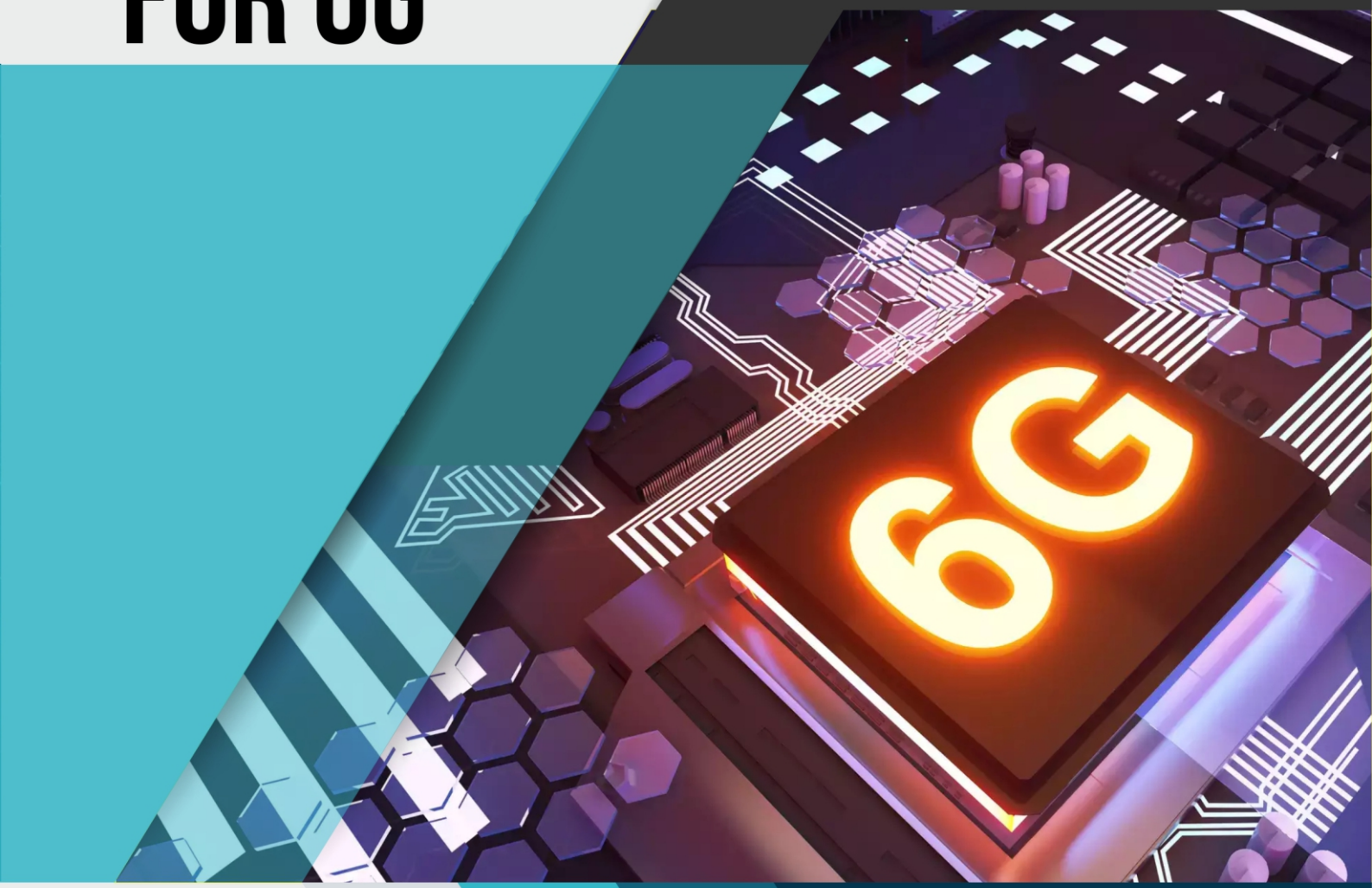
# AN ETHICAL FRAMEWORK FOR 6G




CUTS International
1983-2023

#2410

# An Ethical Framework for 6G

# An Ethical Framework for 6G

*Published by*

**CUTS International**
D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org, Web site: www.cuts-international.org

*Partnership with*

ARPI Australian Risk Policy Institute & iit-b ज्ञानमुत्तमम्

*Supported by*

Australian Government
Department of Foreign Affairs and Trade



#2410

# Contents

*Acknowledgement* ..... *5*
*Abbreviations* ..... *6*
*Executive Summary* ..... *8*
*About the Project* ..... *11*
*Methodology* ..... *12*

**1. Introduction ..... 13**

**2. Cyber Security ..... 17**
2.1. Significance of Cyber Security in 6G Development ..... 17
2.2. Cyber Security Framework in India ..... 18
2.3. Cybersecurity Framework in Australia ..... 27
2.4. Key Cybersecurity Components of the Ethical Framework for 6G ..... 28

**3. Protection of Privacy ..... 31**

**4. Potential Competition Concerns in 6G ..... 34**
4.1. Competition Issues in Telecom Sector ..... 35
4.2. Standard Essential Patents (Seps) and Frand Terms ..... 38
4.3. Pro-Competition Technologies ..... 42
4.4. Competition Issues in the Cloud Services Market ..... 44
4.5. Artificial Intelligence and Competition ..... 48

**5. Consumer Protection ..... 53**
5.1. Consumer Protection Framework in Australia ..... 53
5.2. Consumer Protection Frameworks in India ..... 55

**6. Trusted 6G Ecosystem ..... 57**
6.1. Ingredients of a Trusted Digital Ecosystem ..... 57
6.2. Trusted Network Communication ..... 59
6.3. Cross-Border Data Flow With Trust ..... 60

**7. Inclusive and Sustainable 6G ..... 64**
7.1. 6G: Bridging the Digital Divide ..... 67
7.2 Sustainability ..... 72

**8. Stakeholders Insights ..... 74**
8.1. Cyber security ..... 74
8.2. Privacy ..... 74
8.3. Competition ..... 75
8.4. Consumer Welfare ..... 76
8.5. Trusted Ecosystem ..... 76
8.6. Sustainability and Inclusivity ..... 77

**9. Conclusion and Recommendations..... 78**
9.1. Conclusion.....78
9.2. Recommendation.....79
**References..... 88**
**Endnotes..... 90**

# Acknowledgement

The completion of the research component "Ethical Framework for 6G" would not have been possible without the invaluable contributions of several individuals and institutions. We extend our gratitude to Ujjwal Kumar, Associate Director at CUTS International, for his leadership and guidance throughout this project.

We also acknowledge the efforts and contributions of Sangeetha Mugunthan, former Coordinator, CUTS Washington DC.

We are thankful to V. Sridhar from the International Institute of Information Technology Bangalore (IIIT-B) for his academic insights, expertise and active contribution, which greatly enriched the report.

We also appreciate Tony Charge, President and Chairman of ARPI and Allan Asher, Vice-President of Competition & Consumer Policy at ARPI, for their strategic perspectives and support.

We are grateful for the efforts of Akshay Sharma from the Programme Team, and Sweepthish Jayan and Keval Sharma from the Information Technology Team. We sincerely thank Madhuri Vasnani, Shivendra Shekhawat, Mukesh Tyagi and Rajkumar Trivedi from the Publications Team at CUTS International for their exemplary support in bringing this report to fruition.

We express our sincere gratitude to all individuals, whether or not named above, without whom the publication of this report would not have been possible. Finally, any remaining errors are ours alone.

Asheef Iqubbal and Krishaank Jugiani
Senior Research Associates, CUTS International

# Abbreviations

| | | |
|---|---|---|
| ACCC | : | Australian Competition and Consumer Commission |
| ACMA | : | Australian Communications and Media Authority |
| AI | : | Artificial Intelligence |
| CCMP | : | Cyber Crisis Management Plan |
| CCI | : | Competition Commission of India |
| CERT | : | Computer Emergency Response Team |
| CIIP | : | Critical Information Infrastructure Protection |
| CII | : | Critical Information Infrastructure |
| CMA | : | UK Competition and Markets Authority |
| COC | : | Convention on Cybercrime |
| CTSO | : | Chief Telecommunications Security Officer |
| D2D | : | Device-to-Device |
| DFFT | : | Data Free Flow with Trust |
| DoT | : | Department of Telecommunications |
| DPDP Act | : | Digital Personal Data Protection Act |
| FTC | : | Federal Trade Commission |
| GDPR | : | General Data Protection Regulation |
| ICTs | : | Information and Communication Technologies |
| IoT | : | Internet of Things |
| ITU | : | International Telecommunication Union |
| LEO | : | Low Earth Orbit |
| M&As | : | Mergers and Acquisitions |
| MEC | : | Multi-Access Edge Computing |
| ML | : | Machine Learning |
| NCCIC | : | National Cybersecurity and Communications Integration Centre |
| NCCC | : | National Cyber Coordination Centre |

| | | |
|---|---|---|
| NTNs | : | Non-Terrestrial Networks |
| NTRO | : | National Technical Research Organisation |
| Open RAN | : | Open Radio Access Network |
| ppFL | : | Privacy-Preserving Federated Learning |
| QoE | : | Quality of Experience |
| QoS | : | Quality of Service |
| QKD | : | Quantum Key Distribution |
| RAN | : | Radio Access Network |
| SEPs | : | Standard Essential Patents |
| SSOs | : | Standard Setting Organisations |
| TRAI | : | Telecom Regulatory Authority of India |
| VLCs | : | Visible Light Communications |
| ZTA | : | Zero Trust Architecture |

# Executive Summary

As 6G technologies unlock new capabilities and applications, it is essential to address their ethical and social implications. Key concerns include safeguarding data privacy, cybersecurity, competition, trust, consumer protection and ensuring equitable access to these advanced services. The roles of these elements are interconnected, representing different aspects of next-generation networks. Building an ethical 6G system presents multidisciplinary challenges, constituting technology, regulation, economics, politics, and ethics. This paper explores the fundamental challenges across these critical domains.

- Cybersecurity challenges are heightened by 6G's deep integration across devices, applications, and critical infrastructure. The interconnected nature of 6G, combined with the growth of IoT and autonomous systems, expands the attack surface and requires robust security strategies. Measures like security-by-design, zero-trust architectures, quantum-resistant encryption, AI-driven threat detection, and federated learning are essential. Together, these approaches aim to build resilient systems that protect user data from sophisticated cyber threats.

- Privacy is a central concern in the 6G framework due to the extensive data collection and processing it facilitates. With 6G networks integrating biosensing, digital twins, and autonomous systems, the risks to individual privacy grow significantly. For instance, there is currently no clear method to determine when linked, deidentified data sets become personally identifiable, posing significant risks across digital technologies. Privacy-by-design principles, which embed privacy considerations into technology development from the outset, are essential. Advanced technologies such as secure multi-party computation, synthetic data generation, and blockchain-based data brokerage can enhance data integrity and prevent misuse. However, existing regulations like the GDPR and India's DPDP Act have gaps that must be addressed to keep pace with these evolving challenges.

- With 6G networks set to manage massive data traffic and countless connected devices, energy efficiency is crucial. Sustainable hardware, advanced power management, and efficient network designs are essential to reduce environmental impact and operational costs. Inclusivity and sustainability are crucial to the ethical framework of 6G, aiming to bridge the digital divide and

ensure its benefits reach underserved communities. Making 6G affordable and accessible while adopting environmentally sustainable practices is essential. These efforts align with global sustainable development goals, ensuring 6G promotes societal progress without worsening existing inequalities.

- Consumer protection is another important part of the ethical 6G framework. The rapid advancement of 6G technologies challenges the alignment of consumer rights with technological progress. Strengthening grievance redressal mechanisms and implementing policies to protect users from harms like data breaches, unfair pricing, and exploitative practices are essential to safeguarding digital rights. Transparency and accountability must be prioritised, ensuring stakeholders follow ethical standards and are held responsible for any violations.

- Potential competition concerns are a vital area requiring attention, given the potential for market concentration and anticompetitive behaviours in a 6G-enabled landscape. The interplay between telecommunications and emerging technologies like AI and cloud computing could lead to new forms of dominance and unfair practices. This raises the need for pre-emptive measures to address these concerns, including fostering innovation, encouraging fair competition, and preventing monopolistic tendencies. The role of regulatory bodies, such as the Competition Commission of India and the Australian Competition and Consumer Commission, in monitoring and addressing these challenges also becomes important.

- The future 6G network must integrate embedded trust to ensure higher levels of information security. As 6G connects the physical and digital worlds, the safety of the system depends on secure information. Therefore, building a trustworthy 6G network is essential. Achieving this will require close collaboration among governments, industry leaders, researchers, and civil society. Building trust in 6G systems is crucial for widespread adoption and ensuring that the technology benefits the public. This includes maintaining a free and open cyberspace, addressing challenges related to cross-border data flows and geopolitical tensions, and fostering international cooperation. Global standards that promote interoperability, inclusivity, and innovation will be key to creating a secure and reliable 6G network that serves the public good.

The development of ethical 6G is a dynamic and collaborative process that requires input from various stakeholders and the ability to adapt to emerging challenges. Our goal is to guide the responsible deployment of 6G technologies, ensuring they align with societal values and deliver positive economic, social, and environmental

outcomes. By addressing the complex risks and opportunities of 6G, this framework aims to create a foundation for a future where 6G technology transforms connectivity and services while protecting consumer rights.

Australia and India have potential for collaboration in advancing for ethical 6G development and deployment. Both countries are committed to contributing to global efforts in this area. India's contributions and aspiration can be seen in the Bharat 6G Vision document, while Australia's strong cybersecurity capabilities provide a solid foundation for partnership. By leveraging each other's strengths, this collaboration can play a key role in addressing the growing focus on emerging technologies like 6G. Their shared emphasis on innovation, cybersecurity, and inclusivity creates a strong basis for joint initiatives that promote the responsible advancement of 6G technologies.

# About the Project

The project, titled "Ethical 6G: Identifying Elements of an Ethical Framework for 6G and Creating Opportunities for India and Australia," is a collaborative effort between CUTS International, the Australian Risk Policy Institute (ARPI), and the International Institute of Information Technology, Bangalore (IIITB). This initiative is supported by the Department of Foreign Affairs and Trade (DFAT), Australia, under the Australia-India Cyber and Critical Technology Partnership (AICCTP) Grant.

Recognising the critical importance of cyber technologies and their growing influence on international relations, the AICCTP was formed with the primary aim of fostering an open, secure, free, accessible, stable, peaceful, and interoperable cyberspace. Emerging technologies like Artificial Intelligence, next-generation telecommunications, the Internet of Things, quantum computing, synthetic biology, blockchain, and big data are central to this partnership.

The project is grounded in the comprehensive strategic partnership between India and Australia, signed in June 2020. It focuses on fostering cooperation between both countries, particularly developing next-generation networks such as 5G and 6G, emphasising security, resilience, and diverse technology supply chains. The project aims to identify elements for an ethical framework for future 6G technology, create an enabling environment for Indian and Australian institutions to participate in the 6G standard-making process, and develop opportunities for firms in both nations to invest in and promote 6G in the Indo-Pacific region.

The research outputs are divided into four components:

1. Understanding 6G: Development and Challenges
2. Strategic Opportunities for Australia and India from 6G
3. Standardising Standard Setting for 6G
4. Identifying Elements of an Ethical Framework for 6G

# Methodology

We used a two-stage methodology to investigate the challenges and issues related to 6G deployment. In the first stage, we reviewed recent literature, including research papers, industry reports, and government regulations and policies, focusing on key techno-social aspects of 6G. This included examining standards, cooperation between Australia and India, and ethical frameworks addressing issues such as privacy, trust, competition, and sustainability. In the second stage, based on the insights gained from this literature survey, we conducted structured interviews with experts in the technical, socio-economic, legal, and regulatory fields from August 2022 to February 2024. These interviews were carried out both online and during workshops held in Delhi and Bangalore, India, as well as at the Australian National University in Australia.

| Category | Number of Experts: Technical | Number of Experts: Social science, economics, legal, policy |
|---|---|---|
| Academia (Researchers and Faculty at Universities and Institutes) | 9 | 5 |
| Industry (Mobile Network Operators, Mobile Chip Design firms, Network Equipment Manufacturers, Telecom start-ups, Enterprise service providers) | 4 | 4 |
| Civil Society/ Policy Advocates | 1 | 7 |
| Industry Associations (of Telecom operators, Internet companies) | 3 | 4 |
| Government representatives/ Regulatory bodies | 2 | 6 |
| **Total** | **19** | **26** |

# 1 Introduction

Ethical frameworks guide the moral and legal outcomes of actions, serving as a foundation for advancing ethical technologies.[1] These frameworks, built on ethical ideals, provide technologists with a reference for implementing data-driven solutions. However, principles alone can be mysterious and challenging to apply in practice. The conflict between ethical obligations and corporate realities is often exacerbated by ethical frameworks, standards, and regulations, highlighting the need for a strategic approach to resolve these challenges. The telecommunication sector, in particular, recognises the necessity of an ethical framework. Key ethical issues in this sector include the use and management of personal information, ensuring inclusive access, and data security.[2]

Recent cyber breaches, such as those experienced by Optus, Medibank, and AIIMS, underscore the critical need for ethical frameworks in technology.[3] These incidents have revealed vulnerabilities in current systems and demonstrated the significant economic and consumer welfare losses resulting from poor standards, inadequate rollouts, and fraud. As we transition from 3G, 4G, and 5G technologies to the emerging 6G landscape, it is imperative to anticipate and address these issues proactively. This approach will ensure that stakeholders in the 6G ecosystem are better prepared to safeguard consumer welfare and maintain high security and reliability standards. The rapid advancements in technology, including the integration of artificial intelligence (AI), require a forward-thinking strategy to prevent the pitfalls of previous technological rollouts and enhance overall service quality and consumer trust.

The risks and vulnerabilities associated with 6G technology are complex. These include the potential for increased cyber threats as the connectivity and integration of devices become more pervasive.[4] The concept of virtual nations, where digital environments and identities play a significant role, introduces new dimensions of cybersecurity risks and challenges in governance. The reliance on AI and machine learning in 6G networks increases the potential for sophisticated cyber-attacks, such as adversarial AI and deep fakes, while also raising the risk of internal errors and systemic failures.[5] Additionally, the rapid data processing capabilities of 6G networks could enable more pervasive surveillance techniques, posing serious threats to individual privacy and civil liberties.[6] The vast data capacity and processing power of 6G networks amplify the risk of large-scale data breaches and unauthorised access, necessitating robust encryption, advanced security protocols, and new regulatory frameworks to protect user privacy.[7]

Moreover, the proliferation of IoT devices connected through 6G networks increases the attack surface, requiring comprehensive security strategies to mitigate these risks.[8] The security of autonomous systems, like self-driving cars and drones, also becomes paramount, as vulnerabilities in these technologies could have severe safety implications.[9] The sheer scale and sophistication of 6G technology demand robust and adaptive security measures to counteract potential threats and ensure the integrity of the system.[10] Addressing these risks requires a comprehensive understanding of the technology and a commitment to developing resilient and secure systems. This research project, undertaken as part of the AICCTP initiative, aims to identify and analyse the key elements of an ethical framework for 6G technology.

We have identified six critical components of an ethical framework for 6G technology, each presenting unique challenges and opportunities for policy intervention:

1. *Cybersecurity:* Given the increasing sophistication of cyber threats and the potential for widespread disruption in a 6G-enabled world, robust cybersecurity measures are paramount. This section will examine current cybersecurity regimes in Australia and India, identify strengths and weaknesses, and explore innovative approaches such as security-by-design and zero-trust architectures.
2. *Privacy Protection:* As 6G technologies enable the collection and processing of vast amounts of personal data, protecting individual privacy becomes increasingly complex. This study will analyse existing data protection frameworks and evaluate their adequacy in the context of 6G.
3. *Consumer Protection:* The rapid evolution of 6G technologies and services may outpace existing consumer protection mechanisms. This section will assess current laws in both countries and identify areas for improvement to ensure that consumers are adequately protected in the 6G era.
4. *Competition:* The rollout of 6G has the potential to reshape market dynamics in the telecommunications and digital space. This section will examine issues such as market concentration, standard-essential patents, net neutrality, and the competitive implications of emerging technologies like AI in the context of 6G.
5. *Trusted 6G Ecosystem:* Building trust in the 6G ecosystem is crucial for widespread adoption and success. This section will explore the components of a trusted digital ecosystem, including secure networks, cross-border data flows, and the promotion of a free and open cyberspace in the Indo-Pacific region.
6. *Inclusivity and Sustainability:* Ensuring that 6G technology contributes to bridging the digital divide and supports sustainable development goals is a key ethical imperative. We will examine strategies for achieving ubiquitous and sustainable 6G deployment, addressing issues of accessibility, affordability, and environmental impact.

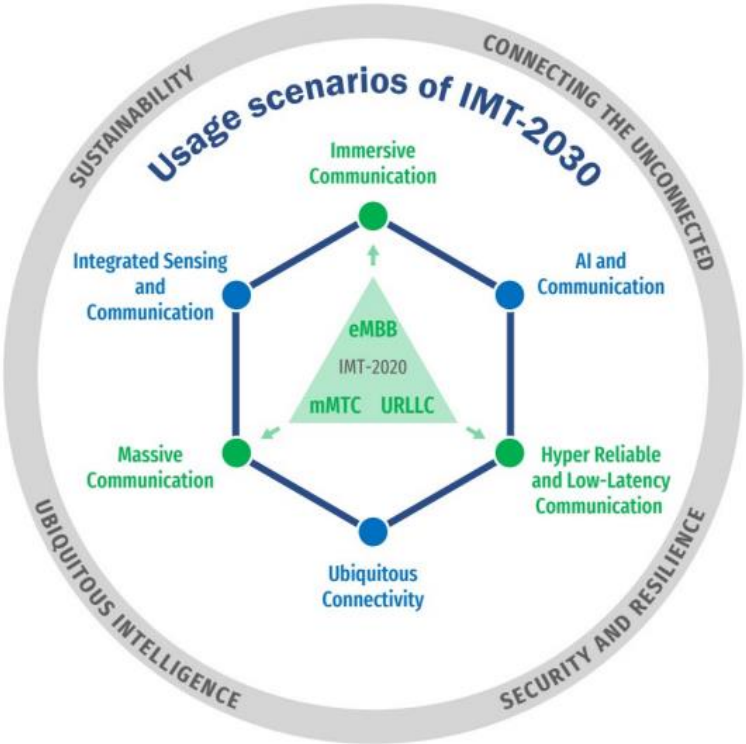
By addressing these six key areas, this research paper aims to provide a comprehensive framework for ethical considerations in the development and deployment of 6G technology.

The Bharat 6G Vision Document and the ITU 6G Vision (IMT-2030) outline several of these components as fundamental guiding principles for the implementation of 6G.

**Figure 1: Key guiding principles for 6G**


*Bharat 6G Vision Document*

**Figure 2: Usage scenario of IMT-2030, ITU**



The findings and recommendations from this study will be valuable for a wide range of stakeholders, including policymakers, industry leaders, researchers, and civil society organisations working towards the responsible advancement of 6G technology. The relevance of this research is underscored by the global nature of 6G development and the need for international cooperation in establishing ethical standards. As 6G technology is expected to enable seamless global connectivity and support critical applications across various sectors, including healthcare, transportation, and smart cities, the ethical implications extend far beyond national borders. Therefore, the collaborative approach between Australia and India through AICCTP serves as a model for international cooperation in addressing complex challenges.

Moreover, the ethical framework developed through this research has the potential to inform not only national policies but also contribute to ongoing discussions at regional and multilateral forums. As both Australia and India play significant roles in shaping technology policy on the global stage.

# 2 Cyber Security

## 2.1. Significance of cyber security in 6G development

The advent of 6G networks promises advancements in wireless communication technology and improved security, incorporating quantum-resistant encryption[11], Artificial Intelligence (AI) driven threat detection[12], and decentralised trust mechanisms[13] to ensure data protection. However, the increased complexity of 6G networks also presents challenges. Its openness, greater connectivity and interoperability blurs the line between internal and external environments, allows for more potential entry points for malicious actors, making it harder to defend against external intruders using traditional security measures like IPsec (Internet Protocol Security) and firewalls.[14]

As data is processed and stored at the edge in edge computing, it becomes more vulnerable to unauthorised access or tampering.[15] Integrating AI and Machine Learning (ML) also raises concerns about potential exploitation.[16] For example, attackers can manipulate AI models or use ML algorithms to develop sophisticated attacks that evade traditional security measures. The proliferation of Internet of Things (IoT) devices in 6G networks provides a larger attack surface due to the massive number of interconnected devices, leading to unauthorised access, data breaches, and potentially compromising the entire network infrastructure.[17]

Technical measures like encryption, access controls, secure communication protocols, rigorous validation of AI systems, quantum security, secure boot processing, firmware updates, and strong authentication mechanisms are necessary to protect against unauthorised access and data breaches.[18] Implementing a Zero Trust security model, where every user and device is treated as untrusted until verified, can help mitigate the risks associated with the blurred network boundaries.[19]

However, technical measures alone may not be sufficient to address the security challenges effectively. Regulatory frameworks are equally important and mandatory to deal with these issues comprehensively. Regulatory frameworks set security requirements, protocols, and audits for organisations and network operators, holding them accountable for breaches and non-compliance. This ensures consistent security measures, addressing security threats, protecting privacy, and maintaining trust.

In 6G networks, data ownership and control become critical due to increased data entities collecting and processing personal data, including users, device manufacturers, cloud providers and network providers.[20] Legal disputes could occur over the rights to access, use, and share the data generated. Security breaches may lead to parties denying responsibility or misusing data, leaving consumers vulnerable.

Telecom networks' borderless nature may cause overlapping laws and jurisdictional conflicts in 6G incidents, involving parties from different locations, making it challenging to adhere to the 'law of the land'.[21] Thus, compliance with regulatory frameworks, including telecom, cyber security, and data protection laws, can be complex when deploying 6G. Additionally, the implementation of 6G networks could raise national security concerns, particularly regarding potential surveillance capabilities and vulnerabilities to cyber-attacks.

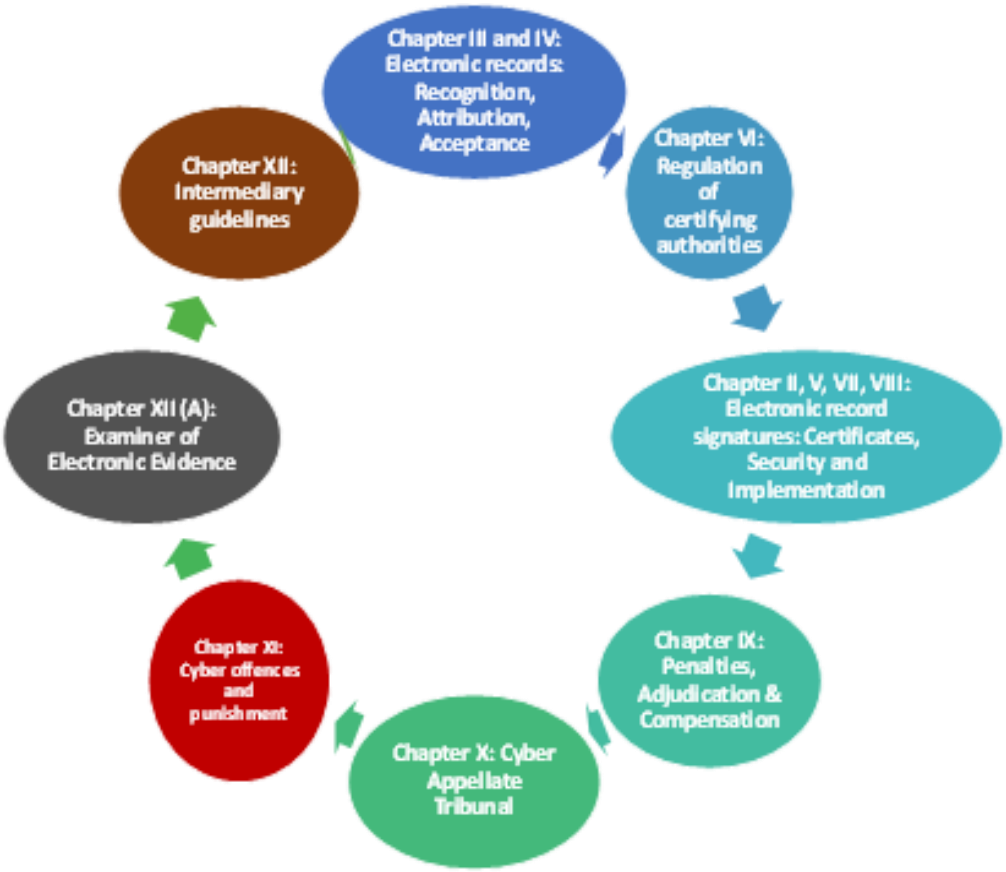
Thus, both India and Australia need adequate policies to address security concerns and protect end-user data. Both the countries can also lead the global south in developing the standards that can guide countries in securing their cyberspace, especially in 6G. Legal frameworks that involve striking a balance between data sharing, security needs and protecting individual rights and freedoms are crucial. 6G cyber regulations encompass a wide range of aspects including data protection, security standards, encryption, vulnerability reporting, IoT device security, liability, and national security. International cooperation will need harmonisation along with adhering to different regional and international regulatory requirements. Addressing these legal challenges will require a comprehensive and cooperative approach involving governments, regulators, industry stakeholders, and legal experts. Clear and adaptable legal frameworks, alongside transparent security practices, will be critical to ensuring the safe and responsible deployment of 6G technology in the future.

## 2.2. Cyber security framework in India

### 2.2.1. Cyber Security Policy, Law and Regulation

The National Cyber Security Policy was drafted by the MeitY in 2013 that addresses all aspects of cyber security with the vision *to build a secure and resilient cyberspace for citizens, businesses and Government*. The policy addresses broadly the various aspects discussed in this chapter including cyber security protection, incidence response, capacity building, protection of critical information infrastructure, research and development, standardisation, and product certification. The Indian IT Act 2000 comprehensively covers all aspects of cyber security (MeitY, 2000). Different chapters and clauses that cover aspects of cyber security are presented in the following Figure.

**Figure 3: Illustration of how Indian IT Act addresses the National Cyber Security**




*Source: Sridhar (2019)*

### 2.2.2. Information Security in India

Presently India has the second largest Internet users, second largest mobile subscribers and second largest broadband subscribers in the world. The Government of India initiated a number of digital technology-enabled programmes such as Aadhaar, MyGov, Government e-Market, DigiLocker, Bharat Net, Start-up India, Skill India and Smart Cities. India is the third largest hub for technology driven start-ups in the world. Thus, there is a huge domestic demand for digitised services in the country.

Increased digitisation has also led to more sophisticated cyber threats. The cyber threat landscape is dynamic and evolving with innovative technologies and attackers. Cyberspace is also increasingly subject to criminal and terrorist activities. Over a period, the nature and pattern of incidents are becoming more sophisticated and complex. The attacks and intrusions targeted previously at only enterprises have started affecting common citizens and society at large.

India witnessed 1.4 million cybersecurity incidents in 2021, and 212,000 incidents in January and February 2022 alone (Internet Society, 2023). According to an IBM survey conducted in 2021, the average cost of a data breach in India is ₹165 million (roughly US$2.12 million). The average mean time to identify a data breach stood at 239 days, and the time to contain a data breach at 81 days (IBM 2020).

Realising the risks associated with cyber security incidents, both enterprises and nation states are taking precautions in terms of deploying security enhancing technologies. The States have also taken recourse to enabling legal protection of cyber citizens against cyberattacks.

### 2.2.3. Cyber Security Protection and Enforcement

Government and business entities across the country have faced cybersecurity challenges in effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and data. Further they face the uphill tasks of detecting, responding to, and recovering from cyber security incidents. Hence protecting the information assets of individuals, society, businesses and government and responding to incidents in a timely manner to mitigate risks forms part of national security functions. Further, there shall be enabling infrastructure to detect and analyse cyber security incidence through cyber forensics and to deter and if required punish cyber criminals from indulging further in malicious activities through appropriate enforcement of cyber laws and regulation is also considered as part of this pillar. The different aspects of this pillar on protection and enforcement are given in the following Figure.

**Figure 4: Protection and Enforcement programmes**


*Source: Adapted from Sridhar (2019)*

### 2.2.4. Incident Response and Crisis Management

The United States' Computer Emergency Response Team (CERT) created in 2000 still stands as a benchmark government initiative to improve cyber security vigilance in the country. Today, The National Cybersecurity and Communications Integration Centre's (NCCIC) coordinates cyber and communications information, technical expertise, and operational integration, promotion of cyber security awareness, analysis, and incident responses for the U.S. The Indian IT Act 2008 specifies as follows (MeitY, 2008, p 29):

The Indian Computer Emergency Response Team (CERT-In) shall serve as the national agency to perform the following functions in the area of cyber security:

1. Collection, analysis and dissemination of information on cyber incidents
2. Forecast and alerts of cyber security incidents
3. Emergency measures for handling cyber security incidents
4. Coordination of cyber incident response activities
5. Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
6. Such other functions relating to cyber security as may be prescribed.

CERT-In has set up phase 1 of National Cyber Coordination Centre (NCCC) to generate necessary situational scenarios of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities. A Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/Departments of Central Government, State Governments/Union Territories (UTs) and their organisational units in critical sectors has been formulated. In addition, several guideline documents and templates have been published to assist development and implementation of sectoral Cyber Crisis Management Plans. CCMP for countering Cyber-Attacks and Cyber Terrorism is updated periodically to take into account the changing scenario of cyber threat landscape (MeitY, 2018a).

While CERT-In is the national centre for cyber security response, different states in their state policies on cyber security have advocated setting up of their own CERTs. These state CERTs are expected to coordinate with CERT-In on various aspects including detect, prevent and mitigate cyber-attacks and incidents. Recent notification by CERT-In reinforces the role of CERT-In in promoting cyber security at all levels – individuals, firms and government (CERT-In, 2023).

The government has also notified the Telecommunications (Telecom Cyber Security) Rules, 2024, under the Telecommunications Act, 2023, to enhance the cyber security

of communication networks. Key provisions include mandatory reporting of security incidents within six hours, the appointment of a Chief Telecommunications Security Officer (CTSO), and the establishment of robust cyber security policies by telecom entities. These rules aim to prevent cyber crimes and ensure the secure handling of telecom data,[22] although concerns have been raised about privacy risks due to extensive data collection and storage without judicial oversight. The rules represent a significant step in fortifying India's telecom infrastructure and ensuring robust cyber security measures.

### 2.2.5. Cyber Crime Investigation

The IT Act 2000 provides the legal framework for handling cybercrimes in the country (MeitY, 2008). Since crime and policing is a concurrent subject, each State has set up its cybercrime police stations and cyber forensic labs to handle cybercrimes. It is notified in Section 79 (A) of the IT Act that an Examiner of Electronic Evidence be set up by the Central Government for providing expert opinion on electronic form evidence before the court of law. MeitY has accredited some of the institutions including Cyber Forensic Labs in certain States under this section. These labs assist the Investigating Officers to analyse the electronic evidence in cybercrime investigation.

While criminal offences can be effectively managed within countries, threats to national cyber security perpetrated by non-state actors who cross national borders. There are instances of cybercrime attacking critical infrastructure in one country and perpetrated by actors residing in other countries. These require cooperation of law enforcement officials across borders to seize the attacker and prosecute. Countries such as Singapore have signed bilateral agreements with other South Asian countries for addressing global cybercrimes (Tan, 2018).

Besides bilateral cooperation, there is deterrent value in participating in international treaties. A joint study by the Hong Kong University of Science and Technology, Yonsei University, and the Singapore Management University determined that states that have signed and ratified the Budapest Convention on Cybercrime experienced a reduction in the number of distributed denial-of-service (DDoS) attacks in their territories (Hui, et al., 2017). Recognizing the importance of international cooperation, the Council of Europe drafted the Convention on Cybercrime (COC), which was adopted by the Committee of Ministers in 2001 (aka Budapest convention). The COC was the first international legislation against cybercrime (CoE, 2001). Apart from providing a substantive legal framework to address international cybercrime, the COC promotes mutual assistance across participating countries in handling forensic evidence of cybercrime. The National Cyber Strategy of the United States indicates the country’s determination to improve international cooperation in investigating cyber terrorism by strengthening the Budapest convention. India, though, did not accede to

the Budapest Convention. Because of the increase in cybercrime, there have been calls for India to reconsider its membership in the Budapest Convention, particularly following the push for digital India.[23] Joining the convention could enhance international collaboration, strengthen legal frameworks, and improve the country's ability to combat cross-border cyber threats effectively.

### 2.2.6. Cyber Secure Critical Information Infrastructure Protection

State's economic prosperity and well-being of its citizens depend on critical information infrastructure across sectors such as Transportation, Telecommunications and the Internet, Banking and Finance, Law and Justice; and that of public sector organisations in the areas of space, energy and utility; and e-government services. With the development of Smart Cities, the urban infrastructure is expected to have more and more digital components. Hence the importance of protecting Critical Information Infrastructure (CII) in the country through cyber protection.

In December 2015, a Ukrainian power station was hacked and merely a quarter of a million residents were left in the dark (Zetter, 2016). In May 2017, a ransomware attack struck more than 40 British hospitals and many other organisations across the world (Woollaston, 2017). One of the recent infrastructure attacks was a major US fuel pipeline that reportedly paid cyber-criminal gang DarkSide nearly $5m (£3.6m) in ransom, following a cyber-attack. In May 2021, the Colonial Pipeline in the U.S. suffered a ransomware cyber-attack and took its service down for five days, causing gas supplies to tighten across the US. The firm reportedly paid the associated cyber-criminal gang DarkSide nearly US$5m in ransom, following a cyber-attack, to resume its operations (BBC, 2021).

Recognizing this, Section 70 of the IT Act recognises CII as a protected system, with computer resources incapacitation or destruction of which shall have a debilitating impact on national security, economy, public health or safety (NCIIPC, 2014, p 5). National Critical Information Infrastructure Protection Centre ("NCIIPC") is an organisation under the administrative control of National Technical Research Organisation ("NTRO") and is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection ("CIIP"). NCIIPC was constituted via a Gazette Notification on 16th January 2014 issued under the Section 70A of the IT Act, 2000. Key responsibilities of NCIIPC include protection of critical infrastructure of the nation through cyber attacks and cyber warfare.

Section 70 of the IT Act enables the government to notify what are critical information infrastructure (CII) and declare them as protected systems. It is noted in this section that CII means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety. Section

70A and 70B of the Act enables the Central Government to set up a national level nodal agency for cyber security incident response, much similar to CERT of the U.S. Consequently CERT-In has been set up by the central government as a national nodal agency under MeitY.
Recently, the TRAI has circulated for public comments draft rules – the Telecommunications (Critical Telecommunication Infrastructure) Rules, 2024[24] – to be notified under the Telecommunications Act, 2023.

As per these rules, a telecom entity has to ensure that Critical Telecommunication Infrastructure (CTI), including spare, hardware and software used therein are in compliance with Essential Requirements (ERs), Interface Requirements (IRs), Indian Telecommunication Security Assurance Requirements (ITSARs), National Security Directive on Telecommunication Sector (NSDTS), and specifications, testing requirements, or conformity assessment issued by competent agencies. Further, among several obligations with respect to CITs, telecom entities are obliged to ensure that vulnerability/threat/risk analysis for telecommunication network architecture of CIT is carried out annually, among others.

### 2.2.7. Products Testing and Certifications for Cyber Security

Testing and certification of IT products for information and cyber security is very important, especially for providing e-government services. The India Common Criteria Certification Scheme (IC3S) has been set up by MeitY as part of Cyber Security Assurance initiatives of the Government of India to evaluate and certify IT security products and protection profiles against the requirements of Common Criteria Standards Version 3.1 R2 at Evaluation Assurance Levels (EAL) 1 through 4 (IC3S, 2018). Presently the scheme provides national certification. The main players in this programme are developers of IT Security Products or Protection Profiles, Sponsors, Common Criteria Test Laboratory (CCTL) and Certification Body. The scheme would also provide a framework for international certification through the National Mutual Recognition Arrangement with the other member countries of Common Criteria Recognition Agreement (CCRA). Along with 24 other countries, India has already become a member of CCRA as a certificate consuming nation and soon will be recognized as a certificate producing nation. As per the article 1 of the CCRA, certificates issued by one-member countries are accepted in other countries without re-certification. As per Common Criteria Portal of India [25]:

> "Common Criteria evaluation is an impartial assessment of an IT product by an independent body. This provides users of such products with confidence in the security functionality provided. It also provides users with a metric to compare the security capabilities of products that they are intending to buy. The IT products to be evaluated are referred to as the Target of Evaluation (TOE). Certification

> provides independent confirmation of the validity of evaluation results, and thereby ensures comparability of these results across all evaluations under the scheme and facilitates mutual recognition of results between national schemes. Certification confirms that the TOE needs its security target to the claimed assurance level and that the evaluation has been conducted in accordance with the standard of the scheme i.e. Common Criteria (e.g. ISO 15408)".

The participation in the scheme and its associated evaluation & certification activities is strictly voluntary (unless mandated by government policy or regulations). In addition, organisations may undertake alternative activities to use Common Criteria and to demonstrate product conformance to IT security requirements. The Certification Body (CB) is the STQC Directorate, Department of Electronics and Information Technology, Govt. of India. The Certification Body has been established under the official administration procedures of Govt. of India to meet the requirements of ISO Guide 65. Individual CCTL can register for empanelment with the STQC directorate as per the associated processes and guidelines. The CB shall enlist the details of the empanelled CCTL indicating the evaluation assurance levels for which they have been empanelled to carry out evaluation as per the requirements of Common Criteria standards. This is similar to the National Information Assurance Partnership (NIAP) that oversees a national program to evaluate Commercial Off-The-Shelf Information Technology products for conformance to the international Common Criteria in the United States (NIAP, 2018).

### 2.2.8. Cyber offences and punishment

Chapter and IX and XI of the IT Act covers all aspects of cybercrime including computer system related theft, appropriation and distortion of electronic records, publishing and dissemination of obscene and explicit material, disclosure of unconsented information, misrepresentation of information, and violation of privacy of individual's information. Privacy related offences as recognised under the Act are discussed in detail in the chapter on Privacy. IT Act also provides in these chapters requirements for protecting computer systems data, damages to computer data and associated penalties and adjudication procedures. The Cyber appellate tribunal for adjudication is presented in chapter X.

While the recognition of electronic records, especially for government processes and services are explained in Chapter III and IV, the Chapters VI, VII and VIII elaborates on the digital certification procedures and associated infrastructure including certifying authorities. Chapter XII of the Act aids cybercrime investigation and forensics by setting up an examiner of electronic evidence as explained in a previous section. Such examiners have been set up in various parts of the country to assist the cybercrime investigating officers and providing support of evidence in the court of law.

### 2.2.9. Electronic intermediaries

In 2021, the Ministry of Electronics and Information Technology (MeitY), in consultation with the Ministry of Information and Broadcasting, introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("Intermediary Rules") under the Information Technology Act, 2000 ("IT Act"). These new rules replaced the earlier Information Technology (Intermediary Guidelines) Rules, 2011.

The Rule 3(1)(j) states that intermediaries must provide information or assistance to government agencies, when requested upon receipt of an order, within 72 hours. This can be for purposes like verifying identity or assisting in the prevention, detection, investigation, or prosecution of crimes, including cybersecurity incidents.

Additionally, under Rule 3(1)(l) intermediaries are required to report any cybersecurity incidents to the Indian Computer Emergency Response Team (CERT-In) and provide any necessary information as per the rules set out in the Information Technology (CERT-In and Manner of Performing Functions and Duties) Rules, 2013.

### 2.2.10. Proposed Digital India Act

There has been consideration in the government to replace the IT Act with a new law to be called Digital India Act, which can comprehensively govern the fast-changing India's digital landscape. The new law can also address cybercrime and promote a secure cyberspace by empowering agencies like CERT-In for cyber resilience; strengthening the penalty framework for non-compliance, advisories on the information & data protection, etc.[26] It also proposes adjudicating user harm against cyber-flashing, dark web, deep fakes, protecting women and children against cybercrime, etc. The most important part is the proposed regulation of hi-risk AI systems through legal, institutional quality testing framework to examine regulatory models, algorithmic accountability, zero-day threat & vulnerability assessment, examine AI based ad-targeting, content moderation etc. It will harmonise laws, regulate emerging technologies such as Artificial Intelligence (AI) and incorporate industry input on blockchain and Web 3.0 regulations to protect digital citizens.[27]

Some media reports also inform about the government working towards a new cyber security law that will aim to establish modern legal guidelines for online safety and combat cyber fraud.[28] It could either act as a supplement or may be integrated into the Digital India Bill, defining penalties for cyber breaches and clarifying the identity of cybercriminals. The legislation responds to the need for specific provisions in addition to the existing criminal laws, ensuring a comprehensive approach to addressing contemporary cybercrime challenges.

## 2.3. Cybersecurity Framework in Australia

In the case of Australia, the Privacy Act 1988, the Crimes Act 1914, the Security of Critical Infrastructure Act 2018 and the Telecommunications (Interception and Access) Act 1979 are some of the regulations that deal with cyber security. The Privacy Act 1988[29] is the principal legislation protecting the handling of personal information about individuals. The Crimes Act 1914[30] includes provisions related to cyber security, addressing offences like unauthorised access to computer data, computer-related fraud, and cybercrimes. The Australian Cyber Security Centre (ACSC)[31] is the Australian Government's lead agency for private and public sector collaboration and information-sharing on cyber security.

In the aftermath of two major cyberattacks – Optus and Medibank – that affected a large population, the Australian Government in December, 2022 announced the overhaul of its cyber security strategy to strengthen the country's critical infrastructure.[32] After conducting wide scale consultations, the government released the 'Australian Cybersecurity Strategy 2023-2030' in November 2023, adopting a collaborative approach between government, industry, and individuals with the goal of Australia becoming a global leader in cybersecurity by 2030 in three phases.

The Strategy embodies the following six interlocking "shields" representing different areas of focus[33]:

- **Shield 1. Strong Businesses and Citizens:** Empowering individuals and businesses to defend themselves online.
- **Shield 2. Safe Technology:** Ensuring the security of technology products and services used by Australians.
- **Shield 3. World-Class Threat-Sharing and Blocking:** Improving information sharing and cyber threat detection capabilities.
- **Shield 4. Protected Critical Infrastructure:** Safeguarding essential infrastructure from cyberattacks.
- **Shield 5. Sovereign Capabilities:** Developing a strong domestic cyber-security industry and expertise.
- **Shield 6. Resilient Region and Global Leadership:** Collaborating with regional and international partners to improve global cyber resilience.

Each 'shield' contains various action points in order to reach the desired goals. The Strategy is supplemented by a 'Plan of Action', to be reviewed every two years. The Strategy provides a good template to be emulated by other countries, including India.

In 2024, the Australian Federal Parliament – the Parliamentary Joint Committee on Intelligence and Security (PJCIS) invited submissions on Cyber Security Legislative Package 2024.[34]ARPI's submission emphasises the urgent need for comprehensive reforms to existing cybersecurity legislation, advocating for a strategic risk policy approach that shifts from outdated risk management practices to a network-centric, vulnerability-focused model. This approach, alongside the adoption of advanced data intelligence and artificial intelligence frameworks, aims to address emerging global threats and enhance resilience in critical infrastructure through more proactive, performance-based regulation.[35]

## 2.4. Key Cybersecurity Components of the Ethical Framework for 6G

Improved cyber security can be ensured through both advanced technologies and effective regulation. However, this is clearly a David-and-Goliath situation, where the former can swiftly outsmart the latter with impunity.

**Security-by-Design**: A paradigm shift in cyber security and privacy protection, in general, is that 6G wireless is projected to be secure by design, which is more than a security enhanced system. The Security-by-Design approach allows seamless integration of security at the heart of the infrastructure, rather than an afterthought, ensuring an intelligent and autonomous end-to-end defence-in-depth security strategy.[36] It should be augmented by a Zero-Trust model with the ability to cope with different situations and unexpected events in extreme conditions.[37]

Apart from incorporating security directly into devices and networks, it is essential to design fail-safe mechanisms and contingency plans for 6G. These plans must address the potential risks from AI, quantum computing, and widespread IoT adoption.[38] Additionally, during the standardisation process, transparency, choice, and control over risks should be provided along with mechanisms for security control, security assurance and privacy preservation.[39] To ensure an end-to-end comprehensive security strategy, these principles should be applied at all levels of the security stack, including the network, devices, applications, and data.[40]

Technologies such as "privacy-preserving federated learning" (ppFL) are being talked about with respect to 6G. ppFL enables collaborative model training without sharing raw data and can thus counter cyber-attacks on neural networks and securely transmit sensitive information like patient data, enhancing privacy through decentralised learning systems.[41] Similarly, quantum computing is expected to significantly improve the security, efficiency, and intelligence of wireless resource optimisation difficulties in 6G communication networks. Quantum communication, particularly through Quantum Key Distribution (QKD), will enhance network security by ensuring secure data

transmission. Quantum algorithms will optimise resource allocation and channel estimation, improving network efficiency. Additionally, quantum machine learning will enable more intelligent, autonomous decision-making in managing network resources, further enhancing network performance and scalability.[42]

Notably, the cybersecurity agencies of the United States, Australia, Canada, New Zealand, the United Kingdom, Germany, the Netherlands, Norway, South Korea, Israel, Japan, Singapore, and the Czech Republic have recently published a document titled "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default."[43] This publication emphasises that it is more crucial than ever for technology manufacturers to prioritise Secure-by-Design and Secure-by-Default principles in their product design and development processes. The joint guide recommends that manufacturers develop a comprehensive roadmap to implement and ensure robust IT security.

Further, the Governments from the United States, Australia, Canada, the Czech Republic, Finland, France, Japan, the Republic of Korea, Sweden, and the United Kingdom have endorsed shared principles for the development of 6G wireless communication systems. These principles emphasise the need for secure, open, and resilient connectivity. They include ensuring 6G technologies contribute to a trusted communications ecosystem that protects national security, prioritising cybersecurity and privacy through security-by-design approaches, and promoting global standards developed via open and transparent processes. Additionally, the principles support international collaboration to foster interoperability and innovation, ensuring a sustainable and inclusive 6G ecosystem.[44]

**Security-by-default:** Security-by-default in the context of 6G signifies the inherent integration of robust security measures as a fundamental and automatic aspect of the 6G network's design and operation. This approach ensures that strong security practices are established from the outset, creating a network environment where security is prioritised as the default setting rather than an optional feature. The goal is to provide enhanced protection against potential threats and vulnerabilities, offering users a secure and trustworthy communication environment without requiring additional configurations or adjustments.

**Artificial Intelligence:** AI will be crucial in designing and optimising 6G networks, making it the first "AI-native" network with integrated AI and machine learning capabilities.[45] These capabilities will handle complexity, enable semantic communication, enhance network security, and support container operations.[46] The potential for comprehensive security in 6G, as an AI-native network, is significant. It aims to integrate AI at its core to implement a defence-in-depth strategy, augmented

by a zero-trust model, ensuring security standards at every level of the network. AI-based security applications, such as differential privacy, protect user data from exposure, while federated learning enables the swift development of global AI-based security models by using distributed data for training. This advancement marks a substantial improvement over current security strategies in existing networks.

**Transparency and Accountability**: The Optus, Medibank and AIIMS cyber-attack have brought to the forefront the importance of accountability and transparency in cyber security. The emergence of 6G technologies will bring new and existing threats, dependent on the design vulnerabilities and efforts to address them.[47] Thus, ensuring trustworthy and accountable 6G systems is important. The processes and methodologies used in the design, development, implementation, and operation of 6G systems should be clear and accessible to relevant stakeholders, including users, regulators, and researchers.[48] It means providing insight into how the technology works, the algorithms used, and the potential risks and vulnerabilities associated with it. Transparent design ensures that the system's intentions and functions are well-understood and can be scrutinised for potential flaws or biases.

If a security breach occurs or unethical practices are identified within the 6G ecosystem, the responsible parties, whether individuals, organisations, or entities, must be held accountable for their actions. This involves identifying and acknowledging any wrongdoing and taking appropriate measures to rectify the situation, compensate affected parties, and prevent similar incidents from happening in the future. Holding stakeholders accountable helps build trust among users and the public while ensuring that Cyber security is taken seriously by all involved parties.

**Legislation:** The legislation needs to be more technology neutral and have stricter application to be effective in combating cybercriminals. The low conviction rate reflects the ineffectiveness of the current cyber laws, and the certainty of punishment is crucial for deterrence. The law must define cyber-attacks and identify information infrastructure, and legacy systems along with measures to replace them. It should also incorporate ways to track cyber-crime, building cyber forensic capacities, and create a platform for continuous sharing and analysis of information between public and private sectors. The focus must also be laid on strengthening human and institutional capacity building through skilling missions, spreading awareness, and organising hackathons. Apart from this, the government should promote the use of cloud infrastructure for its cyberspace, adopt public-private-partnership, and increase the budgetary allocations for cyber security research, development and operations.[49]

# 3 Protection of Privacy

6G is envisioned to achieve ubiquitous connectivity for a billion devices, sensors, and autonomous applications. This advancement lays the groundwork for potential use cases which includes homes, factories, cities, and governments, all of which heavily rely on the exchange of personal data among individuals, organisations, and governmental bodies.[50] However, privacy and data protection presents challenges in 6G spanning various disciplines including technology and regulation. The existing regulations and technological advancements currently have limited effectiveness to meet issues such as hacking, trust, and privacy and security violations. 6G departs from the predominantly device and network-centric framework of its previous generation 5G, towards a more immersive integration with the network infrastructure.[51] This necessitates a more robust approach, as physical safety increasingly hinges upon information technology and the communication networks.

The capabilities of 6G networks will enable a wide array of digital services, including wearable displays, implantable devices, telepresence applications, mixed reality, tactile Internet[52], and autonomous driving.[53] The existing 5G standard overlooks the challenge posed by quantum computing and instead relies on conventional cryptography methods. However, the evolution toward cloud and edge-native infrastructures is anticipated to persist in the architecture of 6G networks. Asymmetric cryptographic algorithms currently in use are expected to require replacement with quantum-safe concepts. Particularly for sensitive data with long-term relevance, this transition needs to be addressed promptly. By taking action now, we can safeguard today's data stored on servers against potential threats posed by future quantum-computer-based algorithms.[54]

Despite the substantial increase in coverage and network heterogeneity, one major challenge arises from the integration of connected devices into various aspects of human life, including implants and cyborg technologies, which raises fears of potential breaches leading to the exposure of sensitive personal information, such as health records.[55] The consequences of security breaches in 6G could be catastrophic, extending beyond financial or reputational damage to encompass potential loss of life, such as fatal accidents resulting from attacks on autonomous driving systems. A significant challenge lies in establishing the threshold at which linked, de-identified datasets cross over into personally identifiable information.[56] This issue carries implications across multiple digital domains, including smart healthcare, industrial automation, and smart transportation.

In the 6G era, the network and its services will continuously generate, store, and process vast amounts of data. Potential digital breaches in 6G pose a threat beyond exposing conventional sensitive information like credit card numbers and confidential business messages. With 6G networks evolving to serve as our digital sixth sense, they will possess capabilities to discern a person's precise location within a room and track and predict their habits. As biosensing technologies integrated into 6G networks emerge, there is a possibility that the network will have access to our most intimate health details. This could include monitoring medical conditions, tracking medication levels, and even alerting individuals to impending health crises such as heart attacks or epileptic seizures. However, the ownership, processing and purposes of such data raise significant risks and concerns.

Judicial bodies worldwide are struggling with privacy infringement cases in the absence of institutionalised metrics delineating the degree of personal information involved, while commercial entities continue to leverage personal data for revenue generation. For data processing, many jurisdictions such as EU's General Data Protection Regulation (GDPR)[57] and India's Digital Personal Data Protection (DPDP) Act[58] have centred consent and anonymity as key safeguards for privacy protection. However, in the context of 6G, these measures may prove insufficient. Even when data is anonymised, it still contains insights into individuals' relationships, habits, and preferences. Further, if these datasets are de-identified or linked, they may have enough personal information to re-identify individuals.[59] Moreover, the smart ecosystem emerging after 5G will entail a shared network infrastructure wherein multiple stakeholders collaborate to offer a range of services to consumers, making it difficult to assess risks and fix accountability.

Existing data protection mandates do not explicitly address the concept of digital twins, which are virtual representations of real-world individuals or objects. However, digital twins may be considered as data subjects themselves, mirroring their physical counterparts. The ambiguity arises when considering the jurisdictional scope of laws governing virtual reality spaces.[60] If no clear jurisdictional framework is established, the determination of applicable laws may fall into the hands of the private sector, particularly large technology corporations with substantial data and regulatory influence. These entities could shape the operational landscape of virtual reality. The absence of a definitive answer to this jurisdictional question poses a risk to privacy and may negatively impact the realisation of potential social and economic benefits associated with 6G technology.

As 6G advances into the terahertz spectrum, enjoying increased bandwidth, densification, and cloudification, it aims to create a hyper-connected world where

billions of devices and nodes seamlessly integrate with terrestrial, oceanic, and space-based communication networks. The proliferation of billions of devices, sensors, and millions of subnetworks, often situated in untrusted domains, will significantly amplify the threat of malicious attacks. To meet future demands, several aspects of 6G will further exacerbate the risk across multiple dimensions. These include the adoption of open interfaces and architectural disaggregation, the integration of open-source and multivendor software, and the involvement of multi-stakeholder supply chains. While security algorithms will harness machine learning techniques to detect attacks and respond optimally, attackers will also instrumentalise machine learning to gain intimate insights into network operations and develop more sophisticated attack strategies.[61]

Advanced privacy technologies will play a crucial role in effectively deploying 6G networks. Safeguarding individual privacy and identity has posed a persistent challenge for standardisation bodies, as different nations have divergent perspectives and regulations. International standards bodies like JTC 1 have established committees dedicated to developing privacy frameworks, although substantial work remains unfinished.[62] One approach to addressing this challenge is to adopt the European Commission's framework of "Privacy by Design."[63] This framework emphasises integrating privacy considerations into the design and development of technologies from the outset. The European Commission has underscored the importance of the security industry in enhancing privacy protection and complying with data protection regulations, recognising the shared responsibility between customers and providers.

Given the interconnectedness of global markets, 'Privacy by Design' is likely to become increasingly central in future communication techniques. It emphasises not only legal compliance but also societal and ethical responsibilities, impacting both technical specifications and the implementation of applications and operating systems.[64] These include secure multi-party computation, which allows data analysis without revealing internal data, distributed storage and processing at edge and central data centres, and federated learning approaches. Additionally, techniques will need to be developed to transform raw data into synthetic data that retains necessary analytical characteristics while safeguarding irrelevant or private information. These technologies will be underpinned by mechanisms that verify data integrity and ownership. Blockchain technology will continue to support distributed data brokerage by securely tracking data access rights.

# 4 Potential Competition Concerns in 6G

The telecom sector continues to be at the epicentre of development, innovation, and disruption.[65] Network effect is one of the most prominent characteristics of the telecom sector, which can result in significant economies of scale or scope.[66] Traditionally, in most countries the telecom sector operated under monopoly conditions either through the control of state institutions or to a limited extent, through private entities. National statutory regulatory agencies formulated rules governing tariffs, service quality and universal service.

This model worked well in developed countries but did not function as effectively in developing countries where networks were often limited to urban regions and more accessible to consumers with a middle or high income. However, with the advancement of telecommunications technology, the natural monopoly began to fade and a more competitive landscape evolved in the industry. Accordingly, in recent times, the telecom sector has largely shed its natural monopoly characteristics and has evolved into a highly competitive market with participation from private players. This marks a shift in the institutional and regulatory framework of the telecom industry.[67]

Potential competition concerns in the 6G ecosystem can be those specific to the telecom sector as well as those related to its interface with associated new technologies like artificial intelligence (AI) and cloud computing, which forms an integral part of 6G networks as per its emerging vision. It is believed that telecom and digital technologies will be closely fused together in 6G, which may give rise to newer competition concerns. It would be, therefore, important to take cognisance of such concerns and think about solutions beforehand.

In the Indian context, the Competition Commission of India (CCI) enforces the provisions of the Competition Act, 2002 and the rules framed thereunder. The regime is to prevent practices that cause an appreciable adverse effect on competition. Similarly, in Australia, the Australian Competition and Consumer Commission (ACCC) regulates competition matters as per its mandate under the Competition and Consumer Act, 2010.

## 4.1. Competition Issues in Telecom Sector

### 4.1.1. Overlap between Competition Authority and Sectoral Regulator

In Australia, the ACCC reports on competition issues in the telecom industry by collecting information to monitor competition, track market developments, and inform regulatory decisions. It publishes reports and uses the collected information for this purpose. The ACCC is required to report annually on competition in the Australian telecom sector and price changes for telecom services in Australia.[68]

In India, the CCI undertook a market study on the telecom sector in India and presented its key findings and observations in a report in January 2021.[69] The CCI concluded that the telecom industry has evolved into a complex data-centric converged service and that going forward, formal and informal lines of communication between various sectoral regulators/government departments such as the Department of Telecommunications (DoT), the Telecom Regulatory Authority of India (TRAI) and the CCI is crucial to ensure that regulatory decisions are robust and consistent. This is particularly relevant because there has always been an inherent jurisdictional tussle between the CCI and sectoral regulators such as the TRAI with regard to the issues that simultaneously fall within the remit of both bodies and the Supreme Court has attempted to resolve this tension.[70]

The question came to the forefront in the matter when Reliance Jio filed a complaint against Airtel, Vodafone and Idea before the CCI contending that these telecom operators had formed a cartel and were indulging in anti-competitive practices by failing to provide adequate points of interconnection. The CCI ordered an investigation into these allegations. Meanwhile, Reliance Jio had also filed letters with the TRAI complaining about similar conduct as well as the denial of mobile number portability. Considering the writ petitions filed against the CCI's investigation into the matter, the High Court of Bombay held that the CCI had no jurisdiction on such matters as the same was in the regulatory domain of the TRAI. The Bombay High Court held that disputes regarding contract clauses, quality of service regulations and interconnection agreements in the telecom sector are to be settled by the TRAI and not the CCI.

On appeal, the Supreme Court upheld this decision and resolved the highly debated issue by deferring to the expertise of the TRAI, which was better suited to resolve the dispute by virtue of being the telecom sector specific authority. The Supreme Court reasoned that if the CCI were allowed to investigate matters that are already being decided by the TRAI, it may lead to conflicting views being given by two regulatory bodies.

### 4.1.2. Abuse of Dominance

A business operating in a dominant position may impose unfair or discriminatory practices to limit or restrict the production of goods or services. Competition that is conducted unfairly or in an unethical manner is undesirable and could amount to abusing the enterprise's dominant position. Related to this is the issue of predatory pricing by giving free services for six months and then charging very low prices in order to capture market share and attract more customers. In India, predatory pricing is dealt with as an abuse of dominance.

In its decision in *Bharti Airtel v. Reliance Jio*,[71] the CCI examined the allegations in the matter in the context of the relevant market of wireless telecom service and noted that according to the available market data, Reliance Jio did not have a market share of more than 7% in each of the telecom circles in India, and the market consisted of several other telecom service providers (such as Vodafone, Idea, Tata, MTNL and others) who have similar financial and technical capabilities. The CCI concluded that Reliance Jio was not in a dominant position in the relevant market, hence no question of its abuse. Thus, it was exempted from predatory pricing simply because it was a new player in the telecom industry. Notably, Jio is the leading market player at present.

### 4.1.3. Cartelisation

Preventing cartel-like behaviour in which rivals collude to fix prices, or to restrict or co-ordinate the supply of services is among the core obligations of competition authorities. It is illegal for businesses to agree to act together in a cartel instead of competing in a dynamic business environment. Cartels cheat consumers by restricting healthy economic growth, driving up prices and reducing innovation and investment. Cartels attempt to increase members' profits while maintaining the illusion of competition.[72]

Cartels includes agreements between competitors with respect to fixing prices, limiting production, market allocation or bid rigging. Such agreements are presumed to cause an appreciable adverse effect on competition, so competition authorities do not necessarily go into a detailed analysis of defining the relevant market as in the case of abuse of dominant position. However, there is no presumption as to the existence of an agreement and this needs to be established with precise and coherent proof by the party alleging the infringement.[73] There have not been any major cartel decisions in the Indian telecom space.

Interestingly, during the COVID-19 pandemic, ACCC relaxed its normal industry controls on the telecom industry, thereby allowing normally prohibited collusion between competitors to deal with unforeseen and unprecedented demands on

telecommunications networks.[74] ACCC allowed NBN Co and certain retail service providers (Telstra, Optus, Vodafone Hutchison, TPG and Vocus) to work together to ensure services during this time when there was a surge in home working, home schooling and video streaming which were placing unprecedented pressure on the national broadband infrastructure. As a result, the providers worked together on measures to facilitate the supply of voice or data services, providing access to certain groups and the sharing of information/resources.

### 4.1.4. M&As in the Telecom Sector

Mergers and acquisitions (M&As) in the telecom industry have now become the norm towards achieving higher efficiencies as well as better collaboration between providers. The Indian telecom sector has witnessed intense change over the last decade most significantly with the arrival of Reliance Jio in the telecom market in 2016 and the Vodafone-Idea merger in 2018, which has shaken the competitive landscape. Other notable M&A transactions in the past that shaped the Indian telecom industry include the Vodafone-Hutch merger in 2007, the Reliance-Infotel merger in 2010, Reliance-Aircel (which was later called off in 2017 due to delays in obtaining regulatory approvals), Airtel-Telenor in 2018, etc.[75]

In Australia, the Telstra-TPG Telecom transaction has been receiving extensive coverage since it failed to receive approval from ACCC when the parties applied for a merger authorization. Telstra Corporation Limited and TPG Telecom Limited proposed spectrum sharing by entering into interrelated agreements to facilitate mobile infrastructure and spectrum sharing in certain regional and urban fringe areas of Australia under a multi-operator core network commercial arrangement. However, ACCC denied approval for the proposed transaction in December 2022 and the Australian Competition Tribunal affirmed ACCC's determination on 21 June 2023, dismissing the application for merger authorization.[76] Had the transaction been approved, Telestra would have purchased TPG's spectrum and transmission towers while TPG would have kept selling 4G and 5G coverage using Telstra's infrastructure.

In 2019, the ACCC also opposed the merger of TPG Telecom and Vodafone-Hutchison because of potential competition issues, even though the parties did not compete in the same markets and neither party was considered a market leader.[77] However, the Australian federal court rejected ACCC's findings and allowed for the merger to go ahead by concluding that it would not substantially lessen competition.[78]

## 4.2. Standard Essential Patents (SEPs) and FRAND Terms

### 4.2.1. Concept of SEP & Competition Law Considerations

A patent covering any part of the technology used in a standard is a 'standard essential patent' (SEP).[79] A patent is deemed 'essential' if an independent evaluator concludes that the patent is essential to the practice of a technical standard. SEPs protect technologies that are essential in complying with a 'standard' i.e., it provides a set of rules, guidelines or characteristics for material, products, processes and services to interoperate.[80]

When it comes to SEPs, competition authorities who otherwise may be hesitant to interfere with IPR-protected technology, may feel more compelled to intervene. Ordinarily, the grant of exclusive rights is recognized as an essential factor for fostering innovation. Since innovation is a contributor to competitiveness, it is often argued that, but for IPR protection, enterprises would lose the incentive to innovate, a process that entails significant investments with no certainty of recoupment. In recognition of this, for example, the (Indian) Competition Act, 2002 grants a limited carve out for restrictions necessary to protect a legitimately accorded IPR, incorporated in agreements, without casting a 'duty to deal'.[81]

However, the rules change when it comes to SEPs, which cannot be exploited like any other patent. Once a standard is selected, competitors and downstream market participants typically invest heavily to ensure that their production processes and devices comply with the relevant standard. The adoption of a standard usually requires the use of patented technology that is compatible with the standard, resulting in industry stakeholders being locked in. This means that certain patents are essential for compliance with the relevant standard, and vest SEP holders with market power. An outright failure to license to a competitor could result in the SEP holder being liable for abuse of dominant position by denying market access or using its dominant position in one market to protect another. Alternatively, asserting an excessively high royalty rate for use of a SEP could result in the SEP holder being liable for abuse of the dominant position by imposing an unfair or discriminatory price.

### 4.2.2. Adoption of FRAND Terms and its Benefits

In order to avoid licensing problems and to ensure access to SEPs for the wide adoption of standards, standard setting organisations (SSOs) created the concept of 'FRAND', following a requirement for licensing SEPs on fair terms to SSO members and non-members who use the standard.[82] FRAND refers to fair, reasonable, and non-discriminatory licensing terms and aims at creating the right balance between the interests of technology users and providers.

There may be several advantages to adopting an industry standard, such as enabling products and services offered by different vendors to interoperate. However, where adopting a standard involves the incorporation of a patent, it is important to ensure that the patent holder does not unjustly exploit its market power. This may be prevented by securing FRAND commitments, where owners of SEPs commit to make them available to third parties on FRAND terms.[83]

Adoption of FRAND terms appears to be a mutually beneficial solution.[84] FRAND licenses are primarily intended to prevent patent hold-up.[85] Similarly, patent owners benefit from their SEPs being widely used and remaining stakeholders ensure they are able to license the relevant SEPs and are protected from paying exorbitant royalty rates. However, the efficacy of FRAND terms is determined by their enforceability. FRAND value is meant to be reasonable and make the business of the implementer sustainable. It also compensates the technology provider for investing in R&D activities and inventing new technological developments.[86]

FRAND licensing obligations are yet to be considered in the Australian courts.[87] If a patentee contravenes Part IV of the Competition and Consumer Act, 2010 in Australia, a person may seek a compulsory licence to licence the patent under the Patents Act. The licence fee of a compulsory SEP licence must not be excessive and the applicant will be required to pay a fee determined by the court as just and reasonable.[88]

### 4.2.3. Recent Developments with regard to SEP-FRAND Obligations in India

India has witnessed several lawsuits on infringement of SEPs that coincided with the rise in local mobile device manufacturers. Cases pertaining to SEPs and FRAND commitments have also been filed before the Competition Commission of India (CCI). These cases pertain to well established technology companies that granted SEPs for their innovations in the telecommunications sector.[89]

One of the first cases in India relating to SEPs was the case where Ericsson sued Micromax for infringement of its SEPs used in mobile phone technologies. Ericsson also filed similar cases claiming infringement of its SEPs against Intex Technologies and Xiaomi Technology.[90] The Delhi High Court granted an *ex parte* injunction in favour of Ericsson and after subsequent appeals to the division bench, entered into an interim agreement where Micromax agreed to pay royalties at the rate demanded by Ericsson. However, Micromax filed information before the CCI alleging that Ericsson had abused its dominant position by demanding an exorbitant and arbitrary royalty rate. CCI ordered an investigation into the matter after concluding that Ericsson held a dominant position in the market for devices in which SEPs were essential for implementing the standard. When Ericsson challenged the CCI's order, the Delhi High Court passed an order in March 2016 recognizing the CCI's jurisdiction.

In addition to Ericsson, patent holders Vringo and Dolby filed suits against infringement of their SEPs by local manufacturers such as Micromax, Intex and iBall. They also filed suits against Chinese mobile device manufacturers Xiaomi and OPPO. All these suits were filed in the High Court of Delhi which is the most preferred forum in India for patent matters. The mobile device manufacturers were immediately restrained from manufacturing and selling the products that were alleged to be infringing the SEPs. But a few months later, the implementers were allowed to sell their products during the pendency of the suits on the condition of payment of royalties to the SEP holders based on an interim arrangement determined by the court.[91]

In July 2018, in two joined (identical) disputes involving importers and assemblers of DVD players in India,[92] the Delhi High Court held that the patent was essential for the DVD standard and accepted the US and EU patents' essentiality certificates. However, the court found an infringement since the defendants failed to prove that the components were imported from Philips' authorised licensees. The court also held that their failure to obtain a licence from Philips to use its SEP *prima facie* led to the finding of infringement because the defendants' products complied with the standard. Since the defendants were not able to prove that the fee charged by Philips was not on FRAND terms, the court fixed the royalty charges as proposed by Philips.[93]

The Delhi High Court's decision in May 2021 in *InterDigital v. Xiaomi*[94] can also be cited concerning the issue of SEPs. US tech company InterDigital filed suit against the Chinese consumer electronics maker Xiaomi, claiming infringement of its 3G and 4G patents due to the use of its technology by Xiaomi without any prior authorization or consent. InterDigital sought a remedy in the form of either a permanent injunction or royalties. Since InterDigital had previously issued licences of its SEPs to third parties, it invited Xiaomi to do the same, but the offered rate was rejected by Xiaomi as not complying with FRAND terms. InterDigital did not grant any access to comparable licence agreements to preserve its confidential commercial information. Subsequently, on 3 June 2020, Xiaomi filed a complaint against InterDigital in Wuhan Intermediate People's Court, China for determining royalty rates that comply with FRAND terms payable for InterDigital's 3G and 4G SEPs.

In retaliation, InterDigital filed a suit against Xiaomi in the Delhi High Court in part to garner leverage regarding the situation before the Wuhan Court. On 23 September 2020, the Wuhan Court issued an anti-suit injunction against InterDigital from pursuing matters in the Delhi High Court. In a 'tit-for-tat' response, on 29 September 2020, InterDigital filed an anti-anti-suit injunction application at the Delhi High Court. On 3 May 2021, the Delhi High Court ruled that barring certain exceptions that apply only

when the foreign forum is vexatious or oppressive, the court of one state cannot bar parties from pursuing the dispute at a forum in another state.

In a most recent judgment[95] (July 2023), the Delhi High Court, overturned its earlier judgements (of 2016 and 2020) related to the jurisdiction of CCI on matters related to patents. As per this latest order the CCI will, in general, not have jurisdiction to deal with the matters related with patents (including SEPs) and its licensing matters under the Competition Act provisions related to 'anti-competitive agreements' or 'abuse of dominance'. The Court felt that the Patents Act, as a specialised legislation, has provisions to deal with such cases, and hence the patent authority will have jurisdiction over such matters. Unless the Supreme Court overturns this judgement, this is the law at present.

More so, there are no formal SEP policies or guidelines in India, apart from these court decisions. Interestingly, China has been using SEP policy to make significant progress in telecom equipment manufacturing, among other things.

### 4.2.4. China's Antimonopoly Guidelines on SEPs

In November 2024, China's State Administration for Market Regulation (SAMR) issued "Antimonopoly Guidelines on Standard Essential Patents (SEP), 2024".[96] The Guidelines have defined SEP-related concepts, put forth analysis principles for antitrust behaviours and established a set of supervision rules, among others.[97] SAMR expects that the guidelines will help promote fair market competition and protect the driving forces of industrial innovation and development.

As per the Guidelines, the following analysis principles will be considered by SAMR in the determination of abuse of SEPs to exclude or restrict competition:[98]

- The same analytical approach as that for the abuse of IPRs to exclude or restrict competition;
- Both the protection of IPRs and the maintenance of fair competition in the market will be taken into account;
- Balancing of the interests of SEP owners and standard implementers;
- Fully considering the information disclosure, licensing commitments and licensing negotiations related to SEPs the process of standard formulation and implementation.

### 4.2.5. SEP and FRAND Terms in the European Union and the United States

In July 2015, the European Court of Justice (ECJ) issued its decision in *Huawei Technologies v. ZTE Corp.*,[99] a seminal case detailing how holders must licence SEPs on FRAND terms. The case concerned the potential for enforcement action by holders of

SEPs to infringe EU competition rules against abuse of a dominant position. The judgement resolved the divergence between the approach taken by some national courts in Europe to applications for injunctions against the use of SEPs when licensing terms were not agreed between the parties. On 29 November 2017, the European Commission (EC) published its long-awaited guidance on litigating and licensing SEPs based on a clear, balanced and reasonable policy for SEPs in the EU.[100]

More recently, on 27 April 2023, the EC proposed a new framework for SEPs, including an impact assessment and its executive summary as well as a proposal for a regulation.[101] The SEP reform aims for a balanced framework, setting a global standard for SEP transparency. The EU stands in sharp contrast to the US, where the Federal Trade Commission and the Antitrust Division of the US Department of Justice declined, in January 2017, to adopt as part of their guidelines any views on anti-competitive behaviour in the specific context of SEP licensing and enforcement. In the US, FRAND breaches are litigated before courts that are typically well versed with the economic and legal underpinnings of both intellectual property and antitrust laws.[102]

## 4.3. Pro-Competition Technologies

Although scholars and policymakers continue to debate the finer details of the application of competition law and policy in digital markets, there is a growing consensus that more work needs to be done and that this must transcend the conventional modes of competition enforcement.[103] Technological interventions can also contribute in dealing with competition concerns, particularly those promoting interoperability and portability. Telecom technologies that facilitates network interoperability, or adopting Open RAN can be pro-competition.

### 4.3.1. Network interoperability

Network interoperability refers to the functional interworking of telecom services across multi-vendor, multi-carrier interconnections according to applicable standards and required specifications.[104] Interoperability is a foundational principle of the internet - it makes the internet what it is.[105] Telephone, telegraph and radio communications all rely on interoperable protocols such that one person using a network in a certain place can reliably place a call to someone in another place. Network interoperability becomes indispensable to achieve end-to-end connectivity. The more diverse networks exist, the greater the need to ensure that they can interoperate in order to make end-to-end communication possible.

Network interoperability is important because it can free customers from vendor lock-ins. Replacing proprietary hardware with open source software allows companies to collaborate, differentiate themselves and deliver new services. Consequently, major

telecom operators have embraced interoperability and openness in order to create a more malleable communications network.[106] Network interoperability can be achieved in two ways – either by having the two networks conform to a common protocol standard, or by defining a standard interface to which all networks need to adhere, or by providing a gateway that translates between the two protocols.[107]

- The benefits of interoperability extend to all elements of the value chain. The user benefits as he can communicate with whoever he wants to with a single terminal. The telecom operator benefits as it can select the best equipment available from different manufacturers based on quality performance and prices. The product manufacturer benefits as it can extend the same equipment set to multiple operators.

Network interoperability, however, is considered a challenging affair because from a cost perspective, designing the network architecture for interoperability implies the willingness to accept associated liabilities. Telecom operators are sensitive to five major liabilities:

- Increased cost of acquisition associated with the addition of interoperable network/application modes.
- Added cost and complexity of adding features to achieve all network compatibility.
- Increased time for acquiring a new system i.e., time to accept interoperability features and perform proper testing required to certify interoperability.
- Increased complexity and cost associated with the management of the configuration of interfaces.
- Increased power and decreased speed to accommodate modes providing backward compatibility.

### 4.3.2. Open RAN

Open radio access network (Open RAN) is a new form of technology which helps mobile carriers open up their networks and share spectrum resources. The concept is based on interoperability and standardisation of RAN elements. Traditionally, base stations necessary for the deployment of mobile communication systems were designed by vendors using proprietary technologies and were provided as a single solution. This meant that if a telecom operator adopted a certain vendor's base station to build a network, it would be forced to continue building its network in that same vendor's base station from then on, resulting in a vendor lock-in. Open sharing however can help reduce the costs of deploying 5G and 6G infrastructure and this in turn creates more efficient spectrum use for all telecom operators.

However, like any other open digital systems, often security concerns are pitched with respect to Open RAN. According to the "Open RAN Security Report" dated 22 May 2023 prepared by the Ministry of Internal Affairs and Communications of Japan in cooperation with the governments of the Quad group, Open RAN technology does not fundamentally alter the security risk landscape for telecommunications compared to more traditional RAN.[108] Only a total of 4% of the analysed security threats are considered unique to Open RAN. Mitigation measures make it feasible to ensure equivalent levels of security between traditional and Open RAN deployments.[109]

The report was developed in the Quad Critical and Emerging Technology Working Group, which was created in 2021 as part of the initial Quad summit among the leaders of Australia, India, Japan and the US. The report demonstrates that:[110]

- Open RAN offers important cybersecurity advantages,
- Risks sometimes attributed to open RAN are common to traditional RAN deployments, and
- These risks can be mitigated and managed through the recommendations presented in the report.

## 4.4. Competition Issues in the Cloud Services Market

Since, cloud services is going to play an integral role in development and deployment of 6G, any competition concerns in this market can adversely affect the 6G ecosystem. Cloud services refer to a model of providing remote access to a multitude of computing resources on demand to customers. The third-party providers make contracts with subscribers for these services, allowing customers to leverage powerful computing resources without having to purchase or maintain hardware and software. The cloud eliminates the need for individuals and businesses to self-manage physical resources themselves, and as a result, only pay for what they use. Convenience and cost-effectiveness have been the driving force in the growth of cloud services market.

### 4.4.1. Models of Cloud Services and Cloud Deployment

Cloud service and deployment models are particularly important considerations when competition authorities have to define markets and determine issues of switching and interoperability of networks by customers. Cloud service models are differentiated by the level of control the customer has over the management and maintenance of the computing resources.[111] In each case, service providers maintain the underlying cloud infrastructure and computing resources are handled by the provider as required by the subscriber's needs. Typical service models are: (a) Software-as-a-service (SaaS), (b) Platform-as-a-service (PaaS) and (c) Infrastructure-as-a-service (IaaS).

Also cloud based deployment comprises private cloud, public cloud, community cloud and hybrid cloud. Multi-cloud is a cloud deployment model that involves using services from more than one public cloud provider by a single customer at the same time. The use of multiple public cloud providers can benefit customers by allowing them access to their preferred services and gain commercial bargaining power against their cloud providers. It also gives customers the flexibility to operate with the best computing environment for each workload, even if these are from different cloud providers.

### 4.4.2. Competition Concerns in Cloud Services

The level of flexibility is facilitated through interoperability or the ability for different systems to interact and work together. Openness and interoperability empower faster innovation, tighter security, and give freedom from vendor lock-in.[112]

While customers are highly aware of the vast range of benefits that cloud technology offers, problems such as high egress fees, lack of interoperability and vendor lock-ins create a set of insurmountable challenges for new players. Customers are hence forced to choose the easy option of using one cloud, resulting in cloud concentration and this in turn raises potential competition concerns. The key market practices which competition authorities have expressed concerns pertain to the issues of licensing, egress fees, imposing technical restrictions on interoperability and offering discounts.[113]

- Licensing restrictions prevent customers from choosing any other cloud provider at the time of migration into the cloud and ultimately locks those customers into its ecosystem.
- Egress fees consist of the charges that customers pay to transfer their data out of a cloud. If dominant players set these at significantly higher rates than other smaller providers, the costs of egress fees can actively discourage customers from using services from more than one cloud provider or switch to an alternative provider.
- Technical restrictions on interoperability are imposed by certain providers to prevent some of their services from working effectively with services from other providers. Interoperability restrictions are typically viewed as anti-competitive tying arrangements.
- Discounts can usually be beneficial to customers by reducing their costs. However, the manner in which discounts are structured can incentivize a customer to use a single cloud service provider for most of their cloud needs, even when better quality alternatives are available. Such forms of incentivizing could raise concerns of potential abuse of dominant position when certain players have a high market share and thereby retain control of the market.

### 4.4.3. Global Competitive Landscape and Ongoing Investigations by Competition Authorities

In today's times, migration to cloud computing is viewed as highly desirable and companies are at different stages of adoption, with analysts predicting that 45% of businesses' IT spending will be on public cloud services by 2026.[114] Amazon Web Services (AWS), Microsoft Azure and Google Cloud are the largest players in the market worldwide for the provision of cloud services.[115] The 'big3' are followed by smaller platforms such as Alibaba Cloud, IBM Cloud, Salesforce, Oracle and Tencent Cloud.[116]

A study[117] by Prof. Frédéric Jenny on unfair licensing practices in the cloud computing industry has found that the cloud computing market exhibits increasing concentration with a limited number of players consolidating their market shares to the detriment of smaller providers.[118] The research indicates that these software providers often bundle the use of their dominant software systems with their cloud infrastructure, making it difficult for customers to switch to independent cloud providers even if they would like to. This also amounts to imposing switching costs on firms if they wish to move to an independent cloud service provider.[119]

In addition, other restrictive software practices found in the study include making it more expensive for firms to transfer data or storage to an independent cloud provider, limiting their software's interoperability on other providers, and giving software discounts to firms who use their cloud infrastructure. Collectively, such practices unfairly reduce competition, raise costs, limit consumer choice and impose difficulties on independent providers to access the market. According to data presented in the research, independent providers have gone from holding nearly 50% of the cloud infrastructure market share in 2015 to only 18% of the market in 2022.[120]

Globally, various competition agencies have initiated market studies and begun investigations to better understand the business landscape of the cloud services market. There is also extensive international collaboration between authorities which are simultaneously involved in conducting surveys to exchange information and swiftly tackle any potential anti-competitive practices in their respective geographic markets.

- *United States*

In March 2023, the Federal Trade Commission (FTC) put out a request for information (RFI) on the business practices of cloud computing providers.[121] The FTC intends to investigate the competitive dynamics of cloud computing, how reliant certain segments of the economy are on cloud services, and the security risks associated with the industry's business practices. From the information received, the FTC learned[122] that there exist competition concerns with respect to software licensing, egress fees

and minimum spend contracts. Fingers have also been raised on the resiliency and security of cloud services, due to lack of competition. Further, due to the close relationship between generative AI and cloud computing could lead to vendor lock-in.

- *UK*

Ofcom, the UK communications regulator, initiated a similar market research study on cloud services. In its summary of findings, Ofcom in March 2023,[123] noted that Microsoft is a leading player in the cloud services industry, and that customers fear lock-in and inability to switch to other providers.[124] The report highlighted similar concerns regarding AWS and noted that collectively, Microsoft and AWS, raised 'significant concerns' that they were harming competition in online cloud services and abusing their market position with practices that make interoperability difficult.[125] Accordingly, in October 2023, Ofcom referred the public cloud infrastructure services market to the UK Competition and Markets Authority (CMA) for further investigation.

- *European Commission*

In its press release dated 27 July 2023, the European Commission (EC) has opened a formal investigation into possible anti-competitive practices by Microsoft regarding tying/bundling Teams, its cloud-based communication and collaboration tool within its cloud-based productivity suits for business customers (including Office 365 and Microsoft 365).[126] This case has the potential to open up issues of abuse of dominant position along with anti-competitive tying and bundling to prevent suppliers of other communication tools from competition in the market. It seems EC is geared to launch a formal complaint based on its inquiry on this matter in coming months.[127] In addition, EC is actively investigating possible cartel activities within the cloud computing market.[128]

Close on heels, German software company Nextcloud had filed a complaint with the EC alleging Microsoft is illegally bundling its OneDrive cloud storage offering with its Windows operating system.[129] Similarly, French cloud provider OVHcloud also filed a complaint against Microsoft with the EC, alleging that Microsoft has abused its dominant position in the cloud services market through its licensing practices by making it more expensive to run its software in rival cloud platforms as well as creating technical difficulties to run such programs. It is reported that the parties are now preparing to settle the complaint.[130] Nevertheless, the competition law developments in this space are fast-paced and likely to soon offer some significant insight into improving the current market practices adopted by cloud service providers.

- *Other Competition Agencies*

*France*: Given the international trend, the French competition authority, Autorité de la concurrence, opened a public inquiry in January 2022 and sought public consultation in July 2022 into the competitive functioning of the cloud sector. While noting that there was a tendency towards concentration around certain powerful stakeholders, the Autorité also looked into practices in the cloud sector that could restrict competition. Accordingly, in May 2023 it issued an opinion on certain provisions of the draft law to secure and regulate the digital space.[131]

*Netherlands*: In September 2022, the Netherlands Authority for Consumers and Markets (ACM) published a market study highlighting the difficulties users face in switching cloud providers and combining services offered by different providers.[132] In this study, the ACM investigated the structure of the cloud market and the behaviour of market players. Based on its findings the ACM proposed changes to the EU Data Act to make interoperability easier.[133]

*Korea*: In December 2022, the Korean Fair Trade Commission (KFTC) concluded its survey on major cloud service providers and announced its key findings.[134] KFTC found the cloud services market to be fairly concentrated. It identified that cloud customers face difficulties in switching service providers or adopting multi-homing due to a lack of interoperability when switching cloud services or implementing multi-cloud. It also found other restrictions such as cost and time required for migrating data. Based on these findings, the survey suggested that a closer examination of cloud service providers' transaction practices may be required to confirm whether cloud service providers engage in anti-competitive practices such as self-preferential treatment or setting disadvantageous transaction terms on customers.

*Japan*: The Japan Fair Trade Commission (JFTC) conducted a similar fact-finding survey regarding trade practices in the cloud service sector and concluded that the 'big 3' were expanding their market shares significantly.[135] It noted that there is a trend that most users do not change from the cloud services they are currently using and that the degree of market concentration is likely to continue to increase with indirect network effects and preferential use of services provided by the current providers.[136]

## 4.5. Artificial Intelligence and Competition

Artificial intelligence (AI) is changing the way companies compete in a wide variety of industries, and is being envisaged to be an integral part of the 6G networks. New digital technologies and the increased use of AI affect the way companies make choices and take decisions.[137] AI could contribute to a more innovative, efficient, sustainable, and

competitive economy, as well as a wide array of societal benefits.[138] AI also has the potential to disrupt the market and the ability to subvert the fundamental balance between competition law and its enforcement.[139] As a result, competition enforcement agencies around the world are studying the potential impact of AI on market competition.

Defining a benchmark for illegality requires determining whether any illegal action was anticipated or planned (through AI programming or instructions) or whether a particular outcome could have reasonably been foreseen, even when there has been no 'agreement' in person.[140] Some enforcement agencies (e.g., the European Commission) have stated that AI remains under a firm's direction and control and so, the firm is liable for the actions taken by the algorithm – even if not fully understood by the individuals who developed or used it.[141] This is in line with decisions of antitrust agencies which have prosecuted and sanctioned even mere facilitators of illegal conduct as if they took part in the illegal conduct itself.

### 4.5.1. Procompetitive Effects of AI

Even though AI technology is still under intense development, it has fundamentally reshaped the way companies make decisions, especially in terms of predictive analytics, automation, and optimization of the decision-making process. Pricing decisions are made faster, products are more easily tailored to individual consumer needs, and marketing activities are better targeted – all of which have a positive impact on labour productivity, costs, and investments, among other things.[142] AI applications may enable faster detection and response to changes in consumer preferences, making markets responsive to the evolution of demand. In addition to providing new tools for consumers to make decisions, AI applications also use the ever-increasing amount of data available about products and consumers in order to develop personalised products and transactions that better-fit individuals and businesses need. Competition policy has an important role to play in ensuring that AI reaches its procompetitive potential.[143]

### 4.5.2. Potential Anti-Competitive Effects of AI

While AI may aid innovation efforts and create superior product/service offerings for customers, competition enforcement will seek to ensure that barriers to entry are not erected so that the development of new AI systems is not hindered. Also, the use of AI could create a new space for collusive pricing or abuse of dominant position.[144] Similarly, price transparency could facilitate consumer decision-making, but it may also lead firms to compete less aggressively by facilitating coordination. Several e-commerce stores use software that allows automatic adjustment of prices to match those offered by competitors, based on huge volumes of data. Using AI algorithms in

such a process can lead to a reduction in competitive pressure and possibly, even collusion. Potential competition concerns in the active involvement of AI technologies in businesses include the issues set out below.

*Information Exchange:* There is an inherent tension between cooperation and the goals of competition law, which at its core, is meant to protect the very processes of rivalry between companies. AI governance is concerned that without cooperation between AI companies, the development of AI would be less safe and beneficial. However, competition law could be a barrier to this because it seeks to promote competition and prevent cooperation that harms consumers. Strategies that seek cooperation rather than competition between companies can therefore raise anti-competitive concerns. Nevertheless, if structured carefully, these cooperation strategies should not raise competition concerns, or achieve their objectives of cooperation and risk reduction.

*Collusion*: Collusion is not limited to agreements on prices. It can include the allocation of different segments of a market among competitors, agreements regarding product quality or total output, and even harmonising the terms and conditions to be offered to consumers.[145] On several occasions, regulators have established that pricing collusion, facilitated through algorithms, can be caught under competition law.[146] Collusion not facilitated by AI, but rather, implemented by AI presents a more complex puzzle for regulators. AI-driven conduct may sit on the blurred lines between tacit and express collusion.

A distinction would need to be drawn between genuinely independent AI conduct, by two separate AI systems employed by different firms that result in parallel market behaviour, and parallel market behaviour that results from some form of communication or signalling between those two separate AI systems.[147] Where parallel behaviour is the result of some form of communication or signalling between separate AI systems, the law prohibiting anti-competitive agreements would apply. In the absence of any anti-competitive agreement or concerted practice with knowing cooperation, AI systems would, generally, not meet the current legal framework to be prohibited. When only parallel pricing patterns are visible to the authority, identifying and proving the existence of an infringement of competition law will be a significant enforcement challenge.

*Abuse of Dominant Position:* AI could be utilised by dominant firms to implement anti-competitive strategies. For example, AI can be deployed to implement predatory pricing strategies with AI being used to quickly analyse pricing data and determine a competitor's response to changes in the market. Dominant firms may also use AI integrated into consumer-facing products to exclude competitors and nudge

customers in a certain direction (for instance, towards their own offerings without consumers' knowledge). Another issue that could arise is that absent some form of monitoring, an abuse may occur without any harm being actually intended. Accordingly, dominant firms employing AI would require closer oversight over how AI tools are being used as well as the consequences of their actions on the market.

### 4.5.3. Market Inquiries

Recent initiatives have been taken by some competition authorities, including the UK Competition and Markets Authority (CMA) and the US Federal Trade Commission (FTC), focusing on understanding the interplay between AI and competition law. On 4 May 2023, the CMA launched a review of AI models to establish guiding principles for their future utilisation.[148] Similarly, in a blog post on 29 June 2023, the FTC highlighted the competition issues associated with generative AI and subsequently opened an investigation in this space under consumer protection laws.[149]

A "Joint Statement on Competition in Generative AI Foundation Models and AI Products," by the European Commission, UK-CMA, US-FTC and US Department of Justice was released in July 2024.[150] Recognising the great potential benefits of AI, the Statement highlights some of the risks to competition.

First is the concentrated control of key inputs, such as specialised chips, substantial computing, data at scale, and specialist technical expertise required to develop foundation models. A small number of firms, therefore, can potentially be in a position to exploit existing or emerging bottlenecks across the emerging AI stacks and AI tools. This may also limit the scope of disruptive innovation, at the expense of fair competition.

Secondly, foundational AI models may aid in extending the market powers of large incumbent digital firms, which can stop innovative AI-driven disruption. With market control, such firms can also dictate adverse terms and conditions in the supply and distribution channels of AI or AI-enabled services to people and businesses.

Thirdly, emerging arrangements between key players could amplify risks. Arrangements like partnerships, financial investments, and other connections between foundational AI firms is a reality. Though this may not always harm competition, but does have potential undermine the competitive process and steer market outcomes in their favour. Besides these there are other competition risks such as algorithms allowing competitors to share competitively sensitive information, fix prices, or collude on other terms, unfair price discrimination or exclusion, etc. violative of competition laws. Competition authorities need to be vigilant about these.

The Joint Statement also illustrates 'Principles for protecting competition in the AI ecosystem,' which will generally serve to enable competition and foster innovation. These principles include: fair dealing, interoperability, and more choice.

Under the Digital Platform Services Inquiry 2020-2025, the ACCC in its last report has proposed to examine potential competition issues relating to generative AI. Such inquiry is likely to consider issues such as high barriers to entry in the market, and the potential for large digital platforms to strengthen and expand their market power through the integration of Large Language Models (LLMs).[151]

As a good practice, Australia is adopting a broader approach via the Digital Platform Regulators Forum (DP-REG), of which the ACCC is a member along with the Australian Communications and Media Authority (ACMA), the eSafety Commissioner (eSafety) and the Office of the Australian Information Commissioner (OAIC). The Forum is closely considering interactions between AI services and competition and consumer regulation.[152] A discussion paper titled "Review of AI and Australian Consumer Law" has been released by the Australian government for the purpose of gathering stakeholders' views.[153]

India has also launched a Market Study on AI and Competition,[154] to understand certain key AI systems and markets/ecosystems, to examine the emerging and potential competition issues in these markets/ecosystems, among others. This will help the Commission to ascertain enforcement and advocacy priorities with respect to AI and its application in markets.

It is to be noted that many countries of the world are in the process of crafting regulatory frameworks for AI, including Australia and India. However, a cautious approach is being adopted so that such regulations do not harm innovation.

# 5 Consumer Protection

Consumer protection in the telecom sector is vital for maintaining fair practices and safeguarding consumer interests, particularly in today's rapidly evolving digital landscape. As reliance on telecommunications services grows, understanding and protecting consumer rights becomes increasingly important. Key aspects of consumer protection include ensuring high Quality of Service (QoS) and Quality of Experience (QoE), addressing issues like call drops, and providing features such as enhanced video streaming and reliable communication. Emphasis is placed on consumer awareness, offering clear information about rights and services to empower informed decisions. Further, effective mechanisms for grievance redressal are necessary to ensure that consumers can lodge complaints and receive support throughout the resolution process.[155] As 6G networks become ubiquitous, consideration of consumer welfare and safeguarding their interests is paramount. Corporate practices, social expectations, codes, regulations, and policies need to work together to empower consumers, prevent unfair practices, and promote transparency.

In this regard, International organisations like the International Telecommunication Union (ITU)[156], the Organisation for Economic Co-operation and Development (OECD)[157], and the UN Commission on International Trade Law (UNCITRAL) contribute to establishing standards, policy principles, and legal frameworks aimed at ensuring consumer protection and quality of service in the telecommunications sector.[158] Further, both Australia and India have implemented laws and regulations to ensure fair practices and safeguard consumer interests in the telecom sector, emphasising the importance of international collaboration and domestic regulatory efforts in achieving these goals. Regulatory bodies, such as the ACCC and ACMA in Australia, and Central Consumer Protection Authority (CCPA), and TRAI in India, play a crucial role in addressing these concerns through enforcement actions and continuously evolving regulatory frameworks.

## 5.1. Consumer Protection Framework in Australia

In Australia, consumer protection within the telecom sector is governed by various organisations and regulations. The Australian Consumer Law grants consumers rights when acquiring telecom products or services, encompassing mobile phone services. The Australian Competition and Consumer Commission (ACCC), as a regulatory body, oversees competition and consumer protection across various industries, including telecommunications.[159] The ACCC, operating under the Competition and Consumer

Act, plays a crucial role in the telecommunications industry, with a focus on promoting competition, addressing market failures, facilitating access to essential infrastructure, and protecting consumers. Administering the telecommunications access regime, the ACCC aims to achieve the long-term interests of consumers by promoting competition, ensuring end-to-end connectivity, and encouraging economically efficient infrastructure use and investment.[160]

The completion of the National Broadband Network (NBN) rollout and the emergence of 5G technology mark a dynamic shift in Australia's telecommunications sector. The ACCC recognises this evolution and prioritises sustaining investment, fostering competitiveness, and balancing national security concerns in regulatory frameworks. Ensuring affordable and reliable communication services for consumers, regardless of location, and facilitating the efficient deployment of new technologies like NBN and 5G are central to the ACCC's mission. In the business sector, the ACCC supports new entrants and increased competition while addressing competition and consumer issues related to spectrum allocations. Overall, the ACCC's approach aims to cultivate a competitive, innovative, and consumer-centric telecommunications landscape in Australia.[161]

***Australian Communications and Media Authority (ACMA):*** Overseeing the communications and media sectors, ACMA plays a crucial role in establishing rules and standards to ensure consumer protection and market competition.[162] One of ACMA's initiatives is the Telecommunications Consumer Protections (TCP) Code, which provides guidelines for service providers to uphold fair treatment of consumers.[163] The TCP Code, serving as the primary regulatory framework for consumer protection in the telecom sector, is an enforceable industry Code of Conduct designed to ensure good service and fair outcomes for all users of telecommunications services in Australia.

The primary objective of TCP Code is to safeguard the interests of customers utilising mobile phones, landlines, internet services, and the NBN. The code enforces guidelines on communication and interactions with customers, sets standards for advertising and sales information, outlines procedures for billing and dispute resolution, defines payment methods, establishes criteria for assessing credit for new customers, and facilitates the smooth process of customers switching service providers. Essentially, the TCP Code ensures that telecommunications providers adhere to a set of standards designed to protect and benefit consumers across various aspects of their service experience.[164]

Additionally, the Telecommunications (Consumer Protection and Service Standards) (Accessible Standard Telephone Services) Regulations 2023 (TASSR 2023) in Australia, operating under the Telecommunications Act 1997, establishes standards for

accessible standard telephone services to protect consumer rights in the telecommunications industry. Administered by the Department of Communications and the Arts, these regulations are part of a comprehensive framework for consumer protection.

The ACCC regulates mobile services to ensure cross-network call accessibility, while the ACMA provides guidance on spectrum matters and monitors the mobile services market. Overall, TASSR 2023 contributes to a broader effort to establish fair and transparent practices in the telecommunications sector for the benefit of both providers and consumers.[165]

Strengthening the consumer protection framework, the Telecommunications Legislation Amendment (Enhancing Consumer Safeguards and Other Measures) Act, 2024 aims to enhance the statutory infrastructure provider (SIP) regime, ensuring widespread access to high-speed broadband for Australians. The Act establishes measures for smoother transitions when SIPs cease services, mandating sufficient notice and allowing NBN Co. to provide alternative infrastructure. It extends the SIP regime to private networks in new developments, ensuring universal access to quality broadband services. Additionally, the Act empowers the Telecommunications Industry Ombudsman to play a clearer role in resolving service connection disputes, fostering collaborative solutions between customers and providers. The Act also grants new powers to ACMA, enabling it to compel developers to rectify defective infrastructure in new developments, thereby shifting the remediation cost from homeowners or providers to developers. The ACMA will also have the authority to publish telecommunications providers' performance metrics, aiding consumers in making informed choices.[166]

## 5.2. Consumer Protection Frameworks in India

Consumer protection in the telecom sector in India is primarily overseen by the Telecom Regulatory Authority of India (TRAI) and the recently enacted Telecommunications Act 2023. The TRAI's mission is to ensure that the interests of consumers are protected while nurturing conditions for the growth of the telecom sector.[167] TRAI has established a framework for consumer protection that includes measures such as ensuring transparency in billing, protecting consumer privacy, and promoting fair competition among service providers.[168]

The Telecom Consumers Protection and Redressal of Grievances Regulations, 2007, establishes mechanisms for grievance resolution, prioritising consumer interests. The Telecommunication Consumers Education and Protection Fund Regulations, 2007, creates a fund to financially assist consumers in need. The Code of Practice for

Metering and Billing Accuracy Regulations, 2006, guarantees accurate practices by service providers. TRAI's initiatives, including the Telecom Consumers Complaint Monitoring System, empower consumers. Consumer outreach efforts educate users about rights and grievance resolution mechanisms.

Further, the Telecommunications Act, 2023 strengthens consumer protection with stringent regulations on service quality, and spam, and introduces a redressal system.[169] The Act has strengthened consumer protection by imposing strict regulations on service quality and spam messages and introducing a grievance redressal system. Some of the key consumer protections under this Act include the requirement for prior consent from users for any message offering, advertising, or promoting goods, services, business, employment, or investment opportunities. The act also enables subscribers to maintain a 'Do Not Disturb' register to block unwanted messages and report any malware or unspecified messages received. Additionally, the act provisions telecom service providers to establish an online mechanism for users to register and inform authorised entities about any malware or unwanted messages.[170]

The Consumer Protection Act (CPA), 2019, which repealed the earlier 1986 law, is an overarching legislation for the protection of consumers. The law establishes a layman-friendly three-tier consumer forums at district, state and national levels. The Act also establishes a regulatory body – Central Consumer Protection Authority (CCPA). The objective of the CCPA is to promote, protect, and enforce the rights of consumers as a class. It is empowered to conduct investigations into violation of consumer rights and institute complaints/prosecution, order recalls of unsafe goods and services, order discontinuation of unfair trade practices and misleading advertisements, and impose penalties on manufacturers/endorsers/publishers of misleading advertisements.[171]

# 6 Trusted 6g Ecosystem

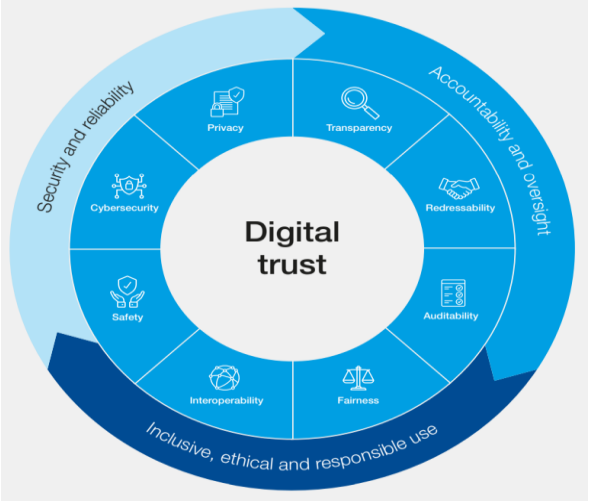
Digital Trust involves faith in digital systems, technologies, and processes to secure data, ensuring privacy and reliability in an interconnected digital world. In today's landscape, it serves as the linchpin for success, impacting brand image, technology adoption, investments, new offerings, and partnership expansion. Achieving digital trust requires strategic implementation of technology, processes, and policies, assuring users that digital products and services are safe and genuine, facilitating secure and worry-free digital interactions.[172]

In the case of 6G technologies, as there will be increased blurring of lines between the physical and digital realms, there will be increased dependence of safety on information security. A trusted ecosystem gains significance, driven by the transition from 5G's pillars: massive machine communication, ultra-low reliable latency, and enhanced mobile broadband, to incorporate sensing and Artificial Intelligence (AI). For enhanced information security too, the network must incorporate embedded trust. This entails the establishment of trust models, policies, and mechanisms.[173]

## 6.1. Ingredients of a trusted digital ecosystem

The World Economic Forum recognises eight dimensions against which the trustworthiness of digital technologies can be operationalised and evaluated. These dimensions span across three goals, viz, security and reliability, accountability and oversight, and inclusive, ethical, and responsible use.[174]

**Figure 5: Digital trust framework (Source: World Economic Forum)**



*Safety*: Safety encompasses efforts to prevent harm such as emotional, physical, and psychological, to individuals or society arising from the utilisation of technology and data processing.[175]

*Cybersecurity:* Cybersecurity includes safeguarding digital systems, encompassing data, technologies, and procedures. It aims to reduce the chances of unauthorised entry and harm to these systems, guaranteeing their resilience and upholding data and system confidentiality, integrity, and availability.[176]

*Privacy:* Privacy pertains to individuals' anticipation of controlling or keeping their personal or personally identifiable data confidential. For organisations, privacy entails meeting this expectation by creating data processing systems that empower individual autonomy through clear information and control over the collection, utilisation, and sharing of personal information.[177]

*Transparency:* Transparency necessitates honesty and clarity around digital operations and uses. By providing insight into an organisation's digital activities, it lessens the information gap between the organisation and its stakeholders.[178]

*Interoperability:* Interoperability is the ability of information systems to connect and exchange data for mutual use without unnecessary burden or restriction.[179]

*Auditability:* Auditability pertains to the capability of both an entity and external parties to examine and verify technology, data processing, and governance processes, including their outcomes. It acts as a mechanism to assess an organisation's commitments and demonstrates the organisation's intention to uphold these commitments.[180]

*Redressability:* Redressability denotes the potential for seeking remedy when individuals, groups, or entities experience adverse consequences due to technological processes, systems, or data utilisation. Trustworthy organisations establish robust procedures for redress when needed, aiming to make affected individuals whole in cases of unintended errors or unforeseen harm.[181]

*Fairness:* Fairness necessitates that an organisation's technology and data processing recognises the possibility of disparate impact and strive to attain impartial and equitable results for all stakeholders based on relevant circumstances and expectations.[182]

## 6.2. Trusted Network Communication

A trusted telecom equipment source refers to a product, company, or technology that has been deemed safe by the government for use in crucial and critical infrastructure.[183] The international supply chains for software and hardware in telecommunications networks can give rise to security apprehensions in the current fragmented geopolitical landscape. This becomes particularly challenging with the growing worry over the perils associated with acquiring and deploying communication technologies from untrustworthy providers. A significant challenge confronting nations is how to gauge the reliability and security of technologies offered by various suppliers. Given their implications for national security, it is imperative that telecommunications systems are exclusively procured from reputable suppliers or manufacturers.[184]

In this regard, the Trusted Network Communications (TNC) specifications facilitate several key aspects of network management. These encompass **network visibility**, which involves identifying users on the network and their access attempts. Additionally, they address **endpoint compliance**, ensuring that devices on the network are secure and that user/device behaviour aligns with established standards. **Network enforcement** capabilities enable the blocking of unauthorised users, devices, or behaviours while granting suitable access levels to authorised devices. Furthermore, TNC specifications allow for **security automation**, enabling the sharing of real-time environmental data without compromising sensitive, private, or protected information.[185]

*6.2.1 Zero Trust for telecom:* The zero trust model, assuming potential internal threats, boosts security by blocking unauthorised access and preventing lateral movement within a network. A zero trust architecture (ZTA) ensures secure access limited to authorised subjects through an identity-centric, policy-based approach. By combining runtime authorization decisions and traditional security principles, ZTA reduces the risk of external breaches and lateral movement during a security incident when properly implemented.[186]

*Key features for zero trust 6G networks:*

1. **Trust Assessment:** Continuous and dynamic evaluations of trust and risk should be conducted for each access request, ensuring ongoing scrutiny based on situational conditions.[187]
2. **Principle of Least Privilege:** Authorised access is strictly tailored, granting the minimum privileges necessary for specific resources without validity for other resources.[188]

3. **Dynamic Policy Framework:** Access decisions hinge on dynamic policies considering security states, credentials, software status, location, and behavioural attributes.[189] Policies, defining access rules and requirements, are managed and enforced by a framework, allowing micro-perimeter enforcement with precise access control based on roles, credentials, and environmental attributes. The core entities are the policy decision point (PDP) and policy enforcement point (PEP). A subject seeks permission from the PDP, providing necessary authentication and authorisation information. Policies, reflecting organisational processes, risk tolerance, and asset sensitivity, dictate protection levels, subject privileges, and environmental conditions influencing allowed behaviour. The policy engine, within the PDP, utilises a trust evaluation algorithm to calculate a subject's trust score, determining resource access based on provided information or additional metadata.[190]
4. **Integrity Monitoring:** Continuous real-time monitoring of network assets and users assesses security compliance and behavioural patterns against policy rules.[191] This monitoring aids in threat detection, gauging the security stance of network assets, and ensuring compliance with security policies. Assessing subjects, resource compliance, trustworthiness, and status is critical in determining whether access to resources should be granted.[192]

## 6.3. Cross-border data flow with trust

Global data traffic surged to 230 exabytes (230 billion gigabytes) per month in 2020, projected to triple to 780 exabytes by 2026.[193] These cross-border data flows crucially support the digital economy, enhancing trade efficiency, resilience, and governmental functions like national security and healthcare. Despite their ubiquity, there is a lack of globally agreed rules governing data collection, storage, and transfer. Existing frameworks are a complex web of unilateral, bilateral, and multilateral agreements, trade rules, and norms, inconsistently accepted or applied. Addressing this fragmentation is essential for fostering a more cohesive and secure global data environment.

The digital economy faces balkanization as economic blocs, such as China, the European Union, and the U.S., pursue contrasting data governance models. China emphasises authoritarian control, the EU leans towards heavy regulation, and the U.S. lacks comprehensive federal digital privacy legislation. For countries like Japan, these models impede the pursuit of a free, open, and interoperable global digital economy. Data Free Flow with Trust (DFFT) emerges as a potential solution to counteract this balkanization, fostering a trusted and interoperable global governance system for cross-border data flows. Operationalising DFFT was explored in 2023 in Japan and was

also adopted in 2022 Bali G20 Members' Regulations of Cross-Border Data Flows, offering recommendations for effective implementation.[194]

The DFFT idea seeks to encourage the unrestricted movement of data between countries, emphasising confidence in privacy, security, and intellectual property (IP). It endeavours to harmonise two interconnected policy goals: *first*, stimulating economic growth by facilitating open data flows, and *second*, safeguarding individual privacy, national security, and IP through reliable regulations. The core of the DFFT concept revolves around establishing trust as a fundamental element.[195]

Despite the international discourse being favourable to advance DFFT, the reality is hindered by geopolitical fragmentation and varied policy approaches. The national approaches are influenced by economic development, privacy protection, human rights, and national security concerns, thereby posing challenges in fully realising the goals of DFFT. There are three basic models for data policies with regard to the cross-border transfer of personal data:

1. *Open Safeguards:* Discretion in safeguarding transfers to the private sector, often guided by public guidelines. Includes private sector adequacy, contracts, and ex-post accountability.
2. *Pre-authorised Safeguards:* Public-sector approval is required before transfer, based on transparent criteria. Encompasses public-sector adequacy and ex-ante legal instruments like contractual clauses.
3. *Limited Transfers:* Imposes strict, less transparent requirements on cross-border data flows. Often requires storing and sometimes processing personal data within the country of origin. Applies to less defined data categories such as "important" or "critical" data.

These models may eventually converge, but the current diverse policy landscape creates costs, operational complexity, and uncertainties for entities seeking cross-border data sharing. OECD, in its report, *"A Preliminary Mapping of Data Localisation Measures"*[196], highlights efforts by countries to foster trusted cross-border data flows. These include policies to regulate data flow across borders, aiming to build trust. Intergovernmental cooperation is advanced through deliberations in forums like the G7 and the G20, standard-setting efforts, research initiatives promoting dialogue in multilateral organisations, and binding agreements among regional partners. Preferential trade agreements also contribute to the collaborative landscape, collectively addressing the complexities of cross-border data governance.

At the G7 summit in Germany (2022), digital ministers discussed DFFT as one of six key points, adopting a "G7 Action Plan." It focuses on: a) strengthening the evidence base

for DFFT; b) building on commonalities for future interoperability; c) continuing regulatory cooperation; d) promoting DFFT in digital trade; and e) sharing knowledge on international data spaces.[197] The G20 summit in Indonesia also emphasised the importance of identifying commonalities, complementarities, and convergence between regulatory approaches to foster future interoperability, as highlighted in the chair's summary of the G20 Digital Economy Ministers' Meeting.[198]

At last year's G20 summit in India, the New Delhi Leaders' Declaration acknowledged the significance of DFFT and cross-border data flows for achieving interoperability of digital public infrastructure while respecting relevant legal frameworks. Additionally, there was a reaffirmation of the role of Data for Development.[199]

In the context of 5G and potential future technologies like 6G, this idea becomes even more crucial as these telecommunications technologies play a central role in enabling the connectivity of devices and systems. Notably, 5G introduces enhanced data speeds and capacity, fostering faster and more efficient data transfer. Low latency is pivotal for real-time applications, like autonomous vehicles and critical infrastructure. Network slicing tailors dedicated networks for specific applications, ensuring optimal performance and security. Improved security features, such as enhanced encryption, contribute to a more secure data flow. Additionally, 5G facilitates edge computing, reducing latency by processing data closer to the source, while widespread Internet of Things (IoT) integration opens new avenues for applications and services.

With these notable security advancements, 5G also has some challenges. Security concerns emerge as the increased data flow in 5G networks raises privacy issues, demanding a delicate balance between optimising data utilisation and safeguarding individual privacy. Establishing global standards for 5G interoperability and security is a significant challenge, emphasising the need for international harmonisation to ensure a trustworthy and cohesive data flow in the interconnected world of 5G telecommunications. The complexity of these challenges requires robust measures to counter cyber threats and uphold trust in data flow.

6G telecommunications promises a revolutionary shift in connectivity, redefining data speeds, security, and sustainability. Expected to surpass the capabilities of 5G, 6G with its unprecedented data speeds and capacity, will set the stage for innovative applications. Security measures in 6G will likely include enhanced encryption, authentication, and potential integration of quantum-resistant cryptography. 6G's support for holographic communication and extended reality introduces immersive experiences, presenting challenges and opportunities for trust in telecommunications.

Prioritising the resilience and reliability of 6G networks is crucial, particularly in critical service scenarios and emergency communications. A key consideration involves developing systems that can withstand disruptions and ensure a dependable data flow even in challenging conditions. Additionally, the integration of artificial intelligence (AI) is essential for managing and securing data flow. AI-driven analytics play a pivotal role in anticipating and addressing emerging threats, contributing to the overall robustness and security of 6G networks. This dual focus on reliability and AI integration underscores the commitment to building a resilient and secure telecommunications infrastructure for the future.

Thus, it is essential to ensure DFFT in 6G networks and also ensure privacy, security, and interoperability, with clear policy and regulatory frameworks. Collaboration among governments, industry stakeholders, and international organisations is vital in shaping these frameworks, and fostering a secure and cohesive environment. A human-centric design approach is critical, prioritising user experience and ethical considerations. 6G networks should aim to empower users with control over their data, emphasising ethical implications for building trust.

# 7 Inclusive and Sustainable 6G

The digital divide, as defined by the Organisation for Economic Co-operation and Development (OECD), refers to the disparities among individuals, households, businesses, and geographic areas at socio-economic levels regarding their access to information and communication technologies (ICTs) and their utilisation of the internet for activities. In simpler terms, it represents the inequalities between those who have access to the internet and ICTs (the digital "haves") and those who do not (the digital "have-nots"). Given the growing significance of the internet and the rapid digital transformation, the UN Deputy Secretary-General, Amina Mohammed, has even suggested that the digital divide could become the "new face of inequality."[200]

The digital divide carries significant social implications that cannot be overlooked. The lack of access to technology has the potential to exacerbate existing social disparities and deprive individuals of essential resources. The digital divide remains a global challenge, with its manifestation varying across countries due to factors such as geography, culture, infrastructure development, socio-economic conditions, education, and literacy levels. According to GSMA data from 2021, while global mobile internet coverage reached approximately 95% of the world's population, only 55% were active users.[201] As of mid-2022, more than 63% of the world's population, or 5.3 billion people, were connected to the Internet. Nevertheless, a significant portion, roughly over a third of the world's population, remains unconnected. Notably, many of these individuals reside in the least developed countries, landlocked developing countries, and small island developing states.[202]

Such discrepancy, termed the "Usage Gap," represents 3.2 billion people—more than one-third of the global population—who reside in areas with mobile internet connectivity but lack actual access. Sub-Saharan Africa exhibited the highest usage gap at 61%, followed closely by South Asia at 54%. India, despite its relatively high usage gap of 61%, has shown a steady decrease over time.[203] Internet usage statistics from 2019 revealed a stark disparity between developed and developing countries, with 87% and 44% utilisation rates, respectively. Urban-rural disparities persist globally, with 76% of urban households enjoying internet access in 2020, compared to only 39% in rural areas. This divide is particularly pronounced in Least Developed Countries (LDCs), where 15% of the rural population lacks mobile coverage entirely, and an additional 10% is limited to 2G networks.[204]

The COVID-19 pandemic accelerated overall internet adoption but simultaneously exacerbated existing digital divides, both between and within countries, stemming from factors such as age, disability, gender, geography, and socioeconomic status. The affordability of broadband internet access remains a significant challenge, particularly in LDCs, where costs often exceed the Broadband Commission for Sustainable Development's target of 2% of monthly gross national income per capita. Data from the International Telecommunication Union (ITU) in 2021 indicated a decline in the number of economies meeting the 2% affordability target for both mobile and fixed broadband services compared to the previous year.[205] The digital divide is likely to widen due to persistent disparities within societies. This concern is grounded in the observation that the evolution of mobile wireless networks could exacerbate existing inequalities. For instance, the uneven distribution of the 5G networks during its initial rollout has already created a gap between regions with advanced network coverage and those without. Moreover, as highlighted in [11], merely expanding network coverage does not close the digital divide. Skills and digital literacy are crucial in bridging this gap; thus, technology must be leveraged not only to enhance connectivity but also to improve digital skills and inclusion.[206]

The evaluation of 6G connectivity may also exacerbate the digital divide in rural or underserved regions, where access to 6G technology could remain limited or non-existent, thus deepening the existing gap between rural and urban areas. Another critical consideration is the affordability of 6G services and devices. Despite the advanced speeds and capabilities offered by 6G, the costs associated with accessing 6G networks and acquiring compatible devices may be prohibitively high for individuals or communities with limited financial resources. This affordability challenge could result in the exclusion of some populations from the benefits of 6G technology, impeding their participation in the evolving digital economy. Addressing the necessary investments to achieve affordable universal connectivity is essential for realising the SDGs. In some regions, bridging the connectivity gap involves primarily upgrading existing coverage and capacity sites. However, in Sub-Saharan Africa, South Asia, and East Asia/Pacific, nearly half of the required investments in radio access network (RAN) infrastructure will need to be developed from the ground up.[207]

| India | Australia |
|---|---|
| While there was a notable increase in mobile internet usage among women in India, from 21% in 2019 to 30% in 2020 during the COVID-19 pandemic and subsequent lockdowns, this percentage remained stagnant throughout 2020-21, | The Australian Digital Inclusion Index (ADII) reveals that although digital inclusion is making gradual progress throughout Australia, a substantial digital divide still exists. Remarkably, one in four people in Australia remains |

| India | Australia |
| --- | --- |
| showing no further growth. In contrast, the proportion of Indian men using mobile internet experienced continuous growth, rising from 45% in 2020 to 51% in 2021, up from 42% in 2019. This discrepancy in internet usage between women and men highlights the gender gap in mobile internet adoption. This gender gap is also evident in smartphone ownership among men and women in the country. Nearly half of the male population in India owns a smartphone, whereas this figure is only slightly over a quarter for the female population.[208]<br><br>According to TRAI's Performance Indicator Reports as of December 2022, the number of broadband subscribers in urban areas stood at 497.14 million, while in rural areas, it was 335.06 million. This data clearly illustrates the rural-urban disparity in broadband subscriptions. In addition, there's a notable difference between the internet teledensity in rural and urban areas as of December 2022. The internet teledensity in rural areas is less than half of that in urban areas. It's worth mentioning that the rural-urban gap was on the rise until 2019. However, since 2019, concerted efforts have been made to enhance coverage in rural areas, leading to a significant reduction in this gap.[209] | digitally excluded as of 2023, according to the ADII. Those particularly vulnerable to being left behind are individuals with low income, education, and employment levels, residents of certain regional areas, people aged over 65, and those with disabilities. Notably, a study by RMIT University found that mobile data speeds in rural towns with substantial Indigenous communities were on average 90% slower than in urban areas. The 2021 Australian Digital Inclusion Index reports a decline in the number of Australians who experience significant digital exclusion. Nevertheless, this percentage remains substantial, affecting 11% of the population.[210] |

## 7.1. 6G: Bridging the Digital Divide

Despite the foundational considerations outlined previously, it is crucial to recognize that emerging 6G wireless networks, while still in their nascent stages, aim to address the unresolved issues of earlier generations. The development of 6G is particularly focused on overcoming the unique challenges faced by remote and rural areas, with the overarching objective of ensuring universal connectivity and promoting digital inclusion. Unlike its predecessors, 6G is not merely an exploration of additional spectrum in high-frequency bands; it represents a transformative shift towards ubiquitous, pervasive, and high-speed Internet connectivity. Notably, 6G has the potential to act as a pivotal advancement by facilitating a high degree of automation in service execution and significantly expanding cellular network coverage. In this section, we explore the potential implementations of technologies that could effectively address and manage the service-delivery divide. These technologies are capable of providing Internet access in areas where traditional network infrastructures are inadequate.

### 7.1.1. Non-Terrestrial Networks

In the evolution from current 5G networks to the envisioned 6G technology, a significant shift towards three-dimensional non-terrestrial networks (NTNs) is anticipated. These NTNs will incorporate airborne and spaceborne platforms, including unmanned aerial vehicles (UAVs), high altitude platform stations (HAPSs), and satellite systems such as Low Earth Orbit (LEO) constellations for last-mile connectivity. Among these, LEO satellites, particularly CubeSats, have garnered considerable attention due to their compact size and cost-effectiveness. These attributes make them ideal for deployment in mega-constellations, offering the potential for global connectivity and high throughput. NTNs present a robust and independent networking solution, ensuring connectivity in scenarios where established network infrastructures are unavailable or terrestrial towers are non-operational, such as in the aftermath of natural disasters. This evolution in network architecture is expected to benefit various sectors, including inter-regional transport, agriculture, maritime operations, mountainous regions, and remote maintenance facilities.

The progress towards NTNs is supported by advancements in aerial and space technologies. These include developments in solid-state lithium batteries and Gallium Nitride technologies. Additionally, new approaches to spectrum allocation are being explored, such as the transition to millimetre-wave (mmWave), Terahertz, and optical bands. Innovative antenna designs are also emerging, featuring reconfigurable phased, inflatable, and fractal antennas created using metasurface materials. Despite these promising developments, several challenges remain to be addressed in the implementation of NTNs. These primarily relate to issues of latency, coverage, and

energy constraints. Emerging LEO satellite initiatives, such as SpaceX's Starlink, show potential in offering global coverage and low-latency services once fully operational. However, critical questions regarding the management of these satellite constellations and the disposal of satellites at the end of their operational life still need to be resolved. The transition to 6G and the incorporation of NTNs represent a significant leap in telecommunications technology. While offering immense potential for global connectivity and enhanced network resilience, this evolution also brings forth new technical and operational challenges that will need to be addressed as the technology matures.[211]

### 7.1.2. Harnessing the Potential of Higher Frequencies

To effectively reduce disparities between digital haves and have-nots and enable the delivery of 6G services, achieving ultra-high-speed communications is crucial. A promising approach involves harnessing previously unexplored portions of the spectrum.[212] While 5G mobile networks have explored the millimetre-wave band, attention is now turning towards TeraHertz and even optical bands. This shift is made possible by recent advancements in electronics and photonics, which have enabled the development of portable equipment capable of operating at these extremely high frequencies. However, signal propagation at these frequencies presents significant challenges, including severe path loss, high molecular absorption, and the need for precise antenna alignment. To extend coverage, Intelligent Reflecting Surfaces (IRS) offers a potential solution. These surfaces enable the creation of virtual line-of-sight (LoS) links by intelligently reconfiguring the wireless propagation environment.[213]

IRSs typically consist of numerous low-cost passive reflecting elements integrated onto a planar surface. These elements can independently manipulate the amplitude and phase of incident signals, collectively achieving fine-grained three-dimensional (3D) passive beamforming to enhance signal directionality. The applications for higher frequencies are diverse, ranging from indoor coverage to earth-to-ground communications. These advancements have the potential to play a significant role in bridging the service-delivery gap and promoting more equitable access to advanced telecommunications technologies. As research and development in this field progresses, it is essential to consider the practical implementation of these technologies in various environments and their potential impact on reducing digital inequalities. The successful integration of these advanced communication methods into 6G networks could mark a significant step towards more inclusive and accessible digital connectivity worldwide.[214]

### 7.1.3. Device-to-Device Communication in the 6G Era

In the emerging 6G era, Device-to-Device (D2D) communication is poised to play a crucial role in expanding network coverage and bridging the digital divide. As the telecommunications industry moves beyond 5G, there is a growing interest in distributed networking approaches to enhance connectivity and scalability. D2D communication offers a promising solution to address the coverage limitations of higher frequency waves anticipated in 6G networks.[215] The fundamental principle of D2D communication involves the use of relay nodes to enable direct communication between devices. This approach effectively extends network coverage and provides access to services for devices located beyond the line of sight of network antennas. By facilitating direct communication between nearby devices, D2D technology can significantly improve network performance, offering high-speed connectivity with low latency.[216]

Such characteristics of D2D communication align well with the stringent requirements expected of 6G networks. The technology's ability to extend coverage and improve connectivity in areas with limited infrastructure makes it particularly valuable in addressing digital inequality. As 6G development progresses, D2D communication is expected to be a key component in expanding access to high-quality connectivity, especially in underserved areas. The integration of D2D communication in 6G networks represents a shift towards more flexible and resilient network architectures. This approach can potentially overcome some of the challenges associated with traditional centralised network structures, offering improved coverage, capacity, and energy efficiency. As such, D2D communication is likely to be instrumental in realising the full potential of 6G technology and its promise of ubiquitous connectivity.[217]

### 7.1.4. A Dedicated Remote-Centred Connectivity Layer

The advent of 6G technology should introduce a new, fourth service tier specifically designed to address fundamental connectivity requirements in remote areas. This remote-centered connectivity layer represents a departure from the traditional urban-centric model of mobile communications, acknowledging the unique needs and challenges of remote locations. This new service category must be carefully tailored to prioritise the specific demands of remote connectivity scenarios. Key focus areas include extended coverage and cost-effectiveness, which are crucial for reaching and serving isolated populations. In contrast to the high-performance metrics typically associated with urban 5G networks, this remote mode can afford to relax certain constraints on throughput and latency, recognizing that basic connectivity often takes precedence over ultra-high-speed services in remote contexts.

To implement this specialised service effectively, the remote connectivity layer should operate on its own dedicated network slice. This approach allows for the integration of specific, moderate levels of edge computing and caching capabilities, optimised for remote environments. By enabling data processing at various levels - edge, local, or central data centres - this architecture enhances the overall scalability of the network. The design of this remote-centric layer with its tailored capabilities and relaxed performance constraints offers a significant advantage: it allows for the provision of connectivity services at more affordable rates. This cost-effectiveness is crucial for bridging the digital divide and ensuring that remote and underserved populations can access essential digital services. By introducing this dedicated remote-centered connectivity layer, 6G technology has the potential to significantly advance the goal of universal connectivity, addressing the unique challenges of remote areas and making digital inclusion a more achievable reality.[218]

### 7.1.5. Multi-Access Edge Computing

Multi-Access Edge Computing (MEC) is emerging as a key technology in the distributed networking landscape, offering significant potential to enhance service delivery and bridge the digital divide. This approach brings computing resources closer to the network edge, near the end-users, providing several advantages over traditional centralised computing models. MEC servers leverage virtualization techniques to allocate resources efficiently to consumers with limited capabilities. They can offer various service models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), tailoring their offerings to meet specific user needs. This flexibility allows for more efficient resource utilisation and improved service delivery. The proximity of MEC infrastructure to end-users results in notably low latency and enhanced context awareness. These characteristics enable the customization of services based on local conditions and user requirements, leading to a more responsive and personalised user experience.[219]

By providing support for communication, computing, and storage at the network edge, MEC significantly improves the Quality of Service (QoS) experienced by users. This improvement in QoS is particularly crucial in addressing the digital divide. Poor service quality has been identified as a significant barrier to the effective delivery of bandwidth-intensive services, especially in underserved areas. By enhancing QoS through MEC, these advanced services become more accessible to a wider range of users, including those in areas with limited network infrastructure. The implementation of MEC technology represents a significant step towards more equitable digital access. By improving service quality, reducing latency, and enabling more efficient resource allocation, MEC has the potential to make advanced digital services more accessible to users across diverse geographical and socioeconomic contexts. This technology thus

plays a vital role in the ongoing efforts to bridge the digital divide and ensure more inclusive access to digital resources and services.[220]

### 7.1.6. Enabling Multiple Radio Access Technologies (RATs) Interoperability

The integration of Multiple Radio Access Technologies (RATs) presents a promising approach to enhancing connectivity in remote areas.[221] This strategy involves combining various wireless communication technologies to create local access solutions tailored to specific geographical and infrastructural challenges. In the effort to digitise remote regions, expansive coverage solutions such as mega-cells are being explored. These mega-cells utilise TV or GSM white spaces (WSs) to extend coverage over large areas. The primary advantage of this approach is the ability to increase the user base served by a single base station, thereby reducing network deployment and management costs. However, this expansion in coverage often comes with certain performance trade-offs and necessitates adjustments to power limits. The transition from 5G to 6G technology is expected to introduce even greater network heterogeneity and scale. The incorporation of Terahertz and optical spectrum solutions in 6G will create new opportunities for enhancing network performance beyond what is currently possible with multi-RAT implementations in 5G.[222]

A particularly promising technology in this context is visible light communications (VLCs). VLC technology has the potential to significantly boost indoor throughput, where people spend the majority of their time. Additionally, it can improve front haul capabilities and even extend connectivity to underwater environments. An added benefit of VLC is its dual functionality – while providing communication capabilities, it simultaneously serves the practical purpose of illumination. This dual-use nature makes VLC a cost-effective technology for enhancing connectivity. The combination of these diverse technologies and approaches in the 6G era offers a comprehensive strategy for addressing connectivity challenges in various environments. By leveraging the strengths of different RATs and innovative solutions like VLC, it becomes possible to extend high-quality connectivity to previously underserved areas, thereby contributing to the reduction of the digital divide.[223]

### 7.1.8. Wireless Backhaul Solutions for Remote Connectivity

Wireless backhaul solutions for remote connectivity offer various options, each with its own set of advantages and challenges. Increasing the number of fibre links can significantly enhance broadband access in unconnected areas but comes with high costs. Conversely, Power Line Communication (PLC) connections provide a more cost-effective solution by using existing wired infrastructure for data transmission, though they face challenges related to adverse channel conditions that must be addressed.

The concept of Non-Terrestrial Networks (NTN), as envisioned for 6G, presents a promising alternative for low-cost, robust, and long-range backhaul, complementing traditional technologies in remote areas. Additionally, recent trends include the development of cost-effective backhaul solutions utilising software-defined technology, which connects previously unconnected communities.

Integrated Access and Backhaul (IAB) is another explored solution, replacing traditional fibre infrastructures with self-configuring relays operating via wireless backhaul.[224] IAB solutions offer lower complexity than traditional fibre networks, facilitating installation in rural areas where laying cables is both challenging and costly. In the realm of 5G, wireless backhaul typically operates at millimetre-wave frequencies. However, 6G-specific technologies, such as Terahertz, could be leveraged to multiplex access and backhaul data within the same frequency bands, potentially reducing the need for additional hardware or spectrum licences.

Free Space Optical (FSO) links also present a viable alternative for expanding network coverage in isolated regions with difficult terrains, though they are sensitive to optical misalignment, requiring further research on spherical receivers and beam scanning to enhance their signal reception from various angles. Beyond backhaul, improving mid-haul and fronthaul connections through AI and machine learning (ML)-based solutions can offer cognitive capabilities for efficient utilisation of available licensed and unlicensed spectrum. This is particularly valuable in remote areas with sparse user distribution, which can lead to spectrum gaps.[225]

Unlicensed spectrum can enhance the return on investment (RoI) for service delivery and improve network flexibility. Exploring new possibilities, such as advanced multiple access schemes and waveforms like non-orthogonal multiple access (NOMA), is crucial. NOMA is especially relevant for Internet of Things (IoT) services, where some sensors are close to base stations while others are further away. AI and ML can be used to control physical and link layers, enabling seamless and context-aware transitions in modulation and coding schemes (MCSs). It is important for these solutions to be lightweight to reduce costs and maintenance while being optimised for the specific target market segment.

## 7.2 Sustainability

Sustainability has become an important concern across all sectors of society, and wireless networks have already made significant contributions to advancing the United Nations Sustainable Development Goals (SDGs) and other climate-related objectives. The advent of 6G technology presents a new opportunity to further enhance the role of wireless networks in promoting global digital inclusion and sustainability. The

potential of 6G to contribute to sustainability is multifaceted. It can provide high-quality services to essential institutions such as schools and hospitals, improving access to education and healthcare. Additionally, 6G can enhance resource efficiency through comprehensive digital asset tracking, enabling better management and utilisation of resources. Furthermore, it can promote environmentally friendly lifestyles and practices through increased digitalization, reducing the need for physical travel and resource-intensive activities.[226]

As 6G technology develops, high network energy performance remains a crucial design consideration. This involves minimising the energy consumption of network nodes to near-zero levels during periods of inactivity and enhancing scalability to handle rapid changes in network traffic. These features are essential for reducing the overall energy footprint of wireless networks. Given the growing emphasis on climate action and sustainability, it is imperative that 6G use cases are developed with technical and policy solutions that prioritise sustainability and aim for net-zero carbon emissions. This approach aligns with global efforts to combat climate change and ensures that the expansion of wireless technology does not come at the cost of environmental degradation. The Next Generation Mobile Networks Alliance (NGMN) advocates for the evaluation of the overall sustainability value of each service or application as a crucial step in the development of 6G. This holistic approach ensures that sustainability is not an afterthought but an integral part of 6G's design and implementation from the outset.[227]

# 8 Stakeholders Insights

## 8.1. Cyber security

From the stakeholders' perspective, the emergence of 6G technology will bring forth cybersecurity challenges stemming from the increased complexity and interconnectivity of networks. Protecting 6G networks from cyber threats will necessitate the implementation of advanced security measures, including AI-driven cybersecurity tools and quantum encryption technologies. The heightened reliance on connected devices, artificial intelligence, and the Internet of Things (IoT) within 6G networks will expand the attack surface, rendering these networks more susceptible to cyber threats. Stakeholders acknowledge that the integration of AI and the proliferation of autonomous systems will create additional attack vectors, making the security landscape even more challenging. Particularly concerning is the issue of adversarial machine learning, wherein malicious actors manipulate AI systems.

To safeguard 6G networks, robust encryption, secure communication protocols, and proactive threat detection mechanisms will be essential. Furthermore, clear guidelines for responding to cybersecurity incidents and protecting critical infrastructure must be established. Addressing the ethical challenges associated with 6G will require regulatory bodies to adopt proactive strategies. This includes anticipating potential harms related to AI, data privacy, and cybersecurity while developing regulations that can adapt as technology evolves. Stakeholders advocate for the integration of cybersecurity measures into every IT budget, recommending that approximately 10 percent be specifically allocated for cyber protection. The role of the state in cybersecurity is seen as critical, especially as it emerges as the largest collector of data. Ensuring that government data collection and usage practices do not undermine privacy and security would be important, and stakeholders emphasise the necessity of international cooperation to tackle global cybersecurity threats.

## 8.2. Privacy

From the stakeholders' perspective, the anticipated massive data generation associated with 6G technology raises concerns regarding privacy. Stakeholders recognise that the vast amounts of data produced by 6G-enabled devices necessitate the implementation of robust data protection measures to safeguard individual privacy. An ethical framework for 6G should include stringent data protection protocols, including anonymisation techniques, consent mechanisms, and transparent

data handling practices. It is critical for stakeholders to ensure that individuals retain control over their personal data and are well-informed about how their data is utilised. Given the unprecedented volume of data that 6G networks are expected to process, strict data minimisation practices should be enforced. This entails requiring informed consent from consumers and establishing clear guidelines for data sharing between entities, which is crucial for protecting personal information while still fostering innovation.

Furthermore, the increased reliance on artificial intelligence and Internet of Things devices within 6G networks amplifies the potential for privacy breaches. Stakeholders stress the importance of developing robust frameworks to protect consumer data, which may include advanced solutions such as quantum encryption technologies and secure data management practices. Finally, educating the public about the privacy implications of 6G technology is crucial. Stakeholders advocate for public awareness campaigns and educational initiatives designed to empower users to make informed decisions regarding their engagement with 6G-enabled services. This proactive approach will help mitigate privacy risks while maximising the benefits of 6G technology.

## 8.3. Competition

Stakeholders expressed concerns that the deployment of 6G networks could exacerbate monopolistic practices, especially among large technology companies. To ensure fair competition, they emphasise the need for a balanced regulatory framework. There is apprehension that 6G, much like 5G and earlier technologies, could lead to increased market concentration. In response, stakeholders advocate for stronger antitrust frameworks, drawing inspiration from models like the Digital Markets Act (DMA) in Europe, to prevent monopolistic behaviour. They stress the importance of regulators actively monitoring the market and enforcing rules to curb the abuse of market power. This includes the development of ex-ante regulations to complement competition enforcement, ensuring that competition authorities are adequately prepared to address the rapid technological advancements in 6G.

Promoting interoperability through open standards is seen as crucial to preventing market concentration, and enabling smaller players to remain competitive. Stakeholders highlight the importance of this in areas like spectrum slicing, where varying use cases demand different bandwidths, which should not be monopolised by a select few companies. Additionally, the evolving relationship between telecom service providers and content/application service providers is viewed as increasingly symbiotic, requiring a regulatory approach that reflects these changes. A “diagonal equity” approach, which applies similar regulatory principles to both telecom and

content companies, is considered necessary to maintain fairness and competitiveness in the 6G market.

## 8.4. Consumer Welfare

From the stakeholders' perspective, ensuring consumer welfare is a fundamental priority within the ethical framework for 6G. The rollout of 6G networks must not only maintain fair competition but also guarantee that consumers have access to affordable, high-quality services. Regulators play a crucial role in ensuring that consumers can access 6G services at reasonable prices, actively preventing monopolistic practices that could result in inflated costs, and ensuring the availability of 6G-enabled services to a diverse consumer base. Protecting consumers from potential exploitation is also vital, particularly regarding data security and privacy. Stakeholders advocate for stringent regulations to prevent the misuse of consumer data by companies and to ensure that consumers are well-informed and retain control over their personal information.

The deployment of 6G technology necessitates substantial infrastructure investments, which call for a fair cost-sharing mechanism. This would involve larger content providers contributing to infrastructure costs to prevent financial burdens from falling disproportionately on consumers. Drawing from successful examples in countries like South Korea, such an approach is seen as essential for a balanced rollout of 6G. Additionally, consumer welfare encompasses the need for public education regarding the potential risks and benefits associated with 6G technology. Stakeholders emphasise the importance of public awareness campaigns and educational initiatives to empower consumers, enabling them to make informed decisions and promoting a culture of digital literacy and ethical responsibility.

## 8.5. Trusted Ecosystem

From the stakeholders' perspective, building a trusted ecosystem is fundamental to the success of 6G technologies. Establishing trust in both the technology itself and the institutions responsible for its development and deployment is crucial. The integrity of 6G networks will largely hinge on the transparency and accountability of the companies and organisations involved in their creation. Stakeholders agree that the artificial intelligence (AI) and algorithms integrated into 6G networks must be transparent, explainable, and free from bias. To this end, there is a pressing need to establish and adhere to standards for ethical AI development. This encompasses the responsible development of AI systems that operate transparently and with accountability.

Furthermore, stakeholders underscored the importance of creating certification and compliance mechanisms that ensure 6G technologies are safe, secure, and reliable.

These mechanisms should be developed in collaboration with international partners to foster global interoperability and build trust. A truly trusted ecosystem requires the active involvement of multiple stakeholders, including government agencies, private companies, civil society, and international organisations. This collaborative approach is essential for ensuring that diverse perspectives are integrated into the governance of 6G technologies, ultimately contributing to their successful implementation and public acceptance.

## 8.6. Sustainability and Inclusivity

From the stakeholders' perspective, sustainability and inclusivity are essential components of the ethical framework for 6G, ensuring that the technology serves humanity as a whole while minimising its environmental impact. The deployment of 6G technology is anticipated to require substantial energy and resources, raising valid concerns about its ecological footprint. Thus, an ethical framework must incorporate guidelines aimed at reducing the carbon footprint of 6G networks, enhancing energy efficiency, and embedding sustainable practices into the design and operation of 6G infrastructure. Stakeholders emphasise the need for 6G technology to align with broader sustainability goals by adopting energy-efficient designs and addressing issues related to electronic waste by promoting the recycling of electronic components.

During the consultation, it was highlighted that, to guarantee that the advantages of 6G technology are equitably accessible, stakeholders recognize the necessity of addressing digital inclusion and the digital divide. This involves deploying 6G networks in underserved and remote regions, as well as ensuring affordable access to 6G-enabled devices and services. The ethical framework for 6G should prioritise equitable access to technology, focusing on marginalised and vulnerable communities to prevent them from being left behind. Efforts must include promoting digital literacy and offering support to communities that may face challenges in adapting to new technologies. International cooperation is seen as vital in tackling the global challenges presented by 6G. Countries like Australia and India are viewed as having the potential to lead in the ethical development and utilisation of 6G technology, setting global benchmarks for privacy, security, and inclusivity.

# 9 Conclusion and Recommendations

## 9.1. Conclusion

The transition to 6G technology presents immense opportunities to transform society through advanced applications. However, it is essential to ensure that 6G development and deployment are guided by an ethical framework, as illustrated above. Our analysis highlights the critical need for transparency and accountability across all aspects of 6G development and implementation. Ensuring that stakeholders are open about their practices and accountable for their actions will build trust and foster a more secure digital environment. Equally important is the protection of privacy; robust measures must be integrated into 6G systems to safeguard personal data and uphold privacy principles. This includes the adoption of privacy-by-design practices and a commitment to privacy-by-default.

Consumer welfare must remain a central concern, with a strong focus on protecting rights and ensuring fair treatment, including quality of service. This involves not only establishing effective mechanisms for grievance redressal but also ensuring that technological advancements do not compromise consumer interests. The promotion of competitive markets with fairness is also crucial; maintaining a level playing field and encouraging innovation through fair competition are essential for a healthy digital economy.

Trust and inclusivity are fundamental to the success of 6G. Building a trusted ecosystem requires addressing digital divides and promoting accessibility so that the benefits of 6G technology are equitably distributed. Additionally, sustainability must be at the forefront of 6G development, with an emphasis on minimising environmental impact through energy-efficient designs and practices. To advance these objectives, it is imperative for inter-governmental bodies to foster global collaboration and support the development of international standards that incorporate these ethical principles.

Governments should, thus, adopt and enforce comprehensive policies that address cybersecurity, privacy, and inclusivity while also promoting fair competition. Industry stakeholders must prioritise ethical design, fair practices, and sustainability in their technology developments and deployments.

## 9.2. Recommendation

### 9.2.1. Cybersecurity

*Robust Security Measures:* 6G networks must be designed with robust security measures from the ground up. This includes implementing end-to-end encryption to protect data confidentiality and integrity, developing secure authentication mechanisms to prevent unauthorised access, employing AI-driven algorithms for real-time threat detection and response, and ensuring the trustworthiness of 6G network components and suppliers.[228][229]

*Developing Security Standards and Best Practices:* Comprehensive security frameworks that address the unique vulnerabilities of 6G technology must be developed and implemented. This includes establishing security standards and best practices for 6G networks, aligned with the principles outlined in the Joint Statement Endorsing Principles for 6G: Secure, Open and Resilient by Design"[230], ensuring the protection of individuals' data, and promoting sustainable and affordable connectivity. Additionally, fostering partnerships between governments, industry stakeholders, and cybersecurity experts is essential to develop global standards and regulations.[231][232]

*Proactive Threat Mitigation:* Anticipating and mitigating potential threats is essential for maintaining a secure 6G ecosystem. This involves continuously monitoring and adapting to evolving cyber threats, conducting regular risk assessments, implementing mitigation strategies, and promoting cybersecurity awareness and training among 6G stakeholders.[233][234]

*International Cooperation and Standardisation:* Promoting international cooperation and information sharing is crucial for enhancing global cybersecurity. Establishing international standards and guidelines for 6G security is a key priority. The "Joint Statement Endorsing Principles for 6G: Secure, Open and Resilient by Design"[235] outlines shared principles for the research and development of 6G systems, fostering cooperation on secure and resilient connectivity.

### 9.2.2. Privacy and Data Protection

*Implement privacy by design and standardised privacy metrics:* Integrate privacy by design principles into the development of 6G technologies and infrastructure from the outset. This should be coupled with the establishment of standardised privacy metrics and thresholds for assessing when linked, de-identified data sets become personally identifiable information. This framework would guide courts, businesses, and developers in maintaining ethical data practices while fostering innovation. Incorporate emerging technologies like blockchain and differential privacy to enhance data protection within this privacy-centric design approach.

*Enhance transparency and user control in data management:* Develop clear, accessible mechanisms for transparency in data collection, usage, and sharing practices by 6G operators and service providers. Empower users with granular control over their personal data, including easy-to-use opt-out options for data sharing. Implement trust technologies such as Trusted Platform Modules (TPMs) and distributed ledger technologies to create tamper-proof records of data access rights and security claims, ensuring transparency across diverse operator domains.

*Adopt quantum-safe cryptography and multi-layered security:* Initiate a transition to quantum-safe cryptographic algorithms to protect against future quantum decryption threats. Integrate Quantum Key Distribution (QKD) and advanced privacy-preserving technologies like homomorphic encryption into 6G networks. Develop a comprehensive, multi-layered security architecture that addresses the challenges of cloud and edge-native infrastructures, incorporating machine learning for automated security measures and physical layer security techniques. For industrial networks, implement protective measures such as jamming detectors and frequency hopping. Throughout this security framework, maintain transparency about the security measures in place and provide clear communication to users about how their data is protected.

### 9.2.3. Consumer Protection

Consumer protection in the telecom sector, particularly with the advent of 5G and forthcoming 6G technologies, is paramount to uphold fair practices, data privacy, and service quality for users. Strengthening regulatory frameworks is essential, involving regular reviews of laws and regulations to accommodate the unique challenges posed by advanced technologies. Collaboration between regulators and industry stakeholders is vital to develop comprehensive guidelines ensuring consumer rights, fair competition, and transparent service offerings. Protecting consumers from unfair practices and ensuring affordable access to 6G services becomes crucial.

Empowering consumers with information is crucial. Telecom companies must provide clear and concise details about service plans, pricing, data usage policies, and network performance to enable informed decisions.

Ensuring quality of service is another key aspect. Establishing benchmarks to monitor network performance and reliability is essential, holding telecom operators accountable for meeting minimum service standards. Promoting competition and innovation is critical for driving service improvement and offering consumers a broader range of choices at competitive prices.

Enhancing consumer education and awareness is pivotal. Educating consumers about their rights, responsibilities, and available recourse mechanisms fosters informed decision-making and empowers users to assert their rights in the telecom marketplace. Effective complaint resolution mechanisms must be established, ensuring efficient redressal of consumer grievances with telecom service providers through independent regulatory bodies or ombudsmen. Establish mechanisms for consumer redressal and grievance handling. Empower consumers with greater control over their personal data and the ability to hold companies accountable for data breaches and misuse.[236]

### 9.2.4. Competition

Though the emerging vision of 6G includes 'security', 'inclusivity' and 'sustainability', it lacks a vision of a competitive 6G ecosystem. Promoting fair competition in the 6G ecosystem is very important for the interests of consumers and businesses alike. Thus, the 'competition' aspect needs to be reflected in the 6G vision.

It should be noted that most of the identified competition concerns in digital markets will directly or indirectly apply to 6G networks. In this regard, competition issues with respect to artificial intelligence and cloud services assume importance. Thus, there is a need to further study the interfaces of competition with AI and cloud services in the context of 6G networks.

Similarly, standard essential patents (SEPs) related to 6G can pose competition concerns. It would be wise to have national strategies on SEPs in the 6G context at the development stage itself. Lessons from China can be drawn in this regard.

In some countries, further consolidation in telecom and associated (such as AI/ML, cloud services) sectors may pose competition concerns in 6G. This would require vigorous M&A scrutiny in that jurisdiction.

Right technological intervention can lead to competitive markets. For instance, since interoperability has a pro-competition effect in markets, it would be advised to take this into account during the development and standardisation of 6G. Similarly, the incorporation of technologies like Open RAN can also have a pro-competition effect benefiting consumers at large.

### ***9.2.5. Trusted 6G Ecosystem***

To address the significant security challenges posed by the integration of 6G technology into both physical and digital realms, it is crucial to implement a robust security framework that embeds trust within 6G networks. Given the potential risks associated with 6G—ranging from personal data breaches to national security threats—a comprehensive approach to security that surpasses current standards is

essential. We recommend the development and implementation of an advanced security framework for 6G networks, which should include several key elements. Firstly, enhanced encryption and authentication protocols are needed to defend against both current and future threats, including those posed by quantum computing. Integrated physical security measures must be established to safeguard against threats that could compromise personal safety or property.

Additionally, the framework should incorporate advanced threat detection and response systems capable of identifying and mitigating sophisticated cyberattacks in real-time. Critical infrastructure components should be securely isolated to prevent cascading failures in the event of a breach. Continuous security audits and updates will be necessary to adapt to evolving threats and technological advancements. Prioritising the development of this security framework will ensure that 6G technology delivers its anticipated benefits while protecting individuals, organisations, and nations from potential security risks.

Moreover, it is essential to strengthen and promote multi-stakeholder collaboration. This collaboration should involve industry, academia, and civil society to ensure that diverse perspectives are incorporated and that consumer protection measures are effectively addressed. Furthermore, international cooperation and the establishment of global standards for secure 6G implementation are vital, addressing national security concerns while promoting global interoperability.

### 9.2.6. Inclusive and Sustainable 6G

*Expanding 6G Through Non-Terrestrial Networks:* Transitioning from 5G to 6G involves integrating Terrestrial Networks and Non-Terrestrial Networks (NTNs), including unmanned aerial vehicles (UAVs), high-altitude platform stations (HAPSs), and Low Earth Orbit (LEO) satellites. Particularly, LEO satellites, like CubeSats, are gaining prominence for their cost-effectiveness and potential for global connectivity. NTNs are crucial for bridging the digital divide by reaching remote areas where traditional infrastructure is lacking. They offer robust, independent connectivity, especially during infrastructure disruptions like natural disasters. For instance, SpaceX's Starlink aims to enhance global coverage and reduce latency through LEO satellites.

Key challenges for NTNs include managing latency, ensuring coverage, and addressing energy constraints. Overcoming these requires advancements in technologies such as solid-state lithium batteries, Gallium Nitride (GaN) components, and innovative spectrum allocation (e.g., millimetre-wave, Terahertz, optical bands). Enhanced antenna designs, like reconfigurable phased arrays and metasurface antennas, are also critical. Addressing these challenges will require collaboration among governments, industry, and research institutions. Effective management of satellite constellations

and protocols for satellite disposal is essential for sustainable and efficient NTNs. By tackling these issues, NTNs can significantly advance global connectivity and inclusivity.

*Harnessing Higher Frequencies and Multi-Access Edge Computing:* To bridge the digital divide and enhance 6G service delivery, focus on integrating higher frequency bands and Multi-Access Edge Computing (MEC) technologies. Exploiting Terahertz and optical bands can dramatically boost data rates and connectivity. Address the inherent challenges of severe path loss and high molecular absorption by deploying Intelligent Reflecting Surfaces (IRS). IRS can create virtual line-of-sight links, improving signal propagation. MEC is crucial for improving service delivery. By positioning computing resources closer to end-users, MEC reduces latency and boosts Quality of Service (QoS), enabling efficient resource use and tailored services. This is particularly effective for extending high-speed, low-latency services to underserved areas. For practical implementation, integrate IRS with higher frequency bands to tackle propagation issues and utilise MEC to enhance connectivity and service quality in regions with limited infrastructure.

*Sustainability and Cost-Effectiveness:* To ensure the responsible advancement of 6G technology, it is imperative that both higher frequency technologies and Multi-Access Edge Computing (MEC) solutions are designed with a strong emphasis on energy efficiency. Implementing strategies to minimise energy consumption and evaluating the environmental impact will be crucial in aligning with sustainability objectives. Specifically, focuses on developing and adopting energy-efficient technologies to mitigate the environmental footprint of 6G networks. Additionally, promote the reuse and recycling of 6G equipment to significantly reduce e-waste. Cost-effectiveness must also be a priority. Assess the financial viability of deploying higher frequency bands and MEC infrastructure to ensure that these advancements remain affordable. Leverage existing resources and infrastructure to optimise investments, thus ensuring that high-quality, equitable digital access is achieved across diverse regions. By integrating these principles, we can foster sustainable growth in 6G technology while bridging the digital divide effectively.

*Sustainable Digital Infrastructure:* To build a sustainable world and ensure global digital inclusion, it is crucial to implement a multifaceted approach. This involves supporting smart automation services worldwide, which can enhance efficiency and connectivity across various sectors. Equally important is developing connectivity solutions for global sensors that monitor environmental conditions, such as forests and oceans, to aid in ecological conservation. Promoting resource-efficient connected agriculture is another key element, optimising resource use and improving sustainability in farming practices. Universal access to digital personal healthcare should be prioritised to

ensure equitable healthcare services for all individuals. Additionally, facilitating access to high-end digital services for institutions like schools and hospitals, regardless of their location, is essential. Accelerating the transition to a circular resource economy can be achieved through global end-to-end life-cycle tracking of goods and the use of autonomous supply chains. This will help reduce waste and enhance recycling automation. Achieving these goals requires a network platform that offers global coverage with exceptional energy, material, and cost efficiency. Integrating embedded autonomous devices and sensors into the network is crucial.

### 9.2.7. Opportunities for India-Australia Collaboration

Global collaboration emerges as a cornerstone for establishing standards for and ensuring a trusted data flow, shaping the future telecommunications landscape with a focus on speed, security, sustainability, user experience, and global cooperation.[237] A trusted, open, and free cyberspace is essential for the development and prosperity of nations, particularly in the context of the Indo-Pacific region. As we look towards the potential implementation of 6G technology, there are numerous opportunities and challenges that both Australia and India need to consider. India and Australia share a mutual interest in developing an open, secure, free, and interoperable cyberspace.[238]

*Collaboration in emerging and critical technologies:* The deployment of 6G technology holds the promise of unprecedented data speeds, low latency, and enhanced connectivity, fuelling innovations in healthcare, education, and industry. A trusted cyberspace nurtures innovation, creating a favourable environment for startups, research institutions, and businesses to flourish. Opportunities abound for Australia and India to prioritise coordination and collaboration in standards-setting bodies. They can work closely on space security governance and actively engage in policy discussions in the Indo-Pacific concerning Artificial Intelligence, data policy standardisation, data protection, and data ethics.

Additionally, both countries should explore opportunities for public–private R&D projects, especially in AI and smart city development, supporting advancements in R&D and high-technology manufacturing. Collaboration on quantum projects, including quantum computing, is another avenue for partnership, involving government science institutions in pilot projects. Governments, with industry and civil society support, should invest in building a robust India–Australia technology partnership. Scholarships could play a pivotal role in fostering stronger research and development ties between the two nations, particularly focusing on areas like Quantum, AI, and space technologies. The programme could be initiated in India, gradually expanding to other countries, and be awarded in consultation with key scientific advisers.

*Economic Growth:* A secure and open cyberspace has the potential to drive the growth of the digital economy, generating new jobs and industries. Collaboration in cyberspace between Australia and India can result in joint research projects, technology exchanges, and mutually beneficial economic partnerships. In the realm of critical minerals, there is a commitment to fostering collaboration and enhancing cooperation. Both nations recognise the importance of diversifying the value/supply chains of critical minerals and applaud ongoing collaborative efforts in geoscientific research, bilateral businesses, and investments. To mitigate the risks of unreliable supply chains, Australia and India should explore a freer trading arrangement for critical minerals, enabling smooth collaboration between their private sectors and facilitating two-way investments. To strengthen critical-mineral cooperation, India may consider establishing an equivalent of Australia's Critical Minerals Facilitation Office, dedicated to collaboration with like-minded countries.

*National Security:* Ensuring national security involves bolstering cybersecurity through enhanced collaboration. Joint efforts on cybersecurity measures can fortify defence against cyber threats, safeguarding the sovereignty and security of both Australia and India. Additionally, robust cybersecurity measures are imperative for the protection of critical infrastructure, particularly communication networks, as they form the backbone of essential services. Strengthening this cooperation not only defends against potential cyberattacks but also contributes to overall national resilience and security. Regular information exchange and joint strategies will be essential in adapting to the evolving landscape of cyber threats and maintaining the integrity of critical systems.

*Diplomacy and Soft Power:* Championing a trusted and open cyberspace not only enhances the diplomatic standing of Australia and India globally but also serves as a potent source of soft power for both nations. Promoting the principles of openness and freedom in the digital realm adds to their influence and attractiveness on the world stage. Both countries are committed to collaborative efforts in strengthening mutual cooperation in various multilateral fora. This includes active participation in the United Nations, where they aim to contribute to the development of international standards, norms, and frameworks for cyberspace. By engaging in these multilateral discussions, Australia and India demonstrate their commitment to shaping a global digital landscape founded on shared values and principles, further solidifying their diplomatic influence and soft power in the international community. In this endeavour both countries can also benefit from the experiences of one another in their domestic norm settings.

### 9.2.9. Challenges for both the countries

*Cybersecurity Risks:* As technology evolves, cyber threats continue to advance, necessitating ongoing investments in cybersecurity measures by both Australia and India. To protect against malicious actors, a proactive approach is essential, involving the development and implementation of cutting-edge security technologies and strategies. In addition to the evolving threat landscape, ensuring the privacy of user data presents a critical challenge for both nations. Regulations must be robustly established and consistently enforced to safeguard personal information. These measures not only protect individuals from potential breaches but also contribute to building trust in the digital ecosystem. Beyond regulatory frameworks, public awareness and education campaigns can play a crucial role in fostering a culture of data privacy, empowering users to take an active role in protecting their personal information. This comprehensive approach will be essential in addressing the multifaceted challenges posed by cyber threats and data privacy concerns in the rapidly advancing technological landscape.

*Infrastructure Development:* The development and deployment of 6G infrastructure entail substantial investment, necessitating strategic planning in funding and infrastructure development for both Australia and India. Collaborative efforts in formulating comprehensive investment strategies will be crucial to ensure the successful establishment of advanced communication networks. Equitable access to cyberspace is a paramount consideration to prevent the creation or worsening of a digital divide within each nation and across the broader Indo-Pacific region. Both countries must work towards inclusive policies and initiatives that bridge the digital gap, fostering widespread access to the benefits of advanced technologies. This involves not only infrastructure development but also initiatives to promote digital literacy, skills training, and affordable connectivity solutions, thus ensuring that the advantages of 6G technology are accessible to all segments of society. A concerted focus on minimising the digital divide will contribute to societal development, economic growth, and technological advancement on a more inclusive and sustainable basis.

*Regulatory Framework:* Attempting a more harmonised set of standards is imperative for the development of 6G technology and cybersecurity. Both Australia and India need to collaboratively work towards developing common standards to ensure interoperability and seamless collaboration in the implementation of advanced technologies. In addition to standardisation, effective regulatory cooperation is crucial. Establishing robust regulatory frameworks, with a focus on cross-border collaboration, becomes essential to navigate challenges related to jurisdiction and legal frameworks. By aligning their regulatory approaches, both nations can create an environment that fosters innovation, encourages investment, and provides a clear and consistent legal

framework for the development and deployment of 6G technology. This collaborative regulatory effort is vital in navigating the complexities of the evolving technological landscape and promoting a conducive environment for the growth and success of advanced communication technologies.

*Geopolitical Considerations:* Navigating geopolitical dynamics while ensuring alignment between cyberspace policies and broader international relations is a nuanced challenge. Both Australia and India must carefully navigate this intersection to maintain diplomatic harmony and global cooperation in the digital realm. Moreover, collaboration with like-minded nations is crucial. Australia and India should actively engage with their allies to address shared challenges in cyberspace governance. This collaborative approach promotes a unified front, facilitating the establishment of international norms, standards, and protocols. By coordinating efforts with other nations that share common values and interests, Australia and India can contribute to the development of a cohesive and inclusive global cyberspace governance framework. This collaborative stance enhances cybersecurity, fosters innovation, and strengthens the influence of both countries in shaping the future of the digital landscape on the world stage.

# References

IBM (2020). Available at: IBM Report: Cost of a Data Breach Hits Record High During Pandemic accessed on 26 Aug 2023.

Internet Society (2022). Available at: India CERT-In Cybersecurity Directions 2022 (internetsociety.org) accessed on 26 Aug 2023.

Sridhar, V. (2019). Emerging ICT Policies and Regulations: Roadmap to Digital Economies. Springer Nature. E-Book ISBN: ISBN 978-981-329-022-8; Hardcover ISBN: 978-981-329-021-1.

Computer Emergency Response Team – India (CERT-IN). (28 Apr 2022). Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

Council of Europe (CoE). (2001). European Treaty Series 185 - Convention on Cyber Crime, Budapest. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf accessed on 12 Feb 2019.

Hui, Kai-Lung; KIM, Seung Hyun; and WANG, Qiu-Hong. Cybercrime deterrence and inter-national legislation: Evidence from distributed denial of service attacks. (2017).MIS Quarterly. 41, (2), 497-523. Research Collection School Of Information Systems. Availa-ble at: http://ink.library.smu.edu.sg/sis_research/3420 Accessed on 12 Feb 2018.

IBM. (2018). Cost of a data breach study: Global overview. Available at: https://www.ibm.com/security/data-breach accessed on 15 Oct 2018.

Indian Common Criteria Certification Scheme (IC3S) . (2018). Available at: http://www.commoncriteria-india.gov.in/Pages/CCSOverview.aspx accessed on 11 Dec 2018.

Karnataka Jnana Ayoga (KJA), Government of Karnataka. (2019). Karnataka Cyber Security Vision 2025.

Ministry of Electronics and Information Technology (MeitY), Government of India, (2008). The Information Technology Act (Amended 2008).

Ministry of Electronics and Information Technology (MeitY), Government of India, (2013). National Cyber Security Policy 2013. Available at: https://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf accessed on 2 Mar 2019.

Ministry of Electronics and Information Technology (MeitY), Government of India, (2018). The Information Technology: Intermediaries Guidelines (Amendment) Rules] 2018.

The Information Technology: Intermediaries Guidelines (Amendment) Rules] 2018.

National Critical Information Infrastructure Protection Centre (NCIIPC). (2017). NCIIPC: Standard Operating Procedures. Available at: http://nciipc.gov.in/documents/SOP-CII.pdf ac-cessed on 14 Sep 2018.

National Institute of Standards and Technology (NIST). (2018). Cyber security is everyone's job. Available at: https://www.nist.gov/sites/default/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf accessed on 9 June 2019.

Tan. E. E. (2018). Cyber Deterrence in Singapore : Framework & Recommendations. (RSIS Working Paper, No. 309). Singapore: Nanyang Technological University.

U.S. Computer Emergency Readiness Team (US-CERT). Available at: https://www.us-cert.gov/about-us accessed on 11 Feb 2019.

Woollaston, V. (2017, May 15). The NHS trusts and hospitals affected by the Wannacry cyberattack. WIRED. Retrieved from http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack accessed on 10 Feb 2019.

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. WIRED. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ accessed on 10 Feb 2019.

British Broadcasting Corporation (BBC). (14 May 2021). US fuel pipeline 'paid hackers $5m in ransom. Available at: https://www.bbc.com/news/business-57112371, accessed 11 Sep 2023.

# Endnotes

1 Ethics Frameworks - IEEE TechEthics, available at: https://techethics.ieee.org/ethics-frameworks/

2 What is Telecom Ethics?, available at: https://insidetelecom.com/what-is-telecom-ethics/

3 Top 10 risks for telecommunications in 2024, available at: https://www.ey.com/en_no/telecommunications/top-10-risks-for-telecommunications

4 6G Network Dangers: 7 Tips for Mitigating Future Concerns, available at: https://www.6gworld.com/blog/6g-network-dangers-7-tips-for-mitigating-future-concerns/

5 AI and 6G Security: Opportunities and Challenges, available at: https://www.researchgate.net/publication/350824466_AI_and_6G_Security_Opportunities_and_Challenges

6 6G Cybersecurity: Risks Need to Be Mitigated Before 6G Arrives, available at: https://www.linkedin.com/pulse/6g-cybersecurity-risks-need-mitigated-before-arrives-charles-alexi-z0sue

7 Security concerns on machine learning solutions for 6G networks in mmWave beam prediction, available at: https://www.sciencedirect.com/science/article/pii/S1874490722000155

8 Security Requirements and Challenges of 6G Technologies and Applications, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8914636/

9 6G Cybersecurity: Risks Need to Be Mitigated Before 6G Arrives, available at: https://www.linkedin.com/pulse/6g-cybersecurity-risks-need-mitigated-before-arrives-charles-alexi-z0sue

10 6G Security Threat Landscape, available at: https://www.researchgate.net/figure/6G-Security-Threat-Landscape_fig2_351275174

11 Post-quantum Cryptography in 6G, available at: http://jultika.oulu.fi/files/nbnfi-fe202201178891.pdf

12 Generative AI for Cyber Threat-Hunting in 6G-enabled IoT Networks, available at: https://arxiv.org/abs/2303.11751#:~:text=Generative%20Artificial%20Intelligence%20(AI)%20can,in%206G%2Denabled%20IoT%20networks.

13 DLT architectures for trust anchors in 6G, available at: https://link.springer.com/article/10.1007/s12243-022-00941-8

14 Security Requirements and Challenges of 6G Technologies and Applications, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8914636/

15 Security and privacy in 6G networks: New areas and new challenges, available at: https://www.sciencedirect.com/science/article/pii/S2352864820302431

16 AI and 6G Security: Opportunities and Challenges, available at: http://jultika.oulu.fi/files/nbnfi-fe2021102051685.pdf

17 Network Generations and the Security Challenge in IoT Applications, available at: https://arxiv.org/abs/2201.01927

[18] Security Requirements and Challenges of 6G Technologies and Applications, available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8914636/

[19] Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN, available at: https://www.sciencedirect.com/science/article/abs/pii/S1389128622003929

[20] A Survey on Privacy for B5G/6G: New Privacy Challenges, and Research Directions, available at: https://arxiv.org/pdf/2203.04264.pdf

[21] Transnational Cybercrime: Issue of Jurisdiction, available at: https://www.ijlmh.com/paper/transnational-cybercrime-issue-of-jurisdiction/

[22] Telecom Cyber Security Rules 2024.pdf

[23] Home Ministry pitches for Budapest Convention on cyber security | India News - The Indian Express

[24] https://dot.gov.in/circulars/draft-telecommunications-critical-telecommunication-infrastructure-rules-2024

[25] http://www.commoncriteria-india.gov.in/overview.php

[26] Proposed Digital India Act 2023, available at: https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

[27] Draft Digital India Act will regulate emerging technologies to protect citizens: Rajeev Chandrasekhar, available at: https://www.thehindubusinessline.com/info-tech/draft-digital-india-act-will-regulate-emerging-technologies-to-protect-citizens-rajeev-chandrasekhar/article66960829.ece

[28] Cybersecurity bill to clearly define contours of online safety, security, available at: https://government.economictimes.indiatimes.com/news/governance/cybersecurity-bill-to-clearly-define-contours-of-online-safety-security/102012099

[29] Privacy Act 1988, available at: https://www.legislation.gov.au/Series/C2004A03712

[30] The Crimes Act 1914, available at: https://www.counterfraud.gov.au/library/crimes-act-1914#:~:text=The%20Crimes%20Act%20sets%20out,criminal%20offences%20and%20related%20matters.

[31] Cyber Security, available at: https://www.asd.gov.au/cyber-security

[32] 2023-2030 Australian Cyber Security Strategy, available at: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

[33] Cdr-Subhash-Dutta-Review-of-the-Australian-Cybersecurity-Strategy-2023.pdf (maritimeindia.org)

[34] Cyber Security Legislative Package 2024, available at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/CyberSecurityPackage

[35] https://arpi.org.au/wp-content/uploads/2024/11/Sub-3-Australian-Risk-Policy-Institute-As-Published-by-PJCIS.pdf

[36] 6G CONCEPTS AND WHAT THEY MEAN FOR SECURITY, available at: https://go.abiresearch.com/hubfs/Marketing/Whitepapers/Conceptualizing%20Security%20in%20a%206G%20World/Conceptualizing%20Security%20in%20a%206G%20World.pdf

[37] 6G starts to take shape with AI, open vRAN integration and ever increased security, available at: https://symphony.rakuten.com/blog/6g-starts-to-take-shape

[38] 6G CONCEPTS AND WHAT THEY MEAN FOR SECURITY, available at: https://go.abiresearch.com/hubfs/Marketing/Whitepapers/Conceptualizing%20Security%20in%20a%206G%20World/Conceptualizing%20Security%20in%20a%206G%20World.pdf

[39] 6G starts to take shape with AI, open vRAN integration and ever increased security, available at: https://symphony.rakuten.com/blog/6g-starts-to-take-shape

[40] 6G CONCEPTS AND WHAT THEY MEAN FOR SECURITY, available at: https://go.abiresearch.com/hubfs/Marketing/Whitepapers/Conceptualizing%20Security%20in%20a%206G%20World/Conceptualizing%20Security%20in%20a%206G%20World.pdf

[41] The brave new terabyte broadband world of 6G is coming, but not just yet, available at: https://techcrunch.com/2023/02/28/the-brave-new-terabyte-broadband-world-of-6g-is-coming-but-not-just-yet/

[42] Quantum for 6G communication: A perspective, available at: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/qtc2.12060

[43] Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default, available at: https://www.cisa.gov/resources-tools/resources/secure-by-design

[44] Joint Statement Endorsing Principles for 6G: SECURE, OPEN & RESILIENT BY DESIGN | National Telecommunications and Information Administration

[45] The Roadmap to 6G: AI Empowered Wireless Networks, available at: https://ieeexplore.ieee.org/document/8808168

[46] 6G starts to take shape with AI, open vRAN integration and ever increased security, available at: https://symphony.rakuten.com/blog/6g-starts-to-take-shape

[47] 6G CONCEPTS AND WHAT THEY MEAN FOR SECURITY, available at: https://go.abiresearch.com/hubfs/Marketing/Whitepapers/Conceptualizing%20Security%20in%20a%206G%20World/Conceptualizing%20Security%20in%20a%206G%20World.pdf

[48] Bharat 6G Vision Document, available at: https://dot.gov.in/sites/default/files/Bharat%206G%20Vision%20Statement%20-%20full.pdf

[49] Cyber security: India must update digital infrastructure, legal framework, available at: https://www.policycircle.org/opinion/cyber-security-digital-india/

[50] Security and privacy for 6G: A survey on prospective technologies and challenges. 2021. Available at https://arxiv.org/pdf/2108.11861.pdf

[51] Security for 5G and Beyond. 2019. Available at https://ieeexplore.ieee.org/document/8712553

[52] W. Saad, M. Bennis, & M. Chen. 2020. A vision of 6g wireless systems: Applications, trends, technologies, and open research problems. IEEE Network. Available at https://ieeexplore.ieee.org/document/8869705

[53] S. Zhang and D. Zhu. 2020. Towards artificial intelligence enabled 6g: State of the art, challenges, and opportunities. Computer Networks. Available at https://www.sciencedirect.com/science/article/abs/pii/S138912862031207X

[54] Toward Data Security in 6G Networks: A Public-Key Searchable Encryption Approach. 2022. Available at https://ieeexplore.ieee.org/document/9919764

[55] Security and privacy in 6G networks: New areas and new challenges. 2020. Available at https://www.sciencedirect.com/science/article/pii/S2352864820302431

[56] From gadget to gadget-free hyperconnected world: Conceptual analysis of user privacy challenges. 2017 European Conference on Networks and Communications, Oulu. Available at https://ieeexplore.ieee.org/document/7980650

[57] General Data Protection Regulation (GDPR). Available at https://gdpr-info.eu/

[58] Digital Personal Data Protection Act, 2023. Available at https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[59] Estimating the success of re-identifications in incomplete datasets using generative models. 2019. Nature Communications. Available at https://www.nature.com/articles/s41467-019-10933-3

[60] Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities. 2020. Available at https://www.sciencedirect.com/science/article/abs/pii/S138912862031207X

[61] 6G White Paper: Research Challenges For Trust, Security And Privacy. 2020. Available at https://oulurepo.oulu.fi/bitstream/handle/10024/36805/isbn978-952-62-2680-4.pdf?sequence=1&isAllowed=y

[62] TC 1/WG 11 (Smart cities) Strategic White Paper. 2019. Smart City: Privacy guidelines for smart cities. Available at https://www.iso.org/standard/71678.html

[63] Privacy by Design. 2014. Available at https://www.edps.europa.eu/data-protection/our-work/subjects/privacy-design_en?page=5#:~:text=Data%20protection%20by%20design%20aims,comply%20with%20data%20protection%20principles.

[64] 6G White Paper: Research Challenges For Trust, Security And Privacy. 2020. Available at https://oulurepo.oulu.fi/bitstream/handle/10024/36805/isbn978-952-62-2680-4.pdf?sequence=1&isAllowed=y

[65] Deloitte 2023 Telecom Industry Outlook, https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/telecommunications-industry-outlook.html

[66] For more details on Network Effect: What it is, How it works, Pros and Cons, see: https://www.investopedia.com/terms/n/network-effect.asp

[67] Regulation, Market Structure and Performance in Telecommunications, OECD Economic Studies No. 32, 2002/I, https://www.oecd.org/economy/outlook/2736298.pdf

[68] https://www.accc.gov.au/by-industry/telecommunications-and-internet/telecommunications-monitoring and https://www.accc.gov.au/about-us/publications/serial-publications/accc-communications-market-report/accc-communications-market-report-2021-22

[69] Market Study on the Telecom Sector in India – Key Findings and Observations (22 January 2021), https://www.cci.gov.in/images/marketstudie/en/market-study-on-the-telecom-sector-in-india1652267616.pdf

[70] In December 2018, the Supreme Court finally ended the jurisdictional conflict between CCI and TRAI. By invoking the doctrine of harmonious construction, the court balanced the scales and gave

the TRAI the power to first determine the rights and obligations of parties, after which – if the TRAI believes that anti-competitive activity has occurred – the CCI's jurisdiction can be invoked. See, *CCI v. Bharti Airtel Limited and Others*, AIR 2019 SC 113

71 *Bharti Airtel Ltd. v. Reliance Industries Ltd. & Anr*., CCI Case No. 03/2017

72 https://www.accc.gov.au/business/competition-and-exemptions/cartels

73 *Neeraj Malhotra v. Deustche Post Bank Home Finance Ltd. & Ors*., Case No. 5/2009

74 Telcos collude to keep Australia online – ACCC winds back anti-cartel controls (7 April 2020) https://ia.acs.org.au/article/2020/telcos-collude-to-keep-australia-online.html

75 India: CCI's Market Study On The Telecom Sector – An Overview (18 February 2021), https://www.mondaq.com/india/antitrust-eu-competition-/1037960/cci%60s-market-study-on-the-telecom-sector--an-overview

76 Telstra Corporation Limited and TPG Telecom Limited proposed spectrum sharing, https://www.accc.gov.au/public-registers/mergers-registers/merger-authorisations-register/telstra-corporation-limited-and-tpg-telecom-limited-proposed-spectrum-sharing

77 Anti-trust watchdog blocks $11 billion merger of Vodafone's Australian business with TPG Telecom (8 May 2019), https://www.reuters.com/article/vodafone-group-m-a-tpg-telecom-idINKCN1SE0XT

78 ACCC will not appeal against Vodafone Hutchison Australia-TPG Telecom merger (5 March 2020) https://www.accc.gov.au/media-release/accc-will-not-appeal-federal-court's-decision-to-allow-tpg-vodafone-merger

79 SEPs are patents that claim an invention that must be used to comply with a chosen industry standard. Any person or organization in the relevant industry must use the SEP in order to comply with the relevant industry standards.

80 India: SEPs and FRAND – litigation, policy and latest developments (2 December 2022) https://globalcompetitionreview.com/hub/sepfrand-hub/2022/article/india-seps-and-frand-litigation-policy-and-latest-developments

81 Section 3(5)(ii) of the Competition Act. In contrast in Australia, with the repeal of section 51(3) of the Competition and Consumer Act, 2010 (CCA), effective since 13 September 2019, there are no intellectual property exemptions under the CCA, which may have previously applied to the licensing of SEPs. See for further details: https://www.accc.gov.au/about-us/publications/guidelines-on-the-repeal-of-subsection-513-of-the-competition-and-consumer-act-2010-cth

82 Alexander Raskovich, Self-Regulation in Standard-Setting Organizations: Frand Royalties in the Process of Discovering Standards, George Mason Law & Economics Research Paper No. 22-37

83 Fair, reasonable, and non-discriminatory (FRAND) licensing terms, EC JRC Science and Policy Report (2015), https://publications.jrc.ec.europa.eu/repository/handle/JRC96258

84 FRAND terms are typically made to standard-setting organizations such as the European Telecommunications Standards Institute.

85 A patent hold-up undermines the competitive process of choosing among technologies and thus threatens the integrity of standard setting activities.

[86] Chapter 31 Standard Essential Patents and FRAND Licensing: The Evolution of the European Approach, (May 2023), https://academic.oup.com/book/46572/chapter/408282982

[87] Australia: Current snapshot of the licensing of SEPs (Standard Essential Patents) in Australia, (23 September 2019), https://www.mondaq.com/australia/patent/847418/current-snapshot-of-the-licensing-of-seps-standard-essential-patents-in-australia

[88] *Ibid*. A compulsory license has never been granted in Australia and it is yet to be seen how the Australian court will apply this provision in relation to the licensing of SEPs and otherwise.

[89] Geeta Gouri, Competition Law and Standard Essential Patent (SEP) in India: A Few Critical Issues to Ponder (24 July 2018), https://link.springer.com/chapter/10.1007/978-981-13-1232-8_12

[90] *Micromax Informatics Limited v Telefonaktiebolaget LM Ericsson (Publ)*, CCI Case 50/2013; *Intex Technologies (India) Limited v Telefonaktiebolaget LM Ericsson (Publ)*, CCI Case 76/2013

[91] India: SEPs and FRAND – litigation, policy and latest developments (2 December 2022) https://globalcompetitionreview.com/hub/sepfrand-hub/2022/article/india-seps-and-frand-litigation-policy-and-latest-developments

[92] *Koninklijke Philips v. Rajesh Bansal*, CS (COMM) 24/2016 and *Koninklijke Philips v. Bhagirathi Electronics*, CS (COMM) 436/2017

[93] Recent Indian Case Law on Standard Essential Patents (4 June 2021), https://patentblog.kluweriplaw.com/2021/06/04/recent-indian-case-law-on-standard-essential-patents/

[94] I.A. 8772/2020 in CS (COMM) 295/2020

[95] Monsanto Holdings Private Limited & Ors vs Competition Commission Of India & Ors, Delhi High Court (13 July, 2023); https://indiankanoon.org/doc/150896661/

[96] https://www.chinaiplawupdate.com/2024/11/chinas-state-administration-for-market-regulation-releases-anti-monopoly-guidelines-in-the-field-of-standard-essential-patents/

[97] https://english.www.gov.cn/news/202411/09/content_WS672ef275c6d0868f4e8ecc4d.html

[98] Article 3 of the Antimonopoly Guidelines on Standard Essential Patents (SEP), 2024

[99] Case C-170/13

[100] An EC Communication on SEPs – Not More Not Less, (30 November 2017) https://www.antitrustlawblog.com/2017/11/articles/intellectual-property-antitrust/ec-communication-frand/

[101] Standard Essential Patents, https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/patent-protection-eu/standard-essential-patents_en

[102] While the US Department of Justice Antitrust Division and the Federal Trade Commission share responsibility for investigating and litigating cases under the Sherman Act, 1890, decisions *re* antitrust violations are taken by federal courts that entertain disputes under all laws, specialized and general.

[103] Pro-competition regulation in the Digital Economy: The United Kingdom's Digital Markets Unit, The Antitrust Bulletin (2022) Vol. 67(2) 341-366, https://journals.sagepub.com/doi/full/10.1177/0003603X221082733

[104] All you need to know about network interoperability (23 May 2016), https://www.comviva.com/blog/references/all-you-need-to-know-about-network-interoperability-comviva/

[105] Interoperability is fundamental to the internet, https://www.newamerica.org/oti/reports/promoting-platform-interoperability/interoperability-is-fundamental-to-the-internet/

[106] Nathan Cranford, The role of network interoperability in telecommunications (19 April 2018), https://www.rcrwireless.com/20180419/fundamentals/the-role-of-network-interoperability-in-telecommunications

[107] Interoperability FAQs, https://www.heavy.ai/technical-glossary/interoperability

[108] Open RAN Security Report (22 May 2023), https://www.ntia.gov/report/2023/open-ran-security-report

[109] Summary of Open RAN Security Report, https://ntia.gov/sites/default/files/publications/summary_of_open_ran_security_report_0.pdf

[110] Mike Dano, Open RAN is mostly secure, finds government report (22 May 2023), https://www.lightreading.com/open-ran/open-ran-is-mostly-secure-finds-government-report

[111] Ofcom Cloud Services Market Research: Summary of Findings (March 2023), https://www.ofcom.org.uk/__data/assets/pdf_file/0031/256459/context-consulting-cloud-services-market-research-summary-of-findings.pdf

[112] Interoperability and Portability for Cloud Computing: A Guide (December 2017), https://www.omg.org/cloud/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf

[113] This has been summarised based on the findings of Ofcom's market study as well as cases filed before the European Commission)

[114] Cloud services in the competition law spotlight (25 October 2022), https://www.solicitorsjournal.com/sjarticle/cloud-services-in-the-competition-law-spotlight?pass=505953

[115] Statistica, Big Three Dominate the Global Cloud Market (28 April 2023), https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

[116] *Id.,* refer to chart on the worldwide market share of leading cloud infrastructure service providers in Q1 2023

[117] Unfair Software Licensing Practices: A quantification of the cost for cloud customers by Prof. Frederic Jenny for CISPE dated 21 June 2023, https://cispe.cloud/new-study-links-unfair-software-licences-to-distortion-of-competition-in-cloud-infrastructure-market/

[118] Ibid., pg. 3

[119] Ibid., pg. 13

[120] Ibid., Figure 7 (*Market Share for IaaS*), pg. 47

[121] An Inquiry into Cloud Computing Business Practices: The FTC is seeking public comments (22 March 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/inquiry-cloud-computing-business-practices-federal-trade-commission-seeking-public-comments

[122] What FTC learnt (16 November 2023) https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/cloud-computing-rfi-what-we-heard-learned

[123] Ofcom Study, Cloud Services Market Research - Summary of Findings, p.12, https://www.ofcom.org.uk/__data/assets/pdf_file/0031/256459/context-consulting-cloud-services-market-research-summary-of-findings.pdf. Ofcom initiated the study on 6 October 2022.

[124] *Id.*, p. 56

[125] Ofcom refers to UK CMA (5 October 2023), https://www.ofcom.org.uk/news-centre/2023/ofcom-refers-uk-cloud-market-to-cma-for-investigation

[126] EC Press Release (27 July 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3991

[127] https://economictimes.indiatimes.com/news/international/business/european-commission-preparing-formal-complaint-against-microsoft-teams-video-app/articleshow/103766255.cms

[128] https://brusselssignal.eu/2023/12/ec-actively-investigating-possible-cloud-computing-cartels/

[129] Microsoft under fire in Europe for OneDrive bundling; legal fight brewing (29 November 2021), https://www.computerworld.com/article/3642834/microsoft-under-fire-in-europe-for-onedrive-bundling-legal-fight-brewing.html

[130] Microsoft kickstarts settlement discussions with European cloud companies over antitrust complaints (20 April 2023) https://techcrunch.com/2023/04/20/microsoft-kickstarts-settlement-discussions-with-european-cloud-trade-body-over-antitrust-complaints/

[131] Cloud computing: The Autorité de la concurrence issues an opinion on certain provisions of the draft law to secure and regulate the digital space (12 May 2023), https://www.autoritedelaconcurrence.fr/en/press-release/cloud-computing-autorite-de-la-concurrence-issues-opinion-certain-provisions-draft

[132] Dutch ACM, Market Study Cloud Services (5 September 2022) https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf

[133] *Id.*

[134] KFTC Announces Results of Cloud Sector Survey (28 December 2022), https://www.kimchang.com/en/insights/detail.kc?sch_section=4&idx=26451

[135] JFTC Report Regarding Cloud Services (28 June 2022), https://www.jftc.go.jp/en/pressreleases/yearly-2022/June/220628.html

[136] JFTC Summary of Report Regarding Cloud Services, https://www.jftc.go.jp/en/pressreleases/yearly-2022/June/220628_2EN.pdf

[137] Herwig C.H. Hofmann and Isabella Lorenzoni, Future Challenges for Automation in Competition Law Enforcement (Stanford Computational Antitrust 2023), https://law.stanford.edu/wp-content/uploads/2023/04/hofmann-lorenzoni.pdf

[138] Gera van Duijvenvoorde, Artificial Intelligence and European Competition Law: Identifying Principles for a Fair Market (6 July 2022), https://link.springer.com/chapter/10.1007/978-94-6265-523-2_19

[139] Sameer Gupta and Sankalp Udgata, Rethinking the Contours of Competition Law: The AI Perspective (5 September 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3444343

[140] Robert Van De Mark, Book Review - Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy by Ariel Ezrachi & Maurice E. Stucke, https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=3297&context=ohlj

[141] Ivaldi M., B. Jullien, P. Rey, P. Seabright and J. Tirole (2003), The Economics of Tacit Collusion, Final Report for DG Competition, European Commission, http://ec.europa.eu/competition/mergers/studies_reports/the_economics_of_tacit_collusion_en.pdf

[142] OECD (2017), Algorithms and Collusion: Competition Policy in the Digital Age, https://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm

[143] Competition Law and AI, https://www.oecd-ilibrary.org/sites/3acbe1cd-en/index.html?itemId=/content/component/3acbe1cd-en

[144] On 4 July 2023, in Conditions générales d'utilisation d'un réseau social - Case C-252/21, (https://curia.europa.eu/juris/liste.jsf?num=C-252/21), the European Court of Justice confirmed that an infringement of data protection rules (e.g. requiring justifications or consent for the processing of personal data), may be an abuse of dominance if carried out by a dominant firm.

[145] Andreas von Bonin and Sharon Malhi, The Use of Artificial Intelligence in the Future of Competition Law Enforcement, Journal of European Competition Law & Practice, (2020) Vol. 11, No. 8

[146] In 2016, the CMA fined several undertakings for agreeing not to undercut each other's prices for posters and frames sold online and implemented this agreement by using automated pricing software. See, CMA press release - CMA issues final decision in online cartel case, https://www.gov.uk/government/news/cma-issues-final-decision-in-online-cartel-case

[147] AI and Competition Law, Hogan Lovells (31 August 2023), https://www.lexology.com/library/detail.aspx?g=c8c06367-e23f-48a9-a814-fc9548a67137

[148] CMA press release - CMA launches initial review of artificial intelligence models (4 May 2023), https://www.gov.uk/government/news/cma-launches-initial-review-of-artificial-intelligence-models

[149] Generative AI raises Competition Concerns (29 June 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns

[150] https://competition-policy.ec.europa.eu/about/news/joint-statement-competition-generative-ai-foundation-models-and-ai-products-2024-07-23_en

[151] https://www.accc.gov.au/media-release/final-digital-platforms-report-to-focus-on-global-developments-and-emerging-competition-and-consumer-issues#:~:text=The%20ACCC%20also%20proposes%20to,Large%20Language%20Models%20(LLMs).

[152] https://fst.net.au/government-news/accc-digital-platforms-report-to-investigate-competition-risks-in-ai/

[153] https://treasury.gov.au/sites/default/files/2024-10/c2024-584560-dp.pdf

[154] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2054673

[155] Consumer Protection | COMMUNICATIONS — Telecommunications

[156] Standards Build Trust: How the International Telecommunication Union Supports Inclusive Sustainable Development | United Nations

[157] Consumer protection and e-commerce

[158] Electronic Commerce | United Nations Commission On International Trade Law

[159] Telecommunications and internet | ACCC

[160] ACCC Statement of Intent – Telecommunications-related functions

[161] ACCC Statement of Intent – Telecommunications-related functions

[162] Telecommunications Consumer Protections Code | ACMA

[163] India, Australia should work together on critical 6G technology: Barry O' Farrell, ET Telecom

[164] Telecommunications Consumer Protections Code | ACMA

[165] Federal Register of Legislation - Telecommunications (Consumer Protection and Service Standards) (Accessible Standard Telephone Services) Regulations 2023

[166] New telco consumer safeguards bill introduced to Parliament | Ministers for the Department of Infrastructure

[167] Consumer Protection | Telecom Regulatory Authority of India

[168] India, Australia should work together on critical 6G technology: Barry O' Farrell, ET Telecom

[169] Telecom Act: What are consumer protections

[170] Telecommunications Act 2023

[171] https://pib.gov.in/PressReleasePage.aspx?PRID=1642422

[172] https://telecoms.com/opinion/the-rising-significance-of-trust-in-the-digital-world/

[173] 6G White paper: Research challenges for Trust, Security and Privacy

[174] https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

[175] Advancing Digital Safety: A Framework to Align Global Action

[176] https://www.weforum.org/platforms/the-centre-for-cybersecurity

[177] https://gdpr.eu/what-is-gdpr/

[178] https://www.newyorker.com/tech/annals-of-technology/the-hidden-costs-of-automated-thinking;

[179] https://www.iso.org/standard/60544.html

[180] https://www.wired.com/story/movement-hold-ai-accountable-gains-steam/

[181] https://hbr.org/2019/04/why-anxious-customers-prefer-human-customer-service

[182] https://www.atlanticcouncil.org/in-depth-research-reports/report/specifying-normative-content/

[183] Explained: What new 'trusted telecom' rules mean for telcos using Chinese equipment | Explained News - The Indian Express

[184] Criteria for Security and Trust in Telecommunications Networks and Services

[185] Trusted Network Communications

[186] 5G zero trust – a zero-trust architecture for telecom

[187] Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN

[188] Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN

[189] Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN

[190] 5G zero trust – a zero-trust architecture for telecom

[191] Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN

[192] 5G zero trust – a zero-trust architecture for telecom

[193] Digital Economy Report 2021 | UNCTAD

[194] G20 Members' Regulations of Cross-Border Data Flows

[195] Operationalizing Data Free Flow with Trust (DFFT)

[196] A Preliminary Mapping of Data Localisation Measures | OECD Trade Policy Papers

[197] MINISTERIAL DECLARATION G7 Digital Ministers' meeting

[198] G20 Bali Leaders' Declaration | The White House

[199] G20 New Delhi Leaders' Declaration

[200] https://press.un.org/en/2021/dsgsm1579.doc.htm

[201] https://www.gsma.com/r/wp-content/uploads/2023/10/The-State-of-Mobile-Internet-Connectivity-Report-2023.pdf

[202] https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

[203] https://www.trai.gov.in/sites/default/files/Cons_P_14092023.pdf

[204] https://www.itu.int/en/mediacentre/Pages/pr27-2020-facts-figures-urban-areas-higher-internet-access-than-rural.aspx

[205] https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2022/ITU_Price_Brief_2022.pdf

[206] Van Dijk, J.A. Digital divide: Impact of access. In The International Encyclopedia of Media Effects; Wiley: Hoboken, NJ, USA, 2017; pp. 1–11.

[207] https://www.eib.org/attachments/publications/unlocking_digital_connectivity_in_africa_en.pdf

[208] https://www.gsma.com/r/wp-content/uploads/2021/06/The-Mobile-Gender-Gap-Report-2021.pdf

[209] https://www.trai.gov.in/sites/default/files/Cons_P_14092023.pdf

[210] https://www.digitalinclusionindex.org.au/wp-content/uploads/2023/07/ADII-2023-Summary_FINAL-Remediated.pdf

[211] Rinaldi, F.; Maattanen, H.L.; Torsner, J.; Pizzi, S.; Andreev, S.; Iera, A.; Koucheryavy, Y.; Araniti, G. Non-Terrestrial Networks in 5G & Beyond: A Survey. IEEE Access 2020, 8, 165178–165200.

[212] Polese, M.; Jornet, J.M.; Melodia, T.; Zorzi, M. Toward end-to-end, full-stack 6G terahertz networks. IEEE Commun. Mag. 2020, 58, 48–54.

[213] Wu, Q.; Zhang, R. Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network. IEEE Commun. Mag. 2019, 58, 106–112.

[214] Mu, X.; Liu, Y.; Guo, L.; Lin, J.; Poor, H.V. Intelligent reflecting surface enhanced multi-UAV NOMA networks. IEEE J. Sel. Areas Commun. 2021, 39, 3051–3066.

[215] Zaidi, Z.; Friderikos, V.; Yousaf, Z.; Fletcher, S.; Dohler, M.; Aghvami, H. Will SDN be part of 5G? IEEE Commun. Surv. Tutor. 2018, 20, 3220–3258.

[216] Zhang, S.; Liu, J.; Guo, H.; Qi, M.; Kato, N. Envisioning device-to-device communications in 6G. IEEE Netw. 2020, 34, 86–91.

[217] Jameel, F.; Hamid, Z.; Jabeen, F.; Zeadally, S.; Javed, M.A. A survey of device-to-device communications: Research issues and challenges. IEEE Commun. Surv. Tutor. 2018, 20, 2133–2168.

[218] https://www.frontiersin.org/journals/communications-and-networks/articles/10.3389/frcmn.2022.785933/full

[219] Taleb, T.; Samdanis, K.; Mada, B.; Flinck, H.; Dutta, S.; Sabella, D. On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. IEEE Commun. Surv. Tutor. 2017, 19, 1657–1681.

[220] Saarnisaari, H.; Dixit, S.; Alouini, M.S.; Chaoub, A.; Giordani, M.; Kliks, A.; Matinmikko-Blue, M.; Zhang, N.; Agrawal, A.; Andersson, M.; et al. A 6G white paper on connectivity for remote areas. arXiv 2020, arXiv:2004.14699.

[221] https://www.sciencedirect.com/science/article/pii/S2405959522000996

[222] https://arxiv.org/pdf/2009.04175

[223] https://arxiv.org/pdf/2009.04175

[224] Kato, N.; Mao, B.; Tang, F.; Kawamoto, Y.; Liu, J. Ten challenges in advancing machine learning technologies toward 6G. IEEE Wirel. Commun. 2020, 27, 96–103.

[225] Saad, W.; Bennis, M.; Chen, M. A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Netw. 2019, 34, 134–142.

[226] https://www.6gflagship.com/white-paper-on-6g-drivers-and-the-un-sdgs/

[227] https://www.ngmn.org/work-programme/ngmn-6g-drivers-and-vision.html

[228] Navigating 6G Security Challenges and Potential Solutions

[229] Security Requirements and Challenges of 6G Technologies and Applications - PMC

[230] https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/26/joint-statement-endorsing-principles-for-6g-secure-open-and-resilient-by-design/

[231] Navigating 6G Security Challenges and Potential Solutions

[232] Security Requirements and Challenges of 6G Technologies and Applications - PMC

[233] Navigating 6G Security Challenges and Potential Solutions

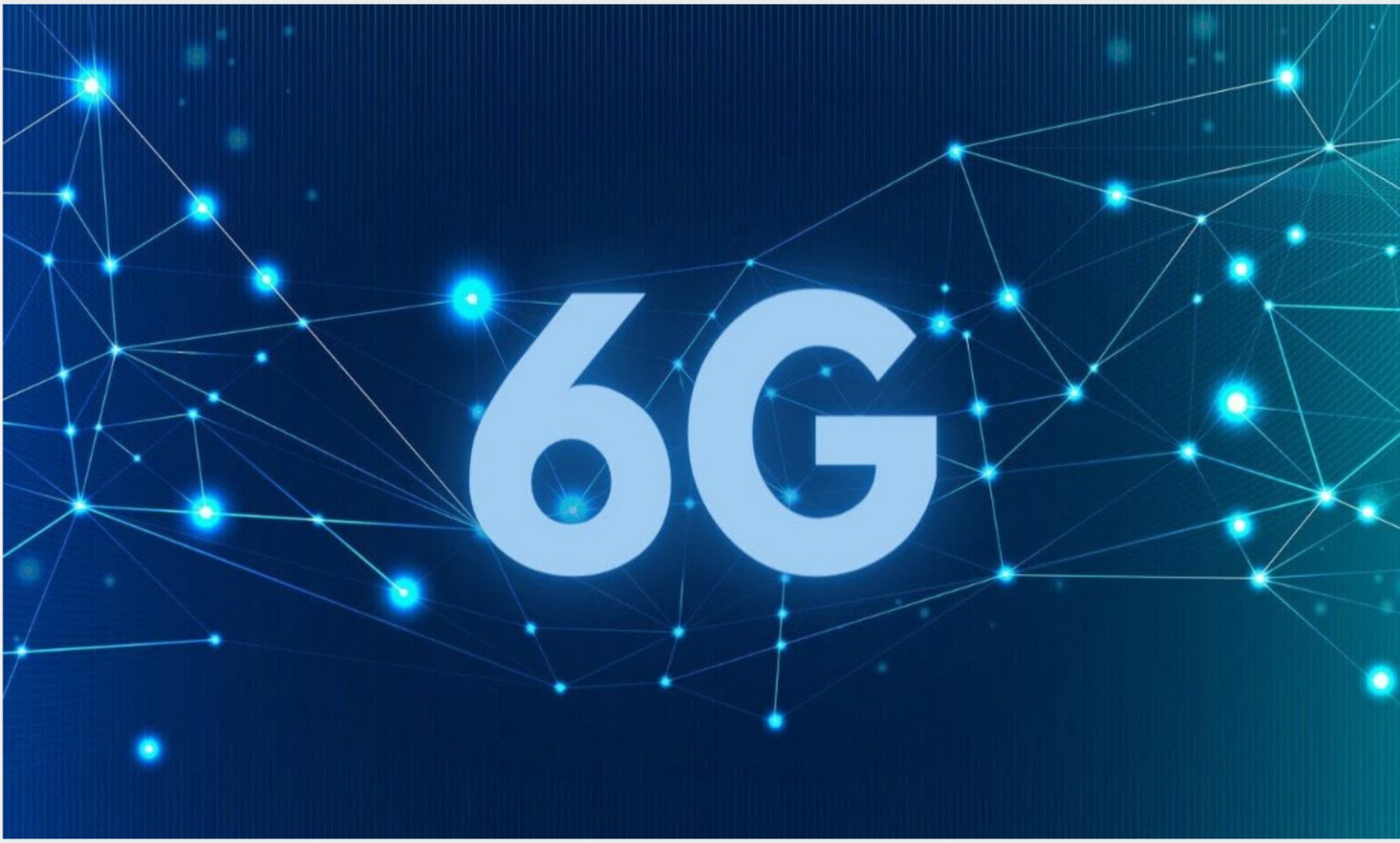
[234] Security Requirements and Challenges of 6G Technologies and Applications - PMC

[235] https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/26/joint-statement-endorsing-principles-for-6g-secure-open-and-resilient-by-design/

[236] Are You Ready To Give Consumers Control Over Their Data?

[237] Critical technologies and the Indo-Pacific: a new India–Australia partnership

[238] India's BHARAT 6G Vision and the Role of Like-Minded Partners - Australian Institute of International Affairs




CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: 91.141.228 2821, Fax: 91.141.228 2485
Email: cuts1@cuts.org, Website: www.cuts-international.org

Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland) and Washington DC (USA).