# MIS761
# Cyber Security Strategies

**Dept. of Information Systems & Business Analytics**

**Deakin Business School**

## Week 6 – Australian Laws and Regulations for Cyber Security

AACSB ACCREDITED

DEAKIN BUSINESS SCHOOL

# Privacy Act
# -Understanding Privacy - Your Rights

- **Privacy as a Fundamental Human Right:**
  - Privacy supports freedom of association, thought, and expression, and protects against discrimination.
  - Definitions of privacy vary globally and personally but generally encompass:
    - Freedom from interference or intrusion.
    - Control over who accesses and uses personal information.
    - The ability to associate freely with others.
- **What Constitutes Personal Information:**
  - Personal information is any data that can identify an individual, such as:
    - Name, address, phone number, or date of birth.
    - Sensitive information like racial origin, political views, or health records.
    - Digital identifiers like IP addresses, voice prints, and biometric data.
  - Sensitive information is subject to stricter privacy protections.

# Privacy Act
# -Privacy in the Digital Age

- **Managing Your Online Presence:**
  - Social media platforms facilitate sharing of personal content like messages, photos, and videos.
  - Information shared online can be accessed widely, sometimes beyond intended audiences.
  - Even with privacy settings, complete control over shared content is challenging; it may persist in archived forms.
- **Your Rights Rights and Responsibilities Under the Privacy Act:**
  - The Privacy Act 1988 safeguards personal information shared on platforms with significant operations in Australia (e.g., Facebook, LinkedIn).
  - If your information is posted without consent, you can request removal from the platform or seek assistance from the Office of the eSafety Commissioner for online abuse or cyberbullying issues.
  - However, the Act does not cover individuals acting privately, though other laws like copyright or defamation might apply.

| If you're concerned about | Contact |
| --- | --- |
| Your personal information being mishandled | The OAIC |
| A data breach | See Data Breach Support and Resources |
| An Australian child being cyberbullied | The Office of the eSafety Commissioner<br>ThinkUKnow |
| An adult experiencing cyber abuse | The Office of the eSafety Commissioner |
| An intimate image or video of you has been shared or someone is threatening to share it without your consent | The Office of the eSafety Commissioner |
| Illegal and harmful content | The Office of the eSafety Commissioner |
| Having been defamed | A lawyer |
| Protecting yourself online | The Office of the eSafety Commissioner<br>The Australian Cyber Security Centre |
| Serious harassment | The police |

https://www.oaic.gov.au/privacy/your-privacy-rights/social-media-and-online-privacy/social-media

# Privacy Act
# -Rights and Responsibilities

**Your Rights Under the Privacy Act:**

- **Informed Consent:** You have the right to know why your personal information is collected, how it will be used, and to whom it may be disclosed.
- **Access and Control:** You can request access to your personal data, correct inaccuracies, and opt-out of unwanted direct marketing.
- **Anonymous Interactions:** In some cases, you may choose not to identify yourself or use a pseudonym.
- **Complaints:** If you believe your data has been mishandled, you can file a complaint against organizations covered by the Privacy Act.

- **Responsibilities Under the Privacy Act:**
  - **Covered Entities:** The Act applies to Australian Government agencies and organizations with an annual turnover of more than $3 million, including large corporations and specific small businesses.
  - **Non-Covered Entities:** State or territory government agencies, public schools, universities (except private ones), media organizations engaged in journalism, and individuals acting personally are generally not covered by the Act.
  - **Small Business Exemptions:**
    - **General Exemption:** Most small businesses with a turnover of $3 million or less are exempt unless they voluntarily opt-in, handle sensitive data, or meet specific criteria (e.g., health service providers, businesses trading in personal information).
    - **Australian Link Requirement:** The Act only applies to small businesses with a significant connection to Australia, such as being incorporated or conducting business within the country.
    - **Consent for Exemption:** Small businesses can exempt themselves by obtaining consent from individuals to collect or disclose their personal data.
    - **Special Cases:** Some small businesses, such as credit reporting bodies or those handling government contracts, are covered regardless of turnover.

# Privacy Act
# -Australian Privacy Principles (APPs)

- **Foundation of Privacy Protection:** The APPs form the core framework within the Privacy Act 1988, guiding how organizations and agencies handle personal information.
- **Flexibility and Adaptability:** As principles-based and technology-neutral laws, the APPs allow entities to customize their practices to suit their specific business models and the evolving technological landscape.
- **Structure of the APPs:** The APPs are designed to cover all stages of personal information management and are grouped into five key parts:
  - **Part 1: Consideration of Privacy (APPs 1 and 2)** - Focuses on the governance and management of personal information.
  - **Part 2: Collection of Information (APPs 3, 4, and 5)** - Outlines rules for collecting personal data, including obtaining consent and notifying individuals.
  - **Part 3: Dealing with Information (APPs 6, 7, 8, and 9)** - Governs how personal information can be used, disclosed, and transferred.
  - **Part 4: Integrity of Information (APPs 10 and 11)** - Ensures the accuracy, completeness, and security of personal data.
  - **Part 5: Access and Correction (APPs 12 and 13)** - Provides individuals with rights to access and correct their personal information.
- **Consequences of Non-Compliance:** Breaching any APP is considered an interference with an individual's privacy, potentially leading to regulatory action and penalties.

# Privacy Act
# - Notifiable Data Breaches (NDB) scheme

- **Mandatory Notification:** Entities must notify individuals and the Commissioner about data breaches likely to cause serious harm. This requirement has been in place since February 22, 2018.
- **Covered Entities:** The NDB scheme applies to entities already obligated under the Privacy Act to secure personal information. Exempt entities under the Privacy Act are also exempt from the NDB scheme.
- **When to Report a Data Breach:**
  - If an organization suspects a breach, it must quickly evaluate the incident to determine if it qualifies as an eligible data breach likely to cause serious harm.
  - **Eligible Data Breach Criteria:**
    - **Unauthorized Access/Disclosure:** Personal information is accessed or disclosed without authorization, or is lost.
    - **Potential for Serious Harm:** The breach is likely to result in serious harm to individuals.
    - **No Remedial Prevention:** The entity cannot mitigate the risk of harm through immediate corrective action.

# Privacy Act
# - Notifiable Data Breaches (NDB) scheme

| Whom | When | How | What |
|---|---|---|---|
| OAIC | Entities must prepare and give a copy of the statement to the Commissioner as soon as practicable after **becoming aware of the eligible data breach** | The OAIC has an online form for entities to lodge all eligible date breach statements under section 26WK of the Privacy Act. | ✓ your organisation or agency's name and contact details<br>✓ a description of the data breach<br>✓ the kinds of information involved<br>✓ recommendations about the steps individuals should take in response to the data breach. |
| Affected individuals | Entities must notify individuals **as soon as practicable after** completing the statement prepared for notifying the Commissioner | Three Options:<br>• Notify All Individuals<br>• Notify Only Those at Risk<br>• Publish Notification<br>  • Uploading the statement alone **isn't enough**.<br>  • Actively share the breach details to reach those at risk.<br>  • Make the statement easy to find.<br>  • Keep it on the website for at least 6 months (**Recommended**). | |

# Privacy Act
# - Case Study: 2022 Medibank Data Breach

- **Incident Summary:** In October 2022, Medibank experienced a significant data breach due to a ransomware attack by the REvil group, affecting 9.7 million customers. Medibank refused to pay a $10 million ransom, leading to the exposure of sensitive personal data on the dark web.
- **Legal and Regulatory Response:**
  - **OAIC Lawsuit:** The Office of the Australian Information Commissioner (OAIC) filed a lawsuit against Medibank, accusing it of failing to protect customer data as required under APP 11.1.
    - *"if an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: from misuse, interference and loss; and from unauthorised access, modification or disclosure".*
  - **Potential Penalties:** Medibank could face penalties up to $2.22 million per breach under Section 13G of the Privacy Act 1988.

https://www.cyberdaily.au/government/10592-oaic-releases-statement-on-medisecure-data-breach

# Privacy Act
# - Case Study: 2022 Medibank Data Breach

- **Key Events Leading to the Breach:**
  - **Initial Vulnerability:** Before August 2022, a third-party contractor was granted extensive admin access to Medibank's network. The contractor's login credentials were saved on his browser and later synced to his personal computer, creating a significant security risk.
  - **Credential Theft:** In early August, a hacker stole these credentials through malware, giving them access to most of Medibank's systems, including critical management consoles and databases.
- **Timeline of the Attack:**
  - **Unauthorized Access:** On 12 August, the hacker tested their access to Medibank's Microsoft Exchange server, and by 23 August, they accessed the network via the company's VPN, which lacked multifactor authentication.
  - **Security Alerts Ignored:** Medibank's security software detected the intrusion on 24-25 August, but the alerts were not properly escalated or investigated, allowing the hacker to remain undetected for over a month.
- **Impact of the Breach:**
  - **Data Exfiltration:** From 25 August to 13 October 2022, the hacker extracted 520 GB of sensitive data, including personal and health information of nearly 10 million customers.
  - **Delayed Response:** Medibank only became aware of the data breach in mid-October, days before the hacker publicly demanded a ransom and eventually released the stolen data on the dark web.
- **Allegations by the Australian Information Commissioner:**
  - **Inadequate Cybersecurity Measures:** The AIC claims that Medibank failed to adequately protect the personal information it held, citing insufficient investment in cybersecurity resources and poor management of information security risks.

https://www.oaic.gov.au/__data/assets/pdf_file/0025/221974/Australian-Information-Commissioner-v-Medibank-Private-Limited-concise-statement.pdf

# Privacy Act
# - Upcoming Reforms

- **End Small Business Exemption:** Impact approximately 2.3 million businesses, representing 95% of all Australian businesses
- **Rationale for Change:**
  - **Increased Cyber Risks:** Small businesses are increasingly targeted by cybercriminals due to perceived weaker defenses.
    - With the rise of online transactions and cloud computing, even small businesses now pose privacy risks.
  - **International Standards:** Unlike Australia, major global privacy laws like the GDPR, CCPA, and Canada's PIPEDA do not exempt small businesses from compliance.
    - Aligns with international norms and may facilitate trade with regions like the EU.
- **Impact on Small Businesses:**
  - **New Obligations:** Small businesses would need to comply with Australian Privacy Principles, including handling personal data such as IP addresses and device identifiers, conducting privacy audits, and implementing data protection measures.
  - **Compliance Costs:** Adapting to these new requirements could impose significant costs, including training, policy development, and secure data management.
- **Preparing for Change:** Small businesses should start preparing by conducting data inventories, updating privacy policies, ensuring informed consent, and setting up systems for data protection and breach reporting.

https://iapp.org/news/a/amending-australias-privacy-act-small-businesses-bigger-responsibilities

# Privacy Act
# - Upcoming Reforms

- **Other Key Reforms**
  - **Stricter Data Breach Reporting:**A proposed 72-hour notification window for reporting eligible data breaches to the regulator.
  - **Expanded Individual Rights:**Introduction of new rights, such as enhanced control over personal data and a "right to be forgotten."
  - **Children’s Online Privacy Code:**Development of specific regulations to protect children’s data in online services.
  - **Stronger Enforcement Powers:**New penalty tiers and enhanced powers for the privacy regulator to enforce compliance more effectively.

https://insightplus.bakermckenzie.com/bm/data-technology/australia-government-responds-to-proposed-changes-to-australias-privacy-regime

# Consumer Data Right (CDR) scheme

- **Overview of the CDR Scheme:**
  - **Empowering Consumers:** The Consumer Data Right (CDR) allows individuals and businesses to securely share their data with accredited third parties, giving them greater choice, control, and convenience in managing their information.
  - **Sector-by-Sector Rollout:** Initially implemented in banking and energy, the CDR will gradually expand to other sectors, enhancing its value for consumers over time.
- **Key Features:**
  - **Opt-In Service:** Participation in the CDR is voluntary. Consumers choose who can access their data, what specific data is shared, and for how long.
  - **Enhanced Comparisons:** CDR simplifies product and service comparisons, helping users find better deals, manage finances, and access tailored services with ease.
  - **Data Security:** CDR includes strict privacy safeguards, with businesses required to follow rigorous data security standards, ensuring that personal information is handled responsibly.

# Consumer Data Right (CDR) scheme

- **Data Protection and Privacy:**
  - **Accredited Data Recipients:** Only businesses accredited by the Australian Competition and Consumer Commission (ACCC) can handle CDR data, ensuring they meet stringent requirements for data security, consent, and privacy protection.
    - IT requirements for data recipients | Consumer Data Right (cdr.gov.au)
  - **Data Deletion and De-Identification:** Consumers can request the deletion or de-identification of their data when it is no longer needed. Businesses must follow strict protocols to ensure data cannot be traced back to individuals.
- **Benefits for Consumers:**
  - **Enhanced Choice:** Easily compare products and services, leading to better value and more personalized offerings.
  - **Control Over Data:** You decide who can access your data, what data they can see, and for how long.
  - **Secure Data Sharing:** Data is transferred securely, with strong privacy and security measures in place.
  - **Time-Saving:** Modern technology streamlines the process of comparing products, reducing the time spent on manual research.
  - **Increased Competition:** The CDR fosters innovation and competition, leading to improved products and services.

# Consumer Data Right (CDR) scheme -Recent Cases

- **Case 1: HSBC Fined for Data Inaccuracies**
  - **Issue:** HSBC was fined $33,000 by the ACCC for failing to provide accurate mortgage rates and credit card balances through the CDR system.
  - **Consumer Impact:** Incorrect data could mislead consumers, affecting their financial decisions.
  - **ACCC's Position:** Accurate, up-to-date data is crucial for the effectiveness of the CDR, especially in helping consumers navigate financial choices.
- **Case 2: iSignthis Denied CDR Accreditation**
  - **Issue:** ACCC refused accreditation to iSignthis due to inadequate data security measures, lack of insurance evidence, and concerns about its suitability as a data recipient.
  - **Significance:** This was the first denial of CDR accreditation, underscoring the ACCC's strict standards for data protection and compliance.

# Cybercrime

- **What is Cybercrime?**
  - **Definition:** Cybercrime involves criminal activities where a computer or network is integral to or the target of an offense, often affecting individuals' data, reputation, or safety.
  - **Types of Cybercrime:** Includes hacking, cyberbullying, unauthorized data modification, distributed denial of service (DDoS) attacks, online fraud, identity theft, and the non-consensual sharing of intimate images.
- **Legal Framework in Australia:**
  - **Comprehensive Legislation:** Cybercrime is addressed under the Criminal Code Act 1995, with laws criminalizing unauthorized data access, telecommunication misuse, and the distribution of malicious software.
  - **State and Territory Laws:** Complementary laws exist across states and territories, covering additional cybercrime-related offenses and enhancing the national legal framework.
- **Key Developments:**
  - **Cybercrime Act 2001:** Modernized computer-related offenses and updated search powers to adapt to technological advancements.
  - **International Cooperation:** Australia is a signatory to the Council of Europe's Convention on Cybercrime, ensuring international collaboration in combating cybercrime.
- **Reporting and Support:**
  - **Incident Reporting:** Victims of cybercrime can report incidents to the Australian Cyber Security Centre or seek support from IDCARE.
  - **Victim Protection:** The eSafety Commissioner provides resources and support for victims, particularly in cases of non-consensual sharing of intimate images.

https://www.cyber.gov.au/report-and-recover/where-get-help

# Online Safety Act 2021 (eSafety)

- **Strengthening Online Safety:**
  - **Modernized Legislation:** The Online Safety Act 2021 enhances Australia's laws to address the evolving threats in the digital world, expanding protections for both adults and children.
  - **Expanded eSafety Powers:** The Act empowers eSafety to take significant actions against online harm, positioning Australia as a global leader in online safety.
- **Key Changes in the Act:**
  - **Adult Cyber Abuse Scheme:** Introduces a world-first scheme to address online abuse targeting adults
  - **Broadened Cyberbullying Coverage:** Extends protections for children beyond social media to other online platforms.
  - **Image-Based Abuse Updates:** Strengthens measures to remove non-consensual intimate images or videos shared online.
  - **Blocking Harmful Content:** Internet service providers can be required to block access to content depicting violent acts like terrorism.

# Online Safety Act 2021 (eSafety)

- **Basic Online Safety Expectations:**
  - **Increased Accountability:** Online service providers must proactively protect users from harmful content and conduct, with new civil penalties for non-compliance.
  - **Transparency and Reporting:** Providers are required to report on their safety practices, with eSafety empowered to publish compliance statements and name non-compliant services.
- **Mandatory Industry Codes:**
  - **Applicability Across Sectors:** New industry codes apply to various segments, including social media, messaging services, search engines, and app distribution platforms.
  - **Content Detection and Removal:** Providers must detect and remove illegal content, such as child sexual abuse material and terrorism-related content, and protect children from age-inappropriate material.
  - **Enforcement Mechanisms:** Codes are enforceable through civil penalties and injunctions, ensuring compliance and a safer online environment.
- **Safety by Design Initiative:**
  - **Proactive Safety Measures:** Encourages embedding safety into the design and development of online products, anticipating risks before they arise.
  - **Focus on Positive Online Experiences:** Aims to create a safer, more responsible online environment by fostering accountability and prioritizing user safety from the outset.

# Online Safety Act 2021 (eSafety) - Recent Enforcement Cases

- **Case 1: Social Media Platform X Fined for Non-Compliance**
  - **Issue:** X (formerly Twitter) was fined $610,500 by the eSafety Commission for failing to cooperate in a probe into anti-child-abuse practices.
  - **Lack of Transparency:** X did not provide sufficient information about its trust and safety measures, raising concerns about its ability to protect against child sexual exploitation.
  - **Consequences:** X faces further penalties if it fails to pay the fine, with potential civil proceedings that could increase the financial penalty to up to $780,000 per day.
- **Case 2: Deepfake Pornography and Contempt of Court**
  - **Issue:** Antonio Rotondo sued for creating and distributing deepfake pornography of Australian women, including public figures.
  - **Serious Charges:** Rotondo violated court orders by continuing to distribute images and was fined $25,000 for contempt.
  - **Potential Consequences:** Rotondo is facing additional charges, including creating obscene publications involving minors, marking a significant legal precedent in prosecuting deepfake crimes.

# Regulations on telemarketing and e-marketing

- **Key Legislation:**
  - **Do Not Call Register Act 2006 & Regulations 2017:** Governs the Do Not Call Register, enabling individuals to opt out of unsolicited telemarketing calls.
  - **Telecommunications Standards:** Includes the Telemarketing and Research Calls Industry Standard 2017 and Fax Marketing Industry Standard 2021, setting rules for telemarketing practices.
  - **Spam Act 2003 & Regulations 2021:** Regulates the sending of commercial electronic messages, prohibiting unsolicited spam without consent.
- **Telemarketing Calls:**
  - **Definition:** Any call with a purpose of promoting, advertising, or offering goods, services, or solicitations, including robocalls and automated messages.
  - **Compliance:** Calls must adhere to regulations, especially if they involve commercial content, and require consent if targeting numbers on the Do Not Call Register.
- **E-Marketing:**
  - **Definition:** Includes emails, SMS, and instant messages with commercial intent, such as promoting goods or services.
  - **Consent Requirement:** Express consent must be obtained before sending e-marketing messages, including to businesses, to comply with the Spam Act.

# Regulations on telemarketing and e-marketing

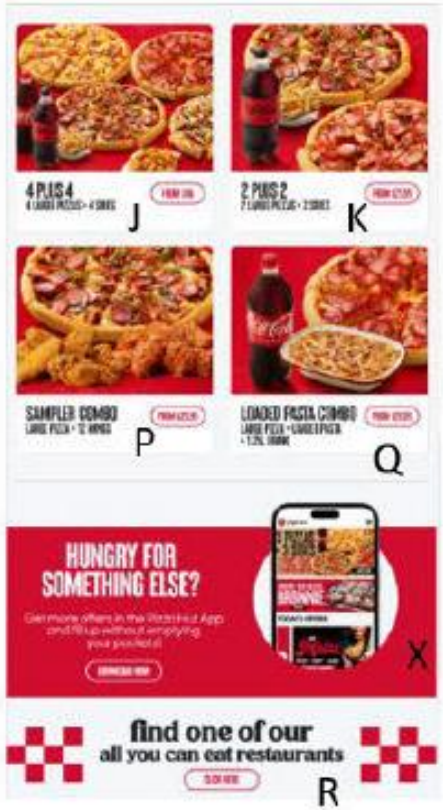
- **Consent Types:**
  - **Express Consent:** Direct, explicit permission from the recipient, such as signing up for a newsletter or ticking a box online.
  - **Inferred Consent:** Based on an existing relationship and reasonable expectation of receiving related marketing, though less reliable than express consent.
- **Do Not Call Register:**
  - **Purpose:** A secure database where consumers can register their numbers to avoid unsolicited telemarketing calls. Over half of active numbers in Australia are registered.
  - **Compliance for Businesses:** Telemarketers must check their call lists against the register within 30 days and avoid contacting registered numbers to prevent penalties.
- **Spam Act Compliance:**
  - **Unsolicited Messages:** Prohibits sending unrequested commercial messages. Businesses must obtain either express or inferred consent.
  - **Sender Identification:** Messages must clearly identify the sender and provide accurate contact information.
  - **Unsubscribe Requirements:** Every commercial message must include a functional and straightforward unsubscribe option that remains active for at least 30 days.
- **Penalties and Enforcement:**
  - **Compliance Monitoring:** The Australian Communications and Media Authority (ACMA) monitors and enforces compliance, using tools like warnings, investigations, and penalties.
  - **Risks of Noncompliance:** Businesses that violate these regulations may face significant fines and reputational damage.

# Regulations on telemarketing and e-marketing -Pizza Hut Australia - Spam Act Violation

Example 1:

From: Pizza Hut Australia <deals@deals.pizzahut.com.au>
Subject: Start your week with your favorite food delivered to your doorstep!







https://www.acma.gov.au/sites/default/files/2024-05/REDACTED%20Pizza%20Pan%20Group%20-%20Spam%20investigation%20-%20Final%20Investigation%20Report.pdf

# Regulations on telemarketing and e-marketing -Pizza Hut Australia - Spam Act Violation

- **Massive Non-Compliance:** Pizza Hut Australia was fined over $2.5 million for sending more than 10 million marketing messages in four months, with nearly half lacking an unsubscribe option.
- **Consent Issues:** Over 5.9 million messages were sent to individuals who either had not given consent or had withdrawn it, violating the Spam Act's consent requirements.
- **Ignored Warnings:** ACMA had issued 15 compliance alerts regarding 39 consumer complaints before launching a formal investigation.
- **Consequences and Remediation:**
  - **Penalty and Undertaking:** In addition to the fine, Pizza Hut must appoint an independent consultant to review and improve its compliance practices and report regularly to ACMA over the next three years.
  - **Company Response:** Pizza Hut attributed the issue to a system error and has committed to rectifying its marketing practices to meet legal and customer expectations.

https://www.abc.net.au/news/2024-05-16/pizza-hut-fined-2-5-million-for-spamming-customers/103854882

# Regulations on telemarketing and e-marketing -Pizza Hut Australia - Spam Act Violation

Example 1:


https://www.acma.gov.au/sites/default/files/2024-05/REDACTED%20Pizza%20Pan%20Group%20-%20Spam%20investigation%20-%20Final%20Investigation%20Report.pdf

# Rules and Industry Code to Combat Scam Calls and SMS

- **Strengthening Consumer Protection:**
  - **Telecommunications Service Provider (Customer Identity Authentication) Determination 2022:** Introduces multi-factor authentication for high-risk transactions like SIM-swap requests and account changes, aimed at preventing identity theft and financial fraud.
  - **Impact of SIM-Swap Scams:** These scams allow fraudsters to take control of a victim's phone number, leading to unauthorized access to online banking and significant financial losses.
- **Combatting SMS Scams:**
  - **Reducing Scam Calls and Scam Short Messages Industry Code:** Requires telcos to identify, trace, and block SMS scams, addressing the rise in such scams, which accounted for 32% of all reported scams in early 2022.
  - **Industry Collaboration:** Developed in partnership with the Communications Alliance, building on the success of the 2020 industry code targeting scam calls.
- **Results and Enforcement:**
  - **Proven Effectiveness:** Since the introduction of the scam call reduction code in 2020, telcos have blocked over 549 million scam calls, significantly reducing complaints.
  - **Ongoing Efforts:** Telcos must also provide customers with information on managing and reporting SMS scams, share data on scam messages, and report identified scams to authorities, further tightening protections.
- **Proposed Legislation:**
  - **SMS Sender ID Register:** The Albanese Government is introducing legislation for a new register to combat SMS impersonation scams. This register will allow telcos to verify whether SMS messages sent under a brand name are legitimate, helping to block or warn against fraudulent messages.
  - **Pilot and Future Steps:** A pilot register was launched in December 2023 with participation from major brands. The government is reviewing feedback to decide whether the register will be mandatory, as part of a broader strategy to disrupt scam activities.

# Recent Compliance Failures in Telecom Industry

**Case 1: Symbio's Breach of Scam Rules**

- **Non-Compliance:** Failed to share scam call info promptly with telcos and ACMA.
- **Impact:** Delayed action against scams; weakened system effectiveness.
- **ACMA Warning:** Potential penalties up to AUD 250,000 for future breaches.

**Case 2: Telstra's SIM-Swap Scam Vulnerability**

- **Fine:** $1,551,000 for inadequate customer ID authentication.
- **Risk:** 168,000 high-risk interactions; exposed customers to SIM-swap fraud.
- **Remedial Action:** Two-year undertaking; independent review of compliance.

# Security of Critical Infrastructure Act 2018

- **Critical Infrastructure:**
  - **Broad Definition:** Includes physical facilities, supply chains, IT systems, and communication networks that, if compromised, could significantly harm the nation.
  - **Interconnected Systems:** Failure in one sector (e.g., energy) can cascade, affecting healthcare, transport, and financial services, emphasizing the need for robust security measures.
- **Purpose of SOCI:**
  - **Protect Critical Infrastructure:** Ensures resilience and protection of essential assets and services, safeguarding Australia's society, economy, and security.
  - **Prevent Cascading Consequences:** Aims to mitigate widespread disruptions and maintain public trust in the government's emergency response capabilities.
- **Applies to 22 Asset Classes in 11 Sectors:**
  - Communications, Data Storage, Defence Industry
  - Higher Education, Energy, Financial Services
  - Food and Grocery, Healthcare, Space Technology
  - Transport, Water and Sewerage

# Security of Critical Infrastructure Act 2018 - Positive Security Obligations

- **Register of Critical Infrastructure Assets:**
  - Requirement: Entities must report ownership, operational, and control information to the government.
  - Purpose: Helps the government understand interdependencies and manage risks.
  - Confidentiality: Information in the register is protected and not publicly accessible.

- **Mandatory Cyber Incident Reporting:**
  - Reporting Timeframes: Critical incidents with significant impacts must be reported within 12 hours; others within 72 hours.
    - Significant Impact: Disruption that materially affects the availability of essential services provided by the critical infrastructure asset.
    - Relevant Impact: Affects the availability, integrity, reliability, or confidentiality of the asset.

- **Critical Infrastructure Risk Management Program (CIRMP):**
  - Requirement: Responsible entities must establish and maintain a written CIRMP.
  - Objective: Identify and mitigate material risks (physical, cyber, supply chain) to critical infrastructure assets.

# Security of Critical Infrastructure Act 2018

- **Government Assistance Measures:**
  - **Information Gathering:** Authorities may direct entities to provide necessary information during incidents.
  - **Action Directions:** Directives to take or refrain from specific actions during emergencies.
  - **Intervention Requests:** Government intervention to manage incidents impacting national security.
- **Enhanced Cyber Security Obligations (ECSO):**
  - **Applies to Systems of National Significance:** Critical systems identified as the most crucial to the nation, due to the cascading consequences that may occur if disrupted
  - **Key Requirements:** Include incident response plans, cyber security exercises, vulnerability assessments, and provision of detailed system information to the government.