|  |
| --- |
| Assume that you are a **consultant** to large telecommunications businesses in Australia.  The Board of Directors for two different carriers/service providers has asked you to advise them on the networking regulations and legislation for the telecommunications industry, including their impact and factors influencing them.  You have been contracted by both businesses to develop:  **Carrier/Service provider 1:**   * one comprehensive report that evaluates the economic and political influences on the networking industry in Australia and describes the impact of regulations and legislation on the networking industry. * one summary report that evaluates the impact of legislation on planning processes and accessibility to networks.   **Carrier/Service Provider 2:**   * one comprehensive report that evaluates the economic and political influences on the networking industry in Australia and describes the impact of regulations and legislation on the networking industry. * one summary report that evaluates the impact of legislation on planning processes and accessibility to networks. |
| Choose any two carriers/service providers in Australia and complete page 4 of your Project Portfolio before starting the assessment.  **Carrier 1:** Optus Networks Pty Ltd  **Service provider 1:** Lebara |

**Carrier:** Entity that **owns or operates physical telecommunications infrastructure** used to supply services to the public.

**Examples:**

Must hold a **Carrier Licence** issued by the Australian Communications and Media Authority (ACMA).

* **Telstra Corporation Limited** (owns copper, fibre, mobile towers)
* **Optus Networks Pty Ltd**
* **NBN Co Limited** (wholesale broadband network)
* **TPG Telecom Ltd** (owns fibre, towers, submarine cables)

**Service Provider**: (Carriage Service Providers (CSPs)) Entity that **uses a carrier’s network** to offer telecommunications services to the public.

**Examples:**

Do **not** need a carrier licence. Must comply with the **Telecommunications Act 1997** and register with ACMA if supplying carriage services to the public.

* **Aussie Broadband** (uses NBN and some own backhaul)
* **Lebara** (resells Telstra/Optus services)
* **iiNet** (resells and partially owns infrastructure but mostly operates as a service provider)
* **Boost Mobile** (resells Telstra network)

ANSWERS

## 4.1 Keep your legislative and regulatory knowledge up to date:

Key telecommunications laws, regulations and policies:

<https://www.dlapiperintelligence.com/telecoms/index.html?t=laws&c=AU>

Rules for carriers and service providers:

<https://www.infrastructure.gov.au/media-communications-arts/internet/rules-carriers-and-service-providers>

### Ways available to keep your legislative and regulatory knowledge up to date

1. Subscribe to newsletters, courses, and webinars

2. Following governmental and specialised associations

3. Company training about legislative and regulatory changes

4. Be aware of the news on social media

5. Social gatherings with colleagues

### The ones I like the most are:

1. Subscribe to newsletters: I usually subscribe to newsletters from my company and suppliers to stay informed of the latest or most important changes.

2. Company training: I usually have to take refresher courses where I've worked.

3. Social gatherings with colleagues: Some colleagues have more knowledge and are more involved in legal issues.

## 4.2 Identify the telecommunications carriers and service providers in Australia

### List the carriers and service providers in Australia:

Register of licensed carriers: <https://www.acma.gov.au/register-licensed-carriers>

**Some telecommunications carriers:**

* 5G Network Operations Pty Ltd
* A.C.N. 625 580 332 Pty Ltd
* AAPT Limited (formerly AAP Telecommunications Pty Ltd)
* Amazon Kuiper Australia Pty Ltd
* EscapeNet Pty Ltd
* Optus Mobile Pty Ltd (formerly Mobilcom (Australia) Pty Limited)
* Telstra Corporation Limited (formerly Australian and Overseas Telecommunications Corporation Limited)
* TPG Telecom Limited (formerly Hutchison 3G Australia Pty Limited)

**Some carriage service providers:**

* Optus AAPT
* iiNet
* JB HiFi
* Kogan Mobile
* MeU Mobile
* Amaysim
* NBN
* Optus
* Telstra
* TPG Telecom
* Virgin Mobile
* Vodafone
* Woolworths
* Aldi Mobile
* Dodo,
* iiNet,
* Lebara Mobile
* Felix Mobile
* Tangerine

## 4.3 Summarise legislation relevant to the networking industry.

|  |  |  |  |
| --- | --- | --- | --- |
| **3. Identify and summarise legislation relevant to the networking industry.** |  |  |  |
| **Legislation** | **Summary** | **Main functions** | **Source** |
| **Telecommunications Act 1997** | Establishes the overarching framework for the telecommunications industry. It regulates carriers and carriage service providers, including licensing rules, carrier immunities when installing infrastructure, and obligations to ensure telecommunications availability for new real estate developments. It also provides consumer safeguards and allocates responsibilities to ACMA. | Defines obligations of telcos, licensing, consumer safeguards, and ACMA’s regulatory powers. | https://www.legislation.gov.au/C2004A05145/latest |
| **Telecommunications (Consumer Protection and Service Standards) Act 1999** | Creates legally enforceable consumer protection standards. It ensures the universal service obligation (including provision of telecommunications to premises across Australia), applies customer service guarantees, and provides funding mechanisms. It is key for consumer safeguards and equitable access. | Ensures access to basic phone services, customer service guarantees, funding for universal service. | https://www.legislation.gov.au/C2004A00441/latest |
| **Telecommunications (Interception and Access) Act 1979** | Prohibits unauthorised interception of communications and sets out circumstances where lawful access is permitted. It establishes warrant processes for interception, regulates data retention by service providers, and creates rules for lawful disclosure of communications data to enforcement agencies. | Sets out interception warrants, stored communication access, and data retention obligations. | https://www.legislation.gov.au/C2004A02124/latest |
| **National Broadband Network Companies Act 2011** | Provides the governance framework for NBN Co, ensuring high-speed broadband rollout to premises nationwide. It defines corporate structure, ownership limits, operational exemptions, and obligations regarding competition and service delivery. | Governs ownership, functions, reporting obligations, competition rules, and restrictions on private sector control. | https://www.legislation.gov.au/C2011A00022/latest |
| **Australian Communications and Media Authority Act 2005** | Establishes the ACMA as the regulator overseeing telecommunications, broadcasting, and radiocommunications. It grants ACMA power to enforce licensing, manage compliance, regulate consumer safeguards, and administer exemptions where appropriate. | Regulates broadcasting, radiocommunications, telecommunications, online content, and enforces compliance. | https://www.legislation.gov.au/C2005A00044/latest |
| **Competition and Consumer Act 2010** | Sets rules on competition and consumer protection. It addresses anti-competitive behaviour in telecommunications markets, ensures access arrangements for carriers, and provides consumer safeguards through the Australian Consumer Law. Exemptions may apply for certain government or public interest activities. | Enforces anti-competitive conduct rules, merger control, consumer law, and regulates telco access arrangements. | https://www.legislation.gov.au/C2004A00109/latest |
| **Broadcasting Services Act 1992** | Regulates broadcasting and online media services. It governs licensing of service providers, media ownership rules, Australian content obligations, and certain exemptions for community or narrowcasting services. | Licences broadcasters, regulates Australian content, media diversity, advertising, and classification obligations. | https://www.legislation.gov.au/C2004A04401/latest |
| **Radiocommunications Act 1992** | Manages the finite availability of the radiofrequency spectrum in Australia. It regulates spectrum allocation and licensing, interference management, and carrier rights and obligations. Exemptions may apply for low-impact or licence-free devices. | Spectrum licensing, interference management, technical standards, and ACMA’s enforcement powers. | https://www.legislation.gov.au/C2004A04465/latest |
| **Privacy Act 1988** | Provides the framework for handling personal information across sectors. It governs disclosure of personal information, sets national privacy principles, outlines exemptions (e.g. for small businesses in some circumstances), and empowers the OAIC to enforce compliance. | Governs data collection, storage, disclosure; creates OAIC as regulator; covers credit reporting and government records. | https://www.legislation.gov.au/C2004A03712/latest |
| **Online Safety Act 2021** | Strengthens the powers of the eSafety Commissioner to remove harmful online content. It applies to Australian and overseas service providers, mandates compliance with removal notices, and includes exemptions for certain types of content or providers. | Removal notices, restrictions on cyber-abuse, protection of children, enforcement against online service providers. | https://www.legislation.gov.au/C2021A00076/latest |
| **Criminal Code Act 1995** | Consolidates federal criminal offences. It covers misuse of telecommunications services, cybercrime, and offences related to disclosure of personal information without authority. It also provides penalties for unlawful interception or access. | Defines terrorism, fraud, cybercrime, misuse of telecommunications services, and penalties. | https://www.legislation.gov.au/C2004A04868/latest |
| **Encryption Act Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018** | Expands interception and access powers, specifically addressing encrypted communications. It allows agencies to compel service providers to assist with lawful access, regulates data retention obligations, and includes exemptions and limitations to balance privacy with national security. | Compels providers to assist agencies, creates new warrant and technical capability powers, balances security with privacy concerns. | https://www.legislation.gov.au/C2018A00148/latest |
| **Copyright Act 1968** | Provides protection for literary, artistic, musical and broadcast works. It governs ownership and licensing of rights, creates exemptions such as fair dealing, and supports enforcement in telecommunications and online environments. | Protects literary, musical, artistic works and broadcasts; sets exceptions, licensing schemes, and enforcement of rights. | https://www.legislation.gov.au/C1968A00063/latest |

### 3. How is the legislation implemented for large telecommunications businesses?

<https://business.gov.au/planning/industry-information/information-media-and-telecommunications-industry>

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Legislative Framework** | **Regulator** | **Impact on planning processes and accessibility** | **For Large business** | **Mechanisms of Regulation** | **Types of Penalties / Sanctions** |
| **Telecommunications Act 1997** | Australian Communications and Media Authority (ACMA), Australian Competition and Consumer Commission (ACCC) | Planning: Provides the core regulatory framework. As deregulation has increased, providers must balance compliance with flexibility to innovate. Accessibility: Supports faster services and future network growth by mandating fair interconnection. Influences 5G rollout, as carriers must comply with infrastructure approval processes. | Imposes carrier licence obligations on large companies. It establishes the framework for network facility access and interconnection with other carriers' networks. It also contains section 313, which can be used by government agencies to request carriers take action to prevent criminal activity. | Industry codes, service provider determinations, licensing, co-regulation, direct enforcement actions | Infringement notices, civil penalties (now up to $10 million per breach under reforms) |
| **Telecommunications (Consumer Protection and Service Standards) Act 1999** | Australian Communications and Media Authority (ACMA) | Planning: Shapes how providers ensure quality of service, especially in underserved areas. Future planning must consider digital inclusion post-COVID-19. Accessibility: Guarantees universal service, but the demand for faster broadband and 5G raises expectations for higher reliability even in difficult network conditions (rural, natural disasters). | Regulates the Universal Service Obligation (USO), which requires the primary carrier (Telstra) to provide a standard telephone service and payphones to all Australians, regardless of location. Large companies must also contribute to the Telecommunications Industry Levy to fund these services. | Industry codes (e.g. Consumer Protection Code), standards registered with ACMA | Breaches attract infringement notices and civil penalties |
| **Telecommunications (Interception and Access) Act 1979** | **Attorney-General's Department (AGD), Australian Federal Police (AFP), Australian Security Intelligence Organisation (ASIO)** | Planning: Requires providers to integrate surveillance capabilities, influencing long-term network architecture. Accessibility: Balances national security with consumer privacy. Demand for faster and encrypted services complicates lawful access, particularly in 5G networks vulnerable to cyberattacks. | Mandates large companies to retain certain types of telecommunications metadata (not content) for at least two years so it can be accessed by law enforcement and security agencies under a warrant. | Authorised interception/access under warrant or legislation | Criminal sanctions for unauthorised interception |
| **National Broadband Network Companies Act 2011** | Australian Competition and Consumer Commission (ACCC) | Planning: Mandates nationwide broadband planning, influencing how Australia addresses future growth and innovation. COVID-19 highlighted the need for resilient and scalable NBN services. Accessibility: Ensures equal access, but demand for faster services and high-quality video (remote work, online education) has pushed the NBN to upgrade capacity. Environmental conditions (fires, floods) challenge reliability. | Specifically obligates NBN Co to be a 'wholesale-only' company, meaning it cannot sell directly to consumers. Large retail telcos (like Telstra and Optus) must purchase access to the NBN Co network to offer services to their customers. | Access and pricing regulation, infrastructure oversight | Competition notices, court actions |
| **Australian Communications and Media Authority Act 2005** | Australian Communications and Media Authority (ACMA) |  | This Act establishes the ACMA as the supervisory regulator for telecommunications. The ACMA uses the powers granted by this Act to enforce industry standards and codes of conduct on large companies. | Establishes ACMA, defines its powers over broadcasting, telecoms, and radiocomm | Administrative enforcement, license conditions |
| **Competition and Consumer Act 2010** | Australian Competition and Consumer Commission (ACCC) | Planning: Ensures providers cannot abuse market power, which directly affects pricing and investment decisions. Accessibility: Encourages innovation (especially during COVID-19) and drives competition for faster, higher-quality services, including 5G. Prevents monopolies that could block rural access or environmentally sustainable investments. | Applies to large companies to regulate competition. The ACCC uses its powers under this Act to prevent anti-competitive conduct, regulate access to essential network infrastructure, and oversee compliance with consumer protection laws. | Anti-competitive conducts, Part XIB/XIC regulation of telecom access | Large fines (up to $50m or % turnover), enforceable undertakings |
| **Broadcasting Services Act 1992** | Australian Communications and Media Authority (ACMA) | Planning: Media convergence with internet services requires future-oriented regulation. Networks must adapt to new streaming demand while complying with broadcast standards. Accessibility: Guarantees diverse content, but network growth (e.g., video streaming post-COVID-19) puts pressure on quality of service. Environmental concerns also affect spectrum use and broadcasting facilities. | Imposes obligations on large companies that also operate broadcasting or subscription television services, such as rules on media ownership and content diversity. | Content regulation, advertising standards, complaints handling, co-regulation | Directions to remove or block content, enforceable notices |
| **Radiocommunications Act 1992** | Australian Communications and Media Authority (ACMA) | Planning: Central for 5G implementation and spectrum allocation. Regulates how spectrum is shared, balancing regulation with flexibility for innovation. Accessibility: Provides opportunities for new services (IoT, faster broadband). COVID-19 accelerated demand for wireless solutions, pushing spectrum efficiency. Environmental factors (e.g., tower placement, radiation concerns) must be managed. | Governs how large telcos obtain and use radiofrequency spectrum licences for wireless services like 4G and 5G. The ACMA administers this licensing process. | Licensing of spectrum, technical standards, interference control | Licence cancellation/suspension, infringement notices |
| **Privacy Act 1988** | OAIC (Office of the Australian Information Commissioner) | Planning: Shapes data handling policies, requiring robust cybersecurity measures in network growth and innovation. Accessibility: Increases consumer trust, but compliance can raise costs for providers. Privacy concerns are central to 5G and cloud-based services accelerated by COVID-19. | Requires large companies handling personal data to comply with the Australian Privacy Principles (APPs). This includes a mandatory data breach notification scheme and taking reasonable steps to secure personal information. | Australian Privacy Principles, investigation of breaches | Civil penalties, enforceable undertakings, criminal penalty for non-compliance |
| **Online Safety Act 2021** | **eSafety Commissioner** |  | Imposes obligations on large social media platforms and internet service providers to address cyberbullying and harmful content. The eSafety Commissioner can issue removal notices to these companies. | Online content scheme, online safety codes, investigation of harmful content | Infringement notices, substantial fines, court orders, daily penalties |
| **Criminal Code Act 1995** | Attorney-General's Department (AGD), Australian Federal Police (AFP) |  | Establishes federal offences related to cybercrime (e.g., hacking and electronic fraud) that apply to large companies. It's used to prosecute individuals or corporations if their actions breach these criminal laws. | General criminal offences, defines penalties applicable across statutes | Criminal sanctions (imprisonment, fines) |
| **Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018** | Attorney-General's Department (AGD), Australian Security Intelligence Organisation (ASIO), Australian Federal Police (AFP) | Planning: Forces companies to plan infrastructure with lawful interception, adding complexity to future network design. Accessibility: Security needs versus consumer rights impact trust. In a world of rising cyberattacks and data breaches, encryption standards are vital for 5G adoption and remote work innovation post-COVID-19. | Compels companies to provide technical assistance to security agencies to access encrypted data. Agencies can issue mandatory notices to companies to provide such assistance, provided a "systemic weakness" is not created. | Access to encrypted communications by law enforcement with warrants | Criminal penalties for failing to comply |
| **Copyright Act 1968** | Attorney-General's Department (AGD), Australian Federal Police (AFP) |  | Imposes responsibilities on telecommunications companies to combat copyright infringement. It is often used to issue court orders to block websites that facilitate piracy. | Copyright protection for content broadcast, infringement provisions | Injunctions, damages, criminal fines for wilful breach |

In summary, large corporations must comply with stricter legislation, acquire special licenses and permits, comply with a special tax regime, comply with employee regulations, intellectual property regulations, and have mandatory insurance.

Large corporations must comply with laws, standards, and initiatives that apply to the media and telecommunications industries, primarily imposed by the ACMA and ACCC.

They must also acquire licenses and permits to operate. These are some of the industries:

- Television license

- Radio license

- Commercial filming licensing

- Broadcast of copyright material

- Filming and photography permits

These licenses are granted by ABLIS (Australian Business License and Information Service).

Regarding taxes, large industries comply with different obligations under GST (Goods and Services Tax).

Finally, large industries have specific insurance policies that they must purchase, for example:

- Business interruption

- Professional indemnity

- Public liability

- Telecommunications

These are some laws that apply:

- Compliance with business indrustry legislation:

- Competition and Consumer Act 2010

- Australian Consumer Law (ACL)

- Copyright Act 1968

- Broadcasting Services Act 1992

- Radiocommunications Act 1992

- Telecommunications Act 1997

- Telecommunications (Consumer Protection and Service Standards) Act 1999

- Do Not Call Register Act 2006

- Spam Act 2003

- Privacy Act 1988

- Disability Discrimination Act 1992: World Wide Web Access

- Public Lending Right Act 1985

- Compliance with business indrustry schemes, standards and conde

- National Classification Scheme

- Broadcasting codes & schemes

- Telecommunications Consumer Protections (TCP) Code

- Compliance with ACCC guides (Australian Competition & Consumer Commission)

- Telecommunications Competition Notice Guidelines

- Review of transmission regulation

### 4. What are the rights of carriers and service providers in installing facilities in Australia?

<https://www.acma.gov.au/local-councils-and-network-facilities#low-impact>

The rights of carriers and service providers at facility sites are known as "powers and immunities," which allow companies certain freedoms depending on the impact as long as they follow the law (Telecommunications Act 1997). Carriers decide whether a facility falls into one of the two categories.

- Low-impact: These are telephone networks and internet network structures

- Not-low-impact: These are primarily networks or infrastructure that can affect a large area, for example, communication towers and overhead lines

These are some rights that the law grants companies when they are low-impact facilities:

- A company can enter the property to inspect it

- Install

- Maintain

Companies must request approval from the local or state government to work on not-low-impact facilities:

|  |  |  |
| --- | --- | --- |
|  | **Carriers** | Telecommunications Act 1997 |
|  | Have the power to enter and inspect land to determine its suitability for a facility. |
|  | Can install "low-impact facilities" on land without needing state, territory, or local government planning approvals, and often without landowner consent. |
|  | Defined in the Telecommunications (Low-impact Facilities) Determination 2018. Includes things like underground cables, pits, small antennae on existing structures, and public payphones. . |
|  | Must provide a minimum 10 business days' written notice to the landowner and occupier before starting work. They must also restore the land to its original condition. |
|  | Landowners can object to a proposed installation on certain grounds. If an objection can't be resolved, the matter can be referred to the Telecommunications Industry Ombudsman (TIO). |
|  | Can access land without notice to address an emergency to protect health, safety, property, or maintain adequate service levels. |
|  |  |  |
| **Aspect of Right** |  |  |
| **Legal Basis** |  |  |
| **Land Access** |  |  |
| **Facility Installation** |  |  |
| **What is a "Low-Impact Facility"?** |  |  |
| **Mandatory Obligations** |  |  |
| **Dispute Resolution** |  |  |
| **Emergency Situations** |  |  |
|  |  |  |
|  | **Service Providers** | Generally, they do not have the same statutory powers and must rely on commercial agreements with property owners or carriers. |
|  | Do not have a statutory right of access. They must obtain permission from the property owner. |
|  | Do not have the right to install facilities on private land without a pre-existing commercial agreement or a specific arrangement with the carrier that owns the network. |
|  | This classification of facility is not relevant to their rights, as they generally don't have the power to install them. |
|  | There are no mandatory obligations to provide notice under a legal framework. Any obligations are based on their commercial agreement with the customer. |
|  | If a dispute arises, it is handled according to the terms of their contract with the customer or through general consumer law. It does not fall under the specific land access dispute mechanisms of the TIO. |
|  | Do not have the right to access land for emergencies. This power is reserved for carriers. |

### 5. What is the impact of legislation on planning processes and accessibility to networks?

The impact of legislation on network planning and access processes is fundamental, as it defines the rules of the game for all companies, promoting competition. It also guarantees (by ACCC) essential access to infrastructure. It also investigates and intervenes in anti-competitive behaviour.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Regulator** | **Summary** | **Main functions** | **Legal Basis** | **Legal Actions / Enforcement Powers** | **Examples of Enforcement** | **Collaborator(s)** | **Type of Collaboration** |
| **Australian Communications and Media Authority (ACMA)** | Independent statutory authority regulating communications and media, including telecommunications. | Issues carrier and service provider licences; manages spectrum; enforces spam and Do Not Call laws; ensures telco compliance with service standards. | Telecommunications Act 1997, Radiocommunications Act 1992, Broadcasting Services Act 1992, Spam Act 2003. | Can issue infringement notices, financial penalties, suspend or cancel licences, and impose enforceable undertakings. | 2022: Optus fined $504,000 for breaching Spam Act 2003 rules by sending marketing without proper consent. | ACCC, OAIC, eSafety Commissioner, Department of Infrastructure, Transport, Regional Development, Communications and the Arts; international regulators such as Ofcom (UK) and FCC (USA). | Co-regulation of telecoms and media, spectrum management, consumer protection, spam enforcement, and international regulatory alignment. |
| **Australian Competition and Consumer Commission (ACCC)** | National competition and consumer regulator overseeing fair trading in telecommunications markets. | Promotes competition; enforces consumer protection; monitors telco pricing; regulates wholesale access to networks (e.g., NBN). | Competition and Consumer Act 2010, Telecommunications Act 1997. | Can launch court proceedings, impose penalties, accept undertakings, and enforce consumer redress. | 2021: Telstra fined $50m for unconscionable conduct towards Indigenous customers in telco sales. | ACMA, OAIC, Treasury, Federal Court of Australia, Consumer advocacy groups; international: OECD Competition Committee, International Competition Network (ICN). | Market regulation, consumer law enforcement, litigation, and international competition policy cooperation. |
| **Attorney-General's Department (AGD)** | Policy agency advising on national security, law enforcement, and telecommunications interception frameworks. | Develops and administers laws on lawful interception, surveillance, and data retention. | Telecommunications (Interception and Access) Act 1979, Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018. | Sets policy direction; authorises frameworks for interception; provides oversight mechanisms. | Drafted and oversaw implementation of the 2018 Assistance and Access Act (“anti-encryption” laws). | AFP, ASIO, ACMA, state and territory police, international security agencies (e.g., Five Eyes: US, UK, Canada, NZ). | Policy development, legislative frameworks, lawful interception, and international security/legal cooperation. |
| **Australian Federal Police (AFP)** | Federal law enforcement agency with jurisdiction over cybercrime and serious telecommunications offences. | Investigates offences involving carriage services (fraud, child exploitation, terrorism communications); works with telcos on lawful access. | Criminal Code Act 1995, Telecommunications (Interception and Access) Act 1979. | Executes search warrants, arrests, seizes assets, collaborates with telcos for lawful interception. | 2023: AFP charged individuals over large-scale SMS phishing scams exploiting telco networks. | AGD, ASIO, ACMA, state and territory police, Australian Signals Directorate (ASD); international: INTERPOL, Europol, FBI (USA). | Criminal investigations, cybercrime enforcement, intelligence sharing, operational taskforces, and joint investigations. |
| **Australian Security Intelligence Organisation (ASIO)** | Australia’s domestic security intelligence agency, focused on counter-terrorism and counter-espionage. | Uses telecommunications data for intelligence gathering; advises government on national security risks involving telcos. | Australian Security Intelligence Organisation Act 1979, Telecommunications (Interception and Access) Act 1979. | Authorised to conduct surveillance, use interception warrants, and collect communications data. | Used powers under TIA Act to intercept communications linked to suspected foreign interference activities. | AGD, AFP, ASD, Department of Home Affairs; international intelligence partners (Five Eyes). | Counter-terrorism, counter-espionage, signals intelligence cooperation, and joint security operations. |
| **OAIC (Office of the Australian Information Commissioner)** | National privacy and data protection regulator. | Oversees the Privacy Act, including telcos’ obligations under the Notifiable Data Breaches (NDB) scheme; investigates misuse of personal information. | Privacy Act 1988, Telecommunications Act 1997. | Can investigate, make determinations, issue compliance notices, and seek civil penalties. | 2023: Investigated Optus and Medibank data breaches under the NDB scheme. | ACMA, ACCC, eSafety Commissioner, AGD; international: Global Privacy Assembly, Asia-Pacific Privacy Authorities Forum. | Privacy and data protection enforcement, cross-border data governance, joint investigations, and policy development. |
| **eSafety Commissioner** | Independent regulator for online safety, with powers over harmful digital communications. | Enforces rules on cyberbullying, image-based abuse, illegal and harmful online content, and telco/ISP obligations for blocking. | Online Safety Act 2021. | Can issue takedown notices, require removal of harmful content, fine platforms, and direct ISPs to block access. | 2022: Ordered ISPs to block websites hosting terrorist and violent extremist material after Christchurch-related content circulated online. | ACMA, OAIC, AFP, Department of Home Affairs; international: Global Online Safety Regulators Network, European Commission, US Federal Trade Commission. | Online harm regulation, takedown orders, cross-border enforcement of online safety standards, policy advocacy. |

### 6. How does the legislation address data security and safety?

"Encryption Act, • The Privacy Act 1988, • Telecommunications (Interception and Access) Act 1979, • National Broadband Network Companies Act 2011"

<https://www.dlapiperdataprotection.com/index.html?c=AU>

Data security and protection legislation primarily defines data retention, critical infrastructure protection, and legal access to data.

Under the legal framework for data retention known as the "Data Retention Scheme" service providers are required to retain and store certain metadata for at least two years. This scheme also stipulates that certain government agencies may be authorized to access retained data. Furthermore, through the "Encryption Act," the government can require assistance companies to intercept encrypted data or access encrypted information for investigations, for example, involving messaging applications.

The government seeks to protect critical infrastructure, so service providers are required to report any cybersecurity incidents that have a significant impact under the "Security of Critical Infrastructure Act 2018."

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Legislation** | **Summary** | **Example** |
| **Privacy Act 1988** | Regulates collection, use, and disclosure of personal information; sets out Australian Privacy Principles; includes Notifiable Data Breaches (NDB) scheme. | Organisations must notify the OAIC and affected individuals of eligible data breaches: - Optus 2022 and Medibank 2022 breaches |
| **Security of Critical Infrastructure Act 2018 (SOCI Act)** | Protects critical infrastructure sectors (including telecommunications, data storage, financial services); mandatory reporting of cyber incidents. | Cloud and telco providers must register assets and report cyber incidents to the Cyber and Infrastructure Security Centre (CISC). |
| **Telecommunications (Interception and Access) Act 1979 (TIA Act)** | Governs lawful interception and access to communications/data by law enforcement and intelligence agencies. | Used by AFP, state police, and ASIO to investigate terrorism, organised crime, and child exploitation cases. |
| **Telecommunications Act 1997** | Regulates carriers and service providers, including obligations to secure networks and retain certain data (metadata retention for 2 years). | Carriers must retain metadata for law enforcement access; ACMA enforces compliance. |
| **Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA Act)** | Grants agencies powers to request technical assistance from service providers to access encrypted data. | Used in serious criminal investigations where encrypted messaging apps are involved.: - WhatsApp - Signal |
| **Criminal Code Act 1995 (Cth)** | Contains cybercrime offences: hacking, malware, unauthorised access, denial-of-service, misuse of carriage services. | State police prosecute offences like online harassment, fraud via phone/internet; AFP handles larger cybercrime operations. |
| **Online Safety Act 2021** | Strengthens powers of the eSafety Commissioner to tackle harmful online content, cyberbullying, image-based abuse. | In 2024, the eSafety Commissioner issued removal notices to X (Twitter) for violent content. |
| **Cybercrime Act 2001** | Amended the Criminal Code to align with international cybercrime standards (Budapest Convention). | Enabled stronger prosecution of hacking and fraud; harmonised Australian law with international frameworks. |
| **Australian Communications and Media Authority Act 2005** | Establishes ACMA; enforces rules on spam, scams, privacy breaches, and online safety compliance. | ACMA fines telcos for failing to protect customers from SMS scams. |
| **Data Availability and Transparency Act 2022** | Provides legal framework for secure data sharing between government agencies and authorised users. | Used in cross-agency projects like improving health, social services, and disaster response through shared datasets. |
| **Spam Act 2003** | Regulates unsolicited commercial electronic messages (email, SMS, instant messaging). Requires consent, accurate sender identification, and opt-out facility. | ACMA enforces compliance:  - Optus was fined $504,000 in 2022 for breaching spam rules by sending marketing emails/SMS without proper consent. |
| **Electronic Transactions Act 1999** | Gives legal recognition to electronic communications, contracts, and digital signatures; ensures online transactions have the same validity as paper-based ones. | Widely used in e-commerce and government services; enabled legally binding e-signatures and digital contracts during COVID-19 remote operations. |

## 4.3 Identify the regulators of the networking industry.

1. The Australian Communications and Media Authority (ACMA)

2. The Australian Competition and Consumer Commission (ACCC)

3. The Office of the Australian Information Commissioner (OAIC)

4. Australian Security Intelligence Organisation (ASIO)

<https://www.directory.gov.au/portfolios/infrastructure-transport-regional-development-communications-and-arts/australian-communications-and-media-authority#:~:text=The%20Australian%20Communications%20and%20Media,communications%20and%20certain%20online%20content>.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Regulator** | **Summary** | **Main functions** | **Legal Basis** | **Legal Actions / Enforcement Powers** | **Examples of Enforcement** | **Collaborator(s)** | **Type of Collaboration** |
| **Australian Communications and Media Authority (ACMA)** | Independent statutory authority regulating communications and media, including telecommunications. | Issues carrier and service provider licences; manages spectrum; enforces spam and Do Not Call laws; ensures telco compliance with service standards. | Telecommunications Act 1997, Radiocommunications Act 1992, Broadcasting Services Act 1992, Spam Act 2003. | Can issue infringement notices, financial penalties, suspend or cancel licences, and impose enforceable undertakings. | 2022: Optus fined $504,000 for breaching Spam Act 2003 rules by sending marketing without proper consent. | ACCC, OAIC, eSafety Commissioner, Department of Infrastructure, Transport, Regional Development, Communications and the Arts; international regulators such as Ofcom (UK) and FCC (USA). | Co-regulation of telecoms and media, spectrum management, consumer protection, spam enforcement, and international regulatory alignment. |
| **Australian Competition and Consumer Commission (ACCC)** | National competition and consumer regulator overseeing fair trading in telecommunications markets. | Promotes competition; enforces consumer protection; monitors telco pricing; regulates wholesale access to networks (e.g., NBN). | Competition and Consumer Act 2010, Telecommunications Act 1997. | Can launch court proceedings, impose penalties, accept undertakings, and enforce consumer redress. | 2021: Telstra fined $50m for unconscionable conduct towards Indigenous customers in telco sales. | ACMA, OAIC, Treasury, Federal Court of Australia, Consumer advocacy groups; international: OECD Competition Committee, International Competition Network (ICN). | Market regulation, consumer law enforcement, litigation, and international competition policy cooperation. |
| **Attorney-General's Department (AGD)** | Policy agency advising on national security, law enforcement, and telecommunications interception frameworks. | Develops and administers laws on lawful interception, surveillance, and data retention. | Telecommunications (Interception and Access) Act 1979, Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018. | Sets policy direction; authorises frameworks for interception; provides oversight mechanisms. | Drafted and oversaw implementation of the 2018 Assistance and Access Act (“anti-encryption” laws). | AFP, ASIO, ACMA, state and territory police, international security agencies (e.g., Five Eyes: US, UK, Canada, NZ). | Policy development, legislative frameworks, lawful interception, and international security/legal cooperation. |
| **Australian Federal Police (AFP)** | Federal law enforcement agency with jurisdiction over cybercrime and serious telecommunications offences. | Investigates offences involving carriage services (fraud, child exploitation, terrorism communications); works with telcos on lawful access. | Criminal Code Act 1995, Telecommunications (Interception and Access) Act 1979. | Executes search warrants, arrests, seizes assets, collaborates with telcos for lawful interception. | 2023: AFP charged individuals over large-scale SMS phishing scams exploiting telco networks. | AGD, ASIO, ACMA, state and territory police, Australian Signals Directorate (ASD); international: INTERPOL, Europol, FBI (USA). | Criminal investigations, cybercrime enforcement, intelligence sharing, operational taskforces, and joint investigations. |
| **Australian Security Intelligence Organisation (ASIO)** | Australia’s domestic security intelligence agency, focused on counter-terrorism and counter-espionage. | Uses telecommunications data for intelligence gathering; advises government on national security risks involving telcos. | Australian Security Intelligence Organisation Act 1979, Telecommunications (Interception and Access) Act 1979. | Authorised to conduct surveillance, use interception warrants, and collect communications data. | Used powers under TIA Act to intercept communications linked to suspected foreign interference activities. | AGD, AFP, ASD, Department of Home Affairs; international intelligence partners (Five Eyes). | Counter-terrorism, counter-espionage, signals intelligence cooperation, and joint security operations. |
| **OAIC (Office of the Australian Information Commissioner)** | National privacy and data protection regulator. | Oversees the Privacy Act, including telcos’ obligations under the Notifiable Data Breaches (NDB) scheme; investigates misuse of personal information. | Privacy Act 1988, Telecommunications Act 1997. | Can investigate, make determinations, issue compliance notices, and seek civil penalties. | 2023: Investigated Optus and Medibank data breaches under the NDB scheme. | ACMA, ACCC, eSafety Commissioner, AGD; international: Global Privacy Assembly, Asia-Pacific Privacy Authorities Forum. | Privacy and data protection enforcement, cross-border data governance, joint investigations, and policy development. |
| **eSafety Commissioner** | Independent regulator for online safety, with powers over harmful digital communications. | Enforces rules on cyberbullying, image-based abuse, illegal and harmful online content, and telco/ISP obligations for blocking. | Online Safety Act 2021. | Can issue takedown notices, require removal of harmful content, fine platforms, and direct ISPs to block access. | 2022: Ordered ISPs to block websites hosting terrorist and violent extremist material after Christchurch-related content circulated online. | ACMA, OAIC, AFP, Department of Home Affairs; international: Global Online Safety Regulators Network, European Commission, US Federal Trade Commission. | Online harm regulation, takedown orders, cross-border enforcement of online safety standards, policy advocacy. |

## 4.4 Summarise the regulatory requirements.

### 1. What are the implications of government regulation and deregulation for Optus (carrier) and Lebara (service provider)?

**Optus (carrier):**

- Regulation:

- Requires a license to operate

- Must comply Telecommunications Act 1997 and any related standards and codes

- Compliance with industry standards is mandatory

- Is required to respond to ACMA, ACCC, and OAIC

- Is required to follow USO (Universal Service Obligation) regulations

- Must comply with Emergency Call Services Requirements Industry Code (Industry Ombudsman scheme)

- Must comply with Emergency Call Services Requirements Industry Code (Industry Ombudsman scheme)

- It is required to follow the "Data Retention Scheme"

- It is required to provide assistance regarding encrypted information to government agencies (Encryption Act)

- Deregulation:

- It benefits from the advantages of "powers and immunities"

**Lebara (service provider):**

- Regulation:

- Must comply with Telecommunications Act 1997 and any related standards and codes

- CSPs must comply Telecommunications Act 1997 and

- Must comply with Emergency Call Services Requirements Industry Code (Industry Ombudsman scheme)

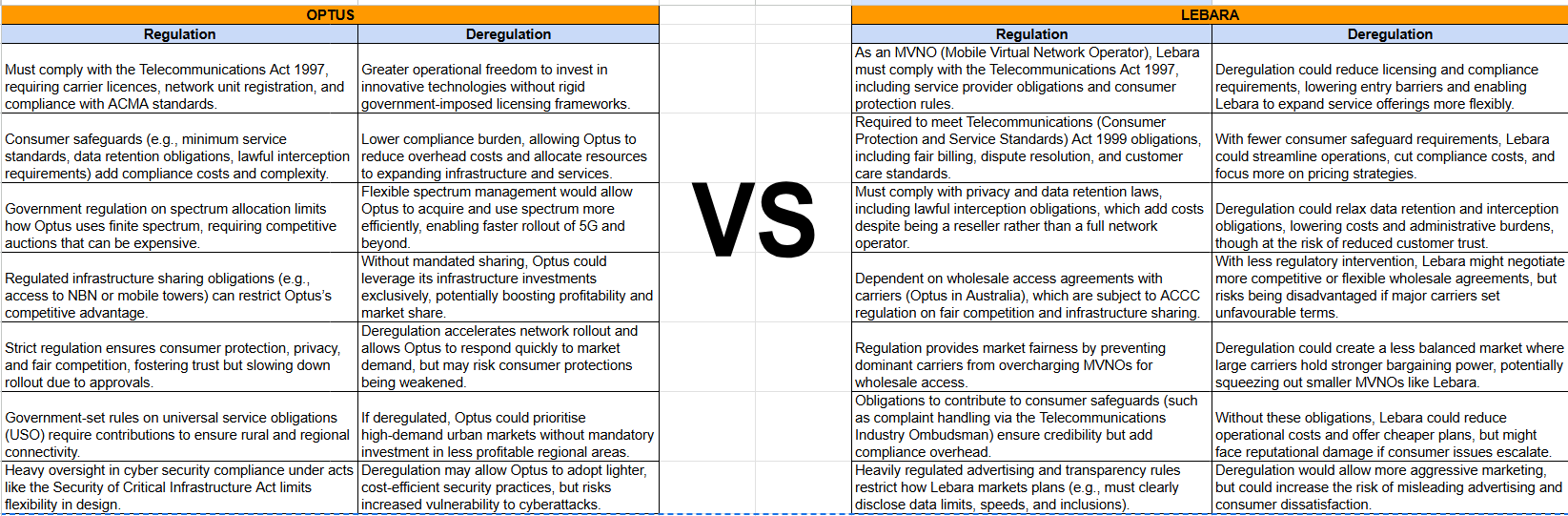
- Must comply with Emergency Call Services Requirements Industry Code (Industry Ombudsman scheme)

- It is required to follow the "Data Retention Scheme"

- It is required to provide assistance regarding encrypted information to government agencies (Encryption Act)

- Deregulation:

- It benefits from the advantages of "powers and immunities"



### 2. What are the licensing requirements for Optus (carrier) and Lebara (service providers)?

Optus:

- Carrier Licence

- Nominated Carrier Declarations: Operate other networks and act as a carrier.

- Spectrum Licences: Operate spectrum frequencies.

Lebara:

- Does not require a license as it is not a carrier

- Spectrum Licence

- Apparatus Licence: Use equipment to work with frequencies.

- Class Licence: Access to shared spectrum.

A screenshot of a computer screen

AI-generated content may be incorrect.

### 3. What method is used by the Australian Competition and Consumer Commission (ACCC) to enforce competitive provisions between service providers?

<https://www.globalcompliancenews.com/antitrust-and-competition/antitrust-and-competition-laws-in-australia/>

The ACCC refers cases to the Commonwealth Director of Public Prosecutions (CDPP), who is responsible for enforcing the law. By law, the ACCC can also require access to infrastructure and data.

Penalties for anti-competitive conduct can include:

- Fines of up to $10 million

- 10% of annual profits

- For boycotts, fines of up to $750,000

- Criminal cartel offenses are punishable by imprisonment of up to 10 years or a fine of $340,000 to $500,000

By law, companies are prohibited from compensating their officers for the payment of fines or any associated legal costs.

|  |  |
| --- | --- |
| **Consumer Commission (ACCC) to enforce competitive provisions between service providers** | |
| **Method** | **Details / How ACCC Enforces** |
| **Legislative Powers** | Competition and Consumer Act 2010 (CCA)  The key legislation under which the ACCC enforces anti-competitive behaviour provisions.  Prohibits cartel conduct, misuse of market power, exclusive dealing, and anti-competitive mergers.  Applies equally to large carriers (e.g., Telstra, Optus) and smaller MVNOs (e.g., Lebara, Amaysim).  Telecommunications Act 1997  Grants the ACCC specific powers to regulate access to telecommunications infrastructure, ensuring new entrants can compete fairly. |
| **Access Regulation** | Declared Services:  The ACCC can "declare" certain telecommunications services (e.g., wholesale access to fixed-line networks, NBN access, mobile roaming).  Once declared, providers must give competitors access on fair and reasonable terms.  Access Determinations:  The ACCC sets binding rules on pricing and non-price terms for declared services.  Ensures wholesale providers (e.g., Telstra, NBN Co, Optus) cannot exploit dominance by overcharging or restricting access.  Final Access Determinations (FADs):  Legally binding terms set by the ACCC if commercial negotiations between providers fail. |
| **Price and Tariff Regulation** | Wholesale pricing oversight:  The ACCC monitors and regulates wholesale charges carriers impose on competitors.  Example: NBN pricing, mobile roaming, transmission services.  Retail price controls (historical):  Used in the past for Telstra to prevent excessive pricing in monopoly areas. |
| **Merger Control** | The ACCC assesses proposed mergers and acquisitions to prevent reduction in competition.  Example: ACCC opposed the TPG–Vodafone merger in 2019 (though later overturned by the Federal Court).  Focus: whether consolidation would substantially lessen competition in mobile, fixed-line, or wholesale markets. |
| **Anti-Competitive Conduct Enforcement** | Cartel Enforcement: Pursues agreements between providers that fix prices, share markets, or rig bids.  Misuse of Market Power: Prevents dominant carriers from leveraging size to damage smaller competitors.  Exclusive Dealing: Stops practices where a carrier limits another provider’s ability to compete (e.g., tying access to network infrastructure with other conditions).  Court Action: The ACCC can take carriers to the Federal Court seeking injunctions, penalties, or compensation. |
| **Monitoring and Reporting** | Market Studies & Inquiries:  ACCC regularly conducts market reviews on broadband, mobile, and data services.  Example: annual Communications Market Report.  NBN Wholesale Market Indicators Report:  Tracks competition by publishing data on wholesale services purchased from NBN Co by retailers.  Price Monitoring:  Monitors prices for fixed-line, mobile, and internet services to ensure competitive trends. |
| **Authorisations & Exemptions** | The ACCC may authorise potentially anti-competitive agreements if the public benefit outweighs detriment.  Allows collaboration in areas like infrastructure sharing (e.g., regional mobile roaming) where consumer benefits are clear. |
| **Consumer Protection Enforcement** | Enforces provisions under the Australian Consumer Law (ACL) against misleading advertising, unfair contract terms, and unconscionable conduct.  Particularly relevant for telcos marketing mobile data inclusions, NBN speeds, or “unlimited” plans. |
| **Undertakings & Compliance Programs** | The ACCC may accept court-enforceable undertakings from providers to change behaviour instead of proceeding with litigation.  Example: Telcos committing to clearer advertising of broadband speeds.  Requires service providers to implement internal compliance programs to prevent recurrence. |

### 4. What are the policies and procedures of the ACCC (at least one)?

<https://www.accc.gov.au/about-us/accc-priorities/compliance-and-enforcement-priorities#:~:text=Accountability%20%E2%80%93%20the%20ACCC's%20decision%2Dmaking,the%20resulting%20or%20potential%20harm>.

This policy establishes priorities to be achieved during the current year and also prioritizes long-term conduct, for example:

- Cartel conduct

- Anti-competitive conduct

- Product safety

- Consumers experiencing vulnerability or disadvantage

- Conduct impacting First Nations Australians

- Small business

- Scams

Policy principles:

- Accountability

- Transparency

- Confidentiality

- Timeliness

- Proportionality

- Fairness

The ACCC has several enforcement measures:

1. Administrative Resolution: Mandates the conduct to be stopped

2. Infringement Notices: Notice and infringement

3. Enforceable Undertakings (Section 87B): An administrative resolution and infringement notice are issued.

4. Court Cases: Imposition of judicial sanctions

5. Debarment: Officials of the offending company are debarred

The ACCC also takes other, less aggressive actions and collaborates with other agencies.

|  |  |
| --- | --- |
| **Consumer Commission (ACCC) to enforce competitive provisions between service providers** | |
| **Method** | **Details / How ACCC Enforces** |
| **Legislative Powers** | Competition and Consumer Act 2010 (CCA)  The key legislation under which the ACCC enforces anti-competitive behaviour provisions.  Prohibits cartel conduct, misuse of market power, exclusive dealing, and anti-competitive mergers.  Applies equally to large carriers (e.g., Telstra, Optus) and smaller MVNOs (e.g., Lebara, Amaysim).  Telecommunications Act 1997  Grants the ACCC specific powers to regulate access to telecommunications infrastructure, ensuring new entrants can compete fairly. |
| **Access Regulation** | Declared Services:  The ACCC can "declare" certain telecommunications services (e.g., wholesale access to fixed-line networks, NBN access, mobile roaming).  Once declared, providers must give competitors access on fair and reasonable terms.  Access Determinations:  The ACCC sets binding rules on pricing and non-price terms for declared services.  Ensures wholesale providers (e.g., Telstra, NBN Co, Optus) cannot exploit dominance by overcharging or restricting access.  Final Access Determinations (FADs):  Legally binding terms set by the ACCC if commercial negotiations between providers fail. |
| **Price and Tariff Regulation** | Wholesale pricing oversight:  The ACCC monitors and regulates wholesale charges carriers impose on competitors.  Example: NBN pricing, mobile roaming, transmission services.  Retail price controls (historical):  Used in the past for Telstra to prevent excessive pricing in monopoly areas. |
| **Merger Control** | The ACCC assesses proposed mergers and acquisitions to prevent reduction in competition.  Example: ACCC opposed the TPG–Vodafone merger in 2019 (though later overturned by the Federal Court).  Focus: whether consolidation would substantially lessen competition in mobile, fixed-line, or wholesale markets. |
| **Anti-Competitive Conduct Enforcement** | Cartel Enforcement: Pursues agreements between providers that fix prices, share markets, or rig bids.  Misuse of Market Power: Prevents dominant carriers from leveraging size to damage smaller competitors.  Exclusive Dealing: Stops practices where a carrier limits another provider’s ability to compete (e.g., tying access to network infrastructure with other conditions).  Court Action: The ACCC can take carriers to the Federal Court seeking injunctions, penalties, or compensation. |
| **Monitoring and Reporting** | Market Studies & Inquiries:  ACCC regularly conducts market reviews on broadband, mobile, and data services.  Example: annual Communications Market Report.  NBN Wholesale Market Indicators Report:  Tracks competition by publishing data on wholesale services purchased from NBN Co by retailers.  Price Monitoring:  Monitors prices for fixed-line, mobile, and internet services to ensure competitive trends. |
| **Authorisations & Exemptions** | The ACCC may authorise potentially anti-competitive agreements if the public benefit outweighs detriment.  Allows collaboration in areas like infrastructure sharing (e.g., regional mobile roaming) where consumer benefits are clear. |
| **Consumer Protection Enforcement** | Enforces provisions under the Australian Consumer Law (ACL) against misleading advertising, unfair contract terms, and unconscionable conduct.  Particularly relevant for telcos marketing mobile data inclusions, NBN speeds, or “unlimited” plans. |
| **Undertakings & Compliance Programs** | The ACCC may accept court-enforceable undertakings from providers to change behaviour instead of proceeding with litigation.  Example: Telcos committing to clearer advertising of broadband speeds.  Requires service providers to implement internal compliance programs to prevent recurrence. |

### 5. What are the planning obligations of USO?

<https://www.acma.gov.au/about-universal-service-obligation>

<https://www.telstra.com.au/consumer-advice/customer-service/universal-service-obligation>

<https://www.lgaq.asn.au/News-and-Media/News-articles/The-Universal-Service-Obligation-History-and-future>

The USO is a company's obligation to guarantee basic access to essential telecommunications services. Telstra, as the largest company, must comply with the USO; the government funds its implementation.

Teltra's obligations are:

1. Provide Standard Telephone Services (STS)

2. Provide payphones

3. Offer access to 24-hour emergency numbers

The current planning obligations are:

1. Universal Access Planning (Modernising Services): Guarantee access to both broadband and voice services for all Australians via NBN.

2. Network Maintenance & Expansion: Ensure access to a standard telephone service (STS) and payphones nationwide.

3. Emergency & Priority Services: Call emergency numbers anytime, anywhere, free of charge.

4. Forward-Looking Plans: Update USO to keep it ahead of new technologies.

Next planning:

The current government wants to take advantage of new technologies, so it wants to ensure that USO in the future meets the following requirements:

- Broadband services are available to 100% of Australian premises, on request, at the completion of the NBN rollout in 2020

- Voice services are available to 100% of Australian premises on request

- Any proposed new service delivery arrangements are more cost effective than the existing USO contract (including any transitional costs) and,

- A new consumer safeguards framework is in place following a review and associated public consultation process.

A diagram of a company

AI-generated content may be incorrect.

### 6. What are the policies and procedures of the USO?

<https://www.infrastructure.gov.au/media-communications-arts/phone/phone-services/universal-service-obligation-voice-services>

<https://www.anao.gov.au/work/performance-audit/management-contract-telephone-universal-service-obligations>

<https://www.acma.gov.au/rules-telstra-payphones>

Telstra is committed to ensuring USO standard telephone services (STS) and payphones are under policies to ensure that the service is reasonably accessible to all Australians anywhere in Australia.

The policies that Telstra complies with are:

* Payphones
* Standard telephone service

The "Universal Access to Broadband Services" framework describes the obligations that the infrastructure must meet:

- Universal Service Guarantee (USG): Access for Australians to both broadband and voice services, anywhere in Australia

- Universal Access to Voice Services: Access for Australians to fixed voice services and payphones

- Modernizing Universal Telecommunications Services: The government seeks to update voice and broadband services to the latest technology

The procedures that Telstra must follow, which are defined by ACMA, are:

* where to locate payphones.
* the criteria to install, remove and maintain payphones.
* their consultation process.
* install or removing payphone

Other services and procedures are also described by Telstra:

* Payphone enquiries & applications
* Reporting faults
* Telstra Smart Payphone
* TTY payphones (payphones for deaf people)
* Making a complaint about a payphone

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts monitors and oversees the implementation of the USO.

A diagram of a company

AI-generated content may be incorrect.

Plan and summarise additional research required for your reports.

## Australian economic conditions

<https://www.abs.gov.au/articles/9-facts-about-economy-march-quarter>

[https://www.oecd.org/en/topics/sub-issues/economic-surveys/Australia-Economic-Snapshot.html](https://www.oecd.org/en/topics/sub-issues/economic-surveys/Australia-Economic-Snapshot.html?utm_source=chatgpt.com)

Data from the first quarter of 2025 show that the Australian economy has shrunk, primarily due to lower public spending and inflation. GDP is also down 0.2% compared to 2024.

First, the Australian economy has suffered losses in imports, exports, and tourism due to weather events in Western Australia and Queensland. However, gold exports were not affected, increasing by $2.1 billion.

The construction sector is also being affected due to delays in public projects, which has caused public investment to fall. The affected sectors are: energy, telecommunications, road, and rail.

Although underlying inflation (excluding volatile services) is down, and in fact is the lowest since 2021, it reflects that the economy is contracting at a steady pace.

Finally, employment grew by 2.2% annually, largely due to a 3.4% annual increase in wages due to investment in the public sector.

## Economic factors that can affect growth (x5)

<https://www.oecd.org/en/publications/oecd-economic-outlook-volume-2025-issue-1_83363382-en/full-report/australia_b563f928.html>

<https://programsandcourses.anu.edu.au/course/pols2094>

1. Weather events

2. Public investment

3. GDP, Inflation

4. International political economy

5. Household consumption

## Political influences on public and commercial enterprises that provide services in networking markets. “*Describe at least one political influence on public and commercial network services.*”

<https://www.homeaffairs.gov.au/cyber-security-subsite/files/factsheet-ransomware-payment-reporting.pdf>

The government created the "Cyber ​​Security Act 2024" in response to the lack of a legal framework for cybersecurity.

Between 2022 and 2023, the data theft scandals that rocked the country highlighted the lack of legal measures to respond to cybercriminals. In 2022, Optus suffered an attack that allowed the personal data of 40% of the population to be published. That same year, Medibank suffered a ransomware attack that compromised the personal data of 9.7 million people, resulting in the data being leaked to the dark web after the ransom was not received. Finally, in 2023, Latitude Financial suffered an attack that exposed the personal data of 14 million people online.

Prior to the Cyber ​​Security Act, the legal framework was provided by the Privacy Act 1988, on the protection of personal data, and the Security of Critical Infrastructure Act 2018, on the protection of critical sectors for the country. Despite the existence of these laws, there were no laws regarding the legal obligations of companies.

The Cyber ​​Security Act requires companies to report serious cybersecurity incidents and report ransom demands starting May 30 of this year. This response to cyber extortion also increased fines for security breaches from 2.2 million to 50 million, or more as determined by law.

In short, the law was created to protect Australians' data, increase transparency in the face of cyberattack incidents, and strengthen national resilience to cyber threats.

## Accessibility of networking services to individuals and organisations across Australia

1. Describe the accessibility of Optus

<https://www.optus.com.au/content/dam/optus/documents/about-us/inclusion-diversity/accessibility/optus-access-and-inclusion-action-plan-2024-2029.pdf>

Optus has an accessibility plan called the "Optus Access and Inclusion Action Plan 2024–2029," which describes industry-leading policies and best practices. It consists of:

- Respect and Rights: Optus is free from discrimination and all types of violence.

- Social Inclusion: Improves understanding of disability.

- Individualized: Optus understands that people with disabilities experience their environment differently.

- Confidence and Acceptance: Optus encourages building confidence in disability.

- Diversity as a Strength: Optus celebrates the strength of people with disabilities.

- Independence: Optus celebrates the freedom of choice.

- Accessible: Optus seeks to remove all barriers.

- In Partnership: At Optus, everyone makes decisions together.

1. Describe the accessibility of Lebara mobile

<https://www.lebara.com.au/support/accessibility/>

Lebara follows the best practices described in the "AMTA Mobile Phone Industry Good Practice Guide: Accessibility for People with Disabilities."

The services Lebara offers primarily focus on communication. Lebara provides a direct number to access the National Relay Service (NSR) for assistance to people with disabilities.

They also offer the option of requesting an interpreter for those seeking assistance in a language other than English.

## Issues that contravene relevant policies, procedures, and legal requirements “Identify issues associated with Optus/Lebara that contravenes relevant policies, procedures, and legal requirements (at least one).”

<https://www.acma.gov.au/sites/default/files/2024-11/Investigation%20report%20-%20Optus%20outage%201Nov23%20%28redacted%29.pdf>

<https://en.wikipedia.org/wiki/2022_Optus_data_breach>

In September 2022, Optus suffered a cyberattack where the personal data of around 10 million people was leaked on the dark web and offered for $400,000. This led to the OAIC (the Office of the Australian Information Commissioner) and ACMA (the Australian Communications and Media Authority) initiating an investigation into possible violations of the data privacy act. The AFP (the Australian Federal Police) is also investigating the data theft.

Class-action lawsuits were also filed against Optus seeking compensation for the damages incurred and to compensate customers for lost time and distress.

Optus had to cover $140 million in costs to replace documents, such as passports and licenses, whose data was leaked.

No fines have yet been imposed against Optus in this case. Due to this and other related cases, the government created the Cyber ​​Security Act in 2024.

-----------------------------------------------------------------------------------

Lebara

<https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7317>

Lebara doesn't have any issues. So I'm going to talk about what will likely happen in the future, generally, for all carriers and service providers.

The new reform called the "Telecommunications Amendment (Enhancing Consumer Safeguards)" is underway. In short, if the reform is approved, three major changes are expected.

First, service providers would be required to register with the so-called "Carriage Service Provider Register," managed by ACMA. ACMA will now have the power to take action more quickly and impose much higher fines, increasing from $250,000 to $10 million.

Second, the creation of the Universal Outdoor Mobile Obligation (UOMO), which is the equivalent of USO but focused on mobile coverage. It is expected to guarantee mobile coverage throughout Australia using low-Earth orbit (LEO) satellites.

Finally, telecommunications providers will be required to implement a mandatory Telecommunications Security and Risk Management Program (TSRMP). Currently, some asset registrations were optional, so the new reform requires the registration of all critical assets and the reporting of all cyber incidents.

## Other research “If you require any further research, summarise it here.”

NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA NA N