www.cftc.gov/media/5476/DigitalAssetsPrimer/download.

6. Commodity Futures Trading Commission 2018, *Customer Advisory: Use Caution When Buying Digital Coins or Tokens,* accessed 30 March 2022, www.cftc.gov/sites/default/files/2018-07/customeradvisory_tokens0718.pdf.

7. Commodity Futures Trading Commission 2018, *Memorandum of understanding between the U.S. Securities and Exchange Commission and the U.S. Commodity Futures trading commission regarding coordination in areas of common regulatory interest and information sharing,* accessed 30 March 2022, www.cftc.gov/sites/default/files/2018-07/CFTC_MOU_InformationSharing062818.pdf.

8. Consumer Product Safety Commission 2021, *Artificial Intelligence and Machine Learning In Consumer Products,* United States federal government, accessed 30 March 2020, www.cpsc.gov/s3fs-public/Artificial-Intelligence-and-Machine-Learning-In-Consumer-Products.pdf.

9. Consumer Product Safety Commission 2021, *Voluntary Standards Tracking Activity Report,* accessed 30 March 2022, www.cpsc.gov/s3fs-public/Voluntary-Standards-Activities-Fiscal-Year-2021-Annual-Report.pdf?VersionId=nbV4e9VCbSXzV8urcG2rGx4me7v72ijq.

10. Consumer Product Safety Commission 2019, *Status Report on the Internet of Things (IoT) and Consumer Product Safety,* accessed 30 March 2022, www.cpsc.gov/s3fs-public/Status-Report-to-the-Commission-on-the-Internet-of-Things-and-Consumer-Product-Safety.pdf.

11. Cybersecurity and Infrastructure Security Agency 2021, *NSA and CISA provide cybersecurity guidance for 5G cloud infrastructures,* accessed 30 March 2022, www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures.

12. Cybersecurity and Infrastructure Security Agency 2021, *Cybersecurity Incident & Vulnerability Response Playbooks,* accessed 30 March 2022, www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

13. Cybersecurity and Infrastructure Security Agency 2017, *US-CERT Federal Incident Notification Guidelines,* accessed 30 March 2022, www.cisa.gov/uscert/incident-notification-guidelines.

14. Cybersecurity and Infrastructure Security Agency 2015, *DHS Guidance for the Expedited Approval Program,* accessed 30 March 2022, www.cisa.gov/sites/default/files/publications/dhs-eap-guidance_508.pdf.

15. *A Parent Guide to the Family Educational Rights and Privacy Act (FERPA)*, accessed 30 March 2022, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/A%20parent%20guide%20to%20ferpa_508.pdf.

16. United States Department of Education Student Privacy Policy Office, *Protection of Pupil Rights Amendment (PPRA),* accessed 30 March 2022, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/20-0379.PPRA_508_0.pdf.

17. EU-U.S. Joint technology competition policy dialogue, *Inaugural joint statement,* accessed 30 March 2022, www.justice.gov/opa/press-release/file/1453916/download.

18. United States Department of Justice 2020, *U.S. and plaintiff states v. Google LLC,* accessed 30 March 2022, www.justice.gov/atr/case/us-and-plaintiff-states-v-google-llc.

19. Attorney General's Cyber-Digital Task Force, *Cryptocurrency enforcement framework,* accessed 30 March 2022, www.justice.gov/archives/ag/page/file/1326061/download.

20. Cybersecurity Unit 2020, *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources,* Computer Crime & Intellectual Property Section Criminal Division, accessed 29 March 2022, www.justice.gov/criminal-ccips/page/file/1252341/download.

21. National Archives, *International traffic in arms regulations (ITAR): continued temporary modification of category XI of the United States munitions list*, State Department, accessed 30 March 2022, www.federalregister.gov/documents/2021/08/27/2021-18544/international-traffic-in-arms-regulations-itar-continued-temporary-modification-of-category-xi-of.

22. National Archives 2021, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* Federal Communications Commission, accessed 30 March 2022, www.federalregister.gov/documents/2021/08/23/2021-17279/protecting-against-national-security-threats-to-the-communications-supply-chain-through-fcc-programs.

23. Cannon, R 2021, *Potential Impacts on Communications from IPv4 Exhaustion & IPv6 Transition,* Federal Communications Commission, accessed 30 March 2022, www.fcc.gov/reports-research/working-papers/potential-impacts-communications-ipv4-exhaustion-ipv6-transition.

24. Dempsey, J & Sun, P 2021, *The Digital Divide in U.S. Mobile Technology and Speeds*, Federal Communications Commission, accessed 30 March 2022, www.fcc.gov/reports-research/working-papers/digital-divide-us-mobile-technology-and-speeds.

25. Board of Governors of the Federal Reserve System 2021, *Community Bank Access to Innovation through Partnerships,* The federal reserve system, accessed 30 March 2022, www.federalreserve.gov/publications/files/community-bank-access-to-innovation-through-partnerships-202109.pdf.

26. National Archives 2021, *Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning*, Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Consumer Financial Protection Bureau, and the National Credit Union Administration, accessed 30 March 2022, www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence.

27. Brainard, L 2021, *Supporting Responsible Use of AI and Equitable Outcomes in Financial Services*, transcript, Board of Governors of the Federal Reserve System, accessed 30 March 2022, www.federalreserve.gov/newsevents/speech/brainard20210112a.htm.

28. Federal Trade Commission 2021, *Non-HSR reported acquisitions by select technology platforms, 2010 2019: an FTC study*, accessed 30 March 2022, www.ftc.gov/system/files/documents/reports/non-hsr-reported-acquisitions-select-technology-platforms-2010-2019-ftc-study/p201201technologyplatformstudy2021.pdf.

29. Federal Trade Commission 2020, *FTC to examine past acquisitions by large technology companies,* accessed 30 March 2022, www.ftc.gov/news-events/news/press-releases/2020/02/ftc-examine-past-acquisitions-large-technology-companies.

30. Federal Trade Commission 2018, *FTC Hearing #7: The Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics,* accessed 30 March 2022, www.ftc.gov/news-events/events/2018/11/ftc-hearing-7-competition-consumer-protection-issues-algorithms-artificial-intelligence-predictive.

31. Federal Trade Commission 2016, *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues,* accessed 30 March 2022, www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

32. Internal Revenue Service 2019, *IRS has begun sending letters to virtual currency owners advising them to pay back taxes, file amended returns; part of agency's larger efforts,* accessed 30 March 2022, www.irs.gov/newsroom/irs-has-begun-sending-letters-to-virtual-currency-owners-advising-them-to-pay-back-taxes-file-amended-returns-part-of-agencys-larger-efforts.

33. *Internal Revenue Service 2014, Internal revenue bulletin: 2014-16*, accessed 30 March 2022, www.irs.gov/irb/2014-16_IRB#NOT-2014-21.

34. Office of the Inspector General 2019, *Audit of NRC's Cyber Security Inspections at Nuclear Power Plants, U.S. Nuclear Regulation Commission Defense Nuclear Facilities Safety Board*, accessed 30 March 2022, www.nrc.gov/docs/ML1915/ML19155A317.pdf.

35. McCree, V 2017, *Update to the U.S. Nuclear Regulatory Commission Cyber Security Roadmap,* Nuclear Regulatory Commission, accessed 30 March 2022, www.nrc.gov/docs/ML1635/ML16354A258.pdf.

36. Office of Nuclear Regulatory Research 2010, *Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities,* accessed 30 March 2022, www.nrc.gov/docs/ML0903/ML090340159.pdf.

37. United States Securities and Exchange Commission 2022, *Strategic Hub for Innovation and Financial Technology (FinHub),* accessed 30 March 2022, www.sec.gov/finhub.

38. President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency 2021, *Report on Stablecoins,* Treasury, accessed 30 March 2022, https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

39. Commodity Futures Trading Commission 2018, *Memorandum of understanding between the U.S. Securities And exchange commission and the U.S. Commodity futures trading commission regarding coordination in areas of common regulatory interest and information sharing,* Commodity futures trading commission, accessed 30 March 2022, www.cftc.gov/sites/default/files/2018-07/CFTC_MOU_InformationSharing062818.pdf.

40. United States Securities and Exchanges Commission 2017, *Investor Bulletin: Initial Coin Offerings,* accessed 30 March 2022, www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins-16.

41. United States Securities and Exchanges Commission 2017, *Guidance Update,* accessed 30 March 2022, www.sec.gov/investment/im-guidance-2017-02.pdf.

42. Givczy, AV, Pairolero, NA & Toole A 2021, 'Identifying Artificial Intelligence (AI) Invention: A Novel AI Patent Dataset', *The Journal of Technology Transfer*, USPTO Economic Working Paper No. 2021-2, accessed 30 March 2022 from SSRN, https://ssrn.com/abstract=3866793.

43. Bradley, WA & Kolev, J 2022, *Software Piracy and IP Management Practices: Strategic Responses to Product-Market Imitation,* accessed 30 March 2022 from SSRN, https://ssrn.com/abstract=3912074.

44. Office of the Chief Economist 2020, *Inventing AI: Tracing the diffusion of artificial intelligence with U.S. patents,* United States Patent and Trademark Office, accessed 30 March 2022, www.uspto.gov/sites/default/files/documents/OCE-DH-AI.pdf.

45. Miller, RD & Toole, AA 2018, *International Collaboration and Ownership on Patents Issued to Chinese Inventors*, Office of the Chief Economist, accessed 30 March 2022, www.uspto.gov/sites/default/files/documents/IPDataHighlights_China_final.pdf.

46. Congress.Gov 2022, *S.2992 - American Innovation and Choice Online Act,* Library of Congress, accessed 30 March 2022, www.congress.gov/bill/117th-congress/senate-bill/2992/cosponsors. See also: Congress.Gov 2022, *H.R.3816 - American Innovation and Choice Online Act*, Library of Congress, accessed 30 March 2022, www.congress.gov/bill/117th-congress/house-bill/3816.

47. Committee on the Judiciary n.d., *Senate Subcommittee on Privacy, Technology and the Law*, accessed 30 March 2022, https://www.judiciary.senate.gov/about/subcommittees/subcommittee-on-privacy-technology-and-the-law.

48. House Committee on Energy and Commerce 2022, *Communications & Technology,* U.S. House of Representatives, accessed 31 March 2022, https://energycommerce.house.gov/newsroom/press-releases/pallone-opening-remarks-at-health-legislative-hearing-on-mdufa.

49. *H.R.3816 - American Choice and Innovation Online Act*, Library of Congress, accessed 30 March 2022, www.congress.gov/bill/117th-congress/house-bill/3816.

50. Committee on the Judiciary, *Subcommittee on Privacy, Technology and the Law,* United States Senate, accessed 30 March 2022, www.judiciary.senate.gov/about/subcommittees/subcommittee-on-privacy-technology-and-the-law.

Authors and Affiliations

Amit Sing	Accenture
Dr Jensen Sass	Australian National University
Johanna Weaver	Australian National University
Sarah O'Connor	Australian National University
Dr Rogier Creemers	Leiden University
Kadri Kaska	e-Governance Academy
Elsa Neeme	NATO Cooperative Cyber Defence Centre of Excellence (CCDOE)
Dr Patryk Pawlak	EU Institute for Security Studies
Cherie Lagakali	Global Forum on Cyber Expertise
Lola Attenberger	The European School of Management and Technology (EMST Berlin)
Jhalak M. Kakkar	National Law University Delhi
Shashank Mohan	National Law University Delhi
Bilal Mohamed	National Law University Delhi
Mira Swaminathan	National Law University Delhi
Hiroki Habuka	The University of Tokyo
Mark Williams	The Azure Forum for Contemporary Security Strategy
Matthew G. O'Neill	The Azure Forum for Contemporary Security Strategy
Caitríona Heinl	The Azure Forum for Contemporary Security Strategy
Dr Yong Lim	Seoul National University
Dr Sangchul Park	Seoul National University
Dr Haksoo Ko	Seoul National University
Jonggu Jeong	Seoul National University
Eunjung Cho	Seoul National University
Haesung Lee	Seoul National University
Benjamin Ang	Nanyang Technological University Singapore
Sithuraj Ponraj	Nanyang Technological University Singapore
Dr Jose Tomas Llanos	University College London
Dr Diana Bowman	Arizona State University
Nicholas Davis	Arizona State University
Walter G. Johnson	Arizona State University

Annex A: List of Organisations Represented by Interviewees

All interviews were conducted on a non-attribution basis to encourage frank responses.
Organisations marked with an asterisk (*) participated at Agency Head or Chief Executive Officer level.
Organisations marked with a (#) participated in multiple interviews.

- Accenture
- Amazon Web Services (AWS)
- Atlassian
- Australian Competition and Consumer Commission (ACCC)*#
- Australian Communications and Media Authority (ACMA)
- Australian Human Rights Commission (AHRC)*
- Australian Research Council Centre of Excellence for Automated Decision-Making and Society*
- Centre for Responsible Tech, The Australia Institute*
- Committee for Economic Development of Australia (CEDA)*
- Department of Home Affairs
- Department of Prime Minister and Cabinet #
- Digital Industry Group Inc. (DIGI)*
- Google
- Gradient Institute*#
- IP Australia*
- International Cyber Policy Centre, The Australian Strategic Policy Institute (ASPI)*
- Microsoft #
- Office of the Australian Information Commissioner (OAIC)*
- Office of the eSafety Commissioner (eSafety)*
- Productivity Commission
- Reset Australia*
- SWIFT Partners*
- Tech Council of Australia*
- Treasury
- UNSW Allens Hub for Technology, Law and Innovation*
- University Technology Sydney (UTS)
- Yahoo!

Annex B: List of Questions posed to Interviewees

1. How do you define 'the tech sector'? Many describe the tech sector as a horizontal enabler, rather than a vertical sector. Do you agree?

2. Within the tech sector, what regulated activities should fall within the mandate of tech regulator(s)? Are some activities more suited to oversight by specialist tech regulator(s), and others more suited to generalist oversight? If yes, please specify.

3. What skills, expertise, and tools would tech regulator(s) need to be effective?

4. What institutional structure would best support developing and sustaining those skills, expertise, and tools?

5. Three tech regulator models are popularly posited: 1) establishment of a stand-alone tech regulator; 2) assimilation of tech-specific responsibilities into the mandates of existing regulators; or 3) a hybrid of one and two. What are the merits and pitfalls of each, and is there an alternative model that should be considered?

6. Can you give examples of countries or jurisdictions with novel and/or effective tech regulator model(s)?

7. What role is there for international engagement with other regulators/governments to shape global approaches to tech regulation?

8. Are there any comparative regulated industries from which lessons could be drawn?

Australian National University

TECH POLICY DESIGN CENTRE

Tech Policy Design Centre
Birch Building (#35), 35 Science Rd, Australian National University, Acton ACT 2601

E: techpolicydesign@anu.edu.au

TPDesignCentre