

**SIDE 1/2**

THE TOOLKIT &amp; THE MAP ·

Fluid data ecology · Sovereignty · Jurisdiction · Regulation models · EU/GDPR · US/UK/AU ·

Africa · Asia

100% ASSIGNMENT · NO EXAM

Compiled by AskSia · mapped to the MECM90002 curriculum ·

asksia.ai/cheatsheet/unimeLb-mecm90002

**0 · How to Use This**

READ FIRST

★ This subject is graded **entirely by writing & a pitch — no exam**: an **argumentative essay (50%, 2500w)**, an **oral presentation (25%, ~3 min · 3 slides)**, and a **written case study (25%, 1500w)**. Hurdles: **≥80% tutorial attendance** + submit every piece.

The marked skill is *narrowing a huge global debate into one sharp, evidence-backed policy argument*. So this sheet is a **thinking + citing bank**: the toolkit + the regional map (Side 1), the scholars, cases & writing engine (Side 2).

-----  
**SIA** → *The whole subject is one move: **pick a region/case, name a specific problem, argue a targeted intervention**. **Description loses marks; analysis ("so what for power, rights, the public interest?") wins them.***

**1 · The Big Picture**

W1–2

Old media (TV, radio, print) was **bounded & territorial** — easy for a nation to regulate. Today's data is the **fluid data ecology**: it sits on servers anywhere, **constantly crosses borders**, and it's unclear where it's stored or who can access it (cloud, IoT, 5G). That fluidity **breaks nation-bound regulation** — the core problem of the whole subject.

**Governance ≠ government**. Government = the state's law over its territory. **Governance** = multi-actor steering by states + IGOs (UN/ITU/OECD) + blocs (EU) + platforms + civil society.

**The course's spine = a spectrum**: **EU rights-based** - **US/UK/AU market-based** - **Global South** (Africa/Asia/LatAm) navigating development, sovereignty & platform power.

**1b · How the Subject Maps**

PARTS

The semester runs in three movements — strong essays keep all three live:

- Concepts (W1–4)** — fluid data ecology, sovereignty, jurisdiction, monopolies
- Regions (W5–10)** — the comparative tour: EU → US/UK/AU → Africa → Asia → LatAm
- Global & future (W11–12)** — IGOs, intervention types, AI & data divides

**The through-question**: in a borderless data world, **who should govern data — the nation-state, the market, or a global order — and how?** Every assignment is a focused answer to this.

**1c · The Core Tension**

YOUR COMPASS

Every topic is a clash of **two truths**: data is **borderless** (flows ignore the map) but law is **territorial** (states rule patches of ground). Whoever you back to resolve it — nation, market, or global body — becomes your thesis.

Reading any case, ask: *which actor asserts control, over what, and at whose expense?*

**2 · Core Concepts I**

W2–4

**Datafication** · converting everyday life & behaviour into machine-readable, monetisable data points (Mejias & Coudry; platforms "colonise" the net).

**Sovereignty** (classical) · supreme authority of a state over its land & people, free of outside interference — since Westphalia (1648). Grimm: it's no fixed meaning & is eroding as states cede power upward.

**Data / digital sovereignty** · the claim to control data, infrastructure & standards. **Plural & contested** (Couture & Toupin): **national** (localisation, sovereign cloud), **individual/subjective** (Estonia e-ID),

**Indigenous** (Māori data), even **platform** sovereignty. **Jurisdiction** · a court's right to apply & enforce law over subject matter in its territory (procedural · substantive · enforcement). **Online tension**: the net is global, but jurisdiction presumes a world cut into territories — hard to "anchor."

**Extraterritoriality** · a state reaching beyond its borders — e.g. Australia's Assistance & Access Act 2018 catches anyone with one Australian end-user.

**2b · The Framing Theory**

W1 · CITE-READY

**Network society** · Castells — power & production run through global "flows" that transcend time & space, weakening the nation-state's grip. Van Dijk: a "culture of connectivity"; Volkmer: an emerging **global public sphere**.

**Deterritorialisation** · new data "territories" where **"code is law"** (Lessig) — software logic shapes the communicative space & shrinks sovereign power (Volkmer).

**Surveillance capitalism** · Zuboff — human behaviour captured as raw material for prediction products; the economic engine beneath datafication.

**2c · Sovereignty · 4 Types**

USE PRECISELY

| TYPE       | CLAIM / EXAMPLE                               |
|------------|---|
| National   | localisation, sovereign cloud (China, Russia) |
| Individual | control your own data (Estonia e-ID)          |
| Indigenous | peoples own data about them (Māori)           |
| Platform   | Big Tech's de-facto rule-setting              |

**2d · Claiming Jurisdiction**

4 BASES

- Territorial** — acts on your soil
- Nationality** — your citizens, anywhere
- Effects** — harm felt in your territory
- Universal** — piracy, war crimes, genocide

Online all four strain at once ⇒ the **TikTok & GDPR fights are really jurisdiction fights**. The deeper point: control follows whoever can *enforce*, not whoever claims the right.

**3 · Core Concepts II**

W2–5

**Transborder data flows** · data moving across borders. Conceptually muddy (Kuner): no shared definition of a "transfer," and **"data transit" is largely unregulated** — data crosses borders continuously, not by a button-press.

**Data localisation** · law requiring citizens' data be stored on in-country servers (Russia's Sovereign Internet; China's 2017 Cybersecurity Law — "data comes in but can't get out"). A core sovereignty tool; risks a *splinternet*.

**Data monopolies / gatekeepers** · Big Tech (Alphabet, Apple, Amazon, Meta, Microsoft, ByteDance...) with gateway power. Pickard: "vertically integrated monstrosities" wielding power "incompatible with a functioning democracy." EU law names them **gatekeepers**.

**Public vs private power** · the worry that states have ceded too much to platforms acting as de-facto centers → an "accountability deficit." Floridi: a "good AI society" can't be left to the market.

**Data colonialism** · extracting data/value from the Global South & Indigenous peoples, reproducing colonial asymmetries (Mejias & Coudry).

**3b · Platforms & the Public**

W2–3

**Intermediaries** · platforms that host & curate content. Their architecture only *partly* allows the central control old media law assumes ⇒ **"many hands"** / cooperative responsibility (Helberger, Pierson & Poell 2018).

**Public interest / public good** · the democratic value data should serve — quality information, equity, protection. Pickard: markets **underproduce** the information democracy needs. Tisman: AI choices are "collective choices — society must stay in control."

**Splinternet** · the risk that data-localisation & rival national rules fragment one global internet into walled national ones.

**3c · The Fluid Ecology in Practice**

CONCRETE

**Cloud** — AWS ~29% · Azure ~20% · Google ~13%; a 2025 AWS outage "broke half the internet." **IoT & 5G** — under-regulated consumer devices. **Datified cars** — "computers on wheels" (Tesla footage leak; VW GDPR fine). **Smart speakers** — Alexa recordings used for AI training.

All show one thing: **data is generated everywhere, stored anywhere, governed by no single map.**

**3d · Who's Responsible?**

THE DEFICIT

Old media law pins responsibility on **one actor** (an editor, a controller). Platforms' scale + layered architecture mean no single actor fully controls content ⇒ a **"responsibility gap"** (Helberger's "many hands") — states cede too much to platforms as de-facto censors.

**4 · The Regulation Models**

THE ANALYTICAL GRID

Every essay leans on one axis. **By philosophy**:

| MODEL                | CENTRES                         | HOME          |
|----------------------|---------------------------------|---------------|
| <b>Rights-based</b>  | citizen / data subject, privacy | EU            |
| <b>Market-based</b>  | free flow, trade, deregulation  | US            |
| <b>State-control</b> | govt primacy, security/ideology | China, Russia |

**By who sets the rules**: **self-regulation** (industry codes; "censors by proxy") · **state regulation** (hard law; risks censorship/splinternet) · **co-regulation** (industry code + state oversight; Obia: "ill-fitting") under North–South power gaps).

**By scale**: national (protect culture/security now) vs global/multi-stakeholder (threats are transnational; uncoordinated fixes → a "legal arms race") the bind (Volkmer): *"states solve global problems through a national lens."*

**5 · Key Debates**

W3, 5

**Regulate data monopolies — necessary & possible?** Yes (too big, market fails the public interest). But hard (global span, layered architecture; old law assigns one responsible actor — Helberger's "many hands"). Breakup "won't fix information problems" (Pickard).

**Power persists (W5)**: today's submarine cables map onto the 19th-C British telegraph (~60% British-owned by 1891) — early advantage entrenches the strong; the *McBride Report* (1980) voiced the Global-South critique.

**5b · "Breaking Points"**

W4

Where fluid data snaps the old sovereignty/jurisdiction frame:

- Civic data spaces must be both **enabled & safeguarded** by democratic states
- No agreed meaning of a "data **transfer**" (Kuner)
- "Data **transit**" undefined & unregulated
- Deterritorialisation** — platform, subjective & Indigenous sovereignties emerge

**SIA** → *Name which model + which breaking point your case sits on — markers reward that precision over a general "the internet is hard to regulate."*

**5c · National Quick-Fixes**

THE RISK

When each state "solves" global problems alone, uncoordinated rules collide into a **"legal arms race"** that "favours the rules of the strongest" (Global Status Report 2019) — and can fragment the net. The pro-global answer: multi-stakeholder bodies (UN Global Digital Compact; OECD AI Principles).

**6 · Europe / GDPR**

W7 · RIGHTS-BASED

The EU = a **"Regulatory Superpower"** with a rights-based, citizen-centred model that "puts people first." Treats the citizen as citizen-AND-consumer (a neoliberal merge — Ranchordas).

**GDPR** (in force 25 May 2018), "the toughest privacy law in the world," builds rights around the **data subject**: access, rectification, **erasure ("right to be forgotten")**, restriction, portability, objection, limits on automated profiling. Roles: data subject · controller · processor · DPO.

**The Brussels effect** · GDPR spreads worldwide — any firm processing EU data must comply (Cervi 2022: GDPR-style laws followed across Africa/Asia/LatAm; the US still has **no federal privacy law**).

**Also**: DSA (2024, platform content rules, VLOPs), DMA (2024, "gatekeepers" — interoperability, no self-preferencing), AI Act (2024, risk tiers).

**Cases**: Google Spain (right to be forgotten, 2014); Netflix €4.75m; TikTok €500m (EU → China transfers); X €120m (DSA, 2025).

**6b · GDPR Roles**

KNOW WHO'S WHO

- Data subject** — the identifiable person
- Controller** — decides why/how data is processed
- Processor** — processes on the controller's behalf
- DPO** — the compliance officer firms must appoint

Given a scenario, **name each role** — a guaranteed analysis point in any EU-data case.

**7 · USA · UK · Australia**

W8 · MARKET-BASED

**US** · liberal/free-market self-regulation (Locke; limited gov). Pillars = **free speech (1st Amendment)** + **antitrust** (Sherman Act 1890). No federal privacy law — only state laws (CCPA). Section 230 shields platforms. *Net neutrality* flip-flops (Title II 2015 → repealed 2018). *US v. Google* (2025): monopolised ad-tech.

**UK** · *"duty of care"* / online-harm model → **Online Safety Act**, enforced by Ofcom.

**Australia** · selective interventionism: Online Safety Act 2021, **News Media Bargaining Code** (Google paid; Meta "went dark"), eSafety Commissioner/ACMA/ACCC, **under-16 social-media ban** (Dec 2025).

**7b · The US Pendulum**

WHY IT SWINGS

Bodies: **FTC** (antitrust + consumer), **FCC** (spectrum/broadband). Politics flips the dial — Obama-era net-neutrality (internet as utility) → Trump-era deregulation ("AI free from ideological bias"; Meta drops fact-checking, 2025).

**EU vs US in one line**: the EU regulates to protect *rights*; the US deregulates to protect *markets & speech*.

**8 · Africa**

W6 · BETWEEN PARADIGMS

Navigates between the colonial "development-communication" legacy & mobile-first "leap-frogging." **Double colonisation**: old empire + new dependency on Western Big Tech (undersea cables, cloud — Mwema & Birhane).

Challenges: 55-state harmonisation, connectivity/*digital divide*, election-time **internet shutdowns**, low-resource-language moderation gaps, cheap data-labour. Framework: **AU Digital Transformation Strategy 2020–30** (Digital Single Market). Contrast: Kenya (model · "Silicon Savannah" · M-Pesa · Ushahidi) vs Rwanda & Uganda (state-led, "Not Free").

**9 · Asia**

W9 · CONTROL VS COMMERCE

**No GDPR-equivalent**; a mix of democratic, authoritarian & semi-authoritarian systems. Spine = **mis/disinformation** + rising **digital authoritarianism** (shutdowns, surveillance). Mis = false/unintentional; dis = false/intentional (Wardle & Derakhshan typology).

**China** state-control/cyber-sovereignty (Great Firewall; lowest Freedom House). **India** highest disinfo risk (WhatsApp). **Pakistan** PECA + 2021 blocking rules (X blocked). **Indonesia** paid "buzzers." Soft law: ASEAN fake-news guideline.

**10 · Latin America**

W10 · POPULISM VS PLATFORMS

Post-colonial legacy + unstable democracies + concentrated media. Accepts **"digital corporate sovereignty"** (Becerra & Waisbord) — platforms become gatekeepers of discourse. Weak regulation; **Brazil's LGPD** is the region's GDPR-style law.

**Cases**: El Salvador (Bukele · Pegasus spyware); Venezuela ("Patria") digital ID as surveillance); **Brazil's X/Musk vs Justice de Moraes** (2024 — sovereignty vs free speech); Mexico sues Google ("Gulf of America").

**10b · The Global South Lesson**

SYNTHESISE

Across Africa, Asia & LatAm one pattern recurs: **weak or absent national regulation + dependence on Western Big Tech** ⇒ platforms become de-facto sovereigns of the public sphere. The "intervention" is often **building capacity**, not just passing a law — a sharp angle for an essay.

**10c · Reading a Region**

A METHOD

For any region, pin four things: its **philosophy** (rights / market / state-control), its signature **law**, a  **vivid case**, and a **scholar**. **That quartet = a ready-built body paragraph**. Then contrast two regions to show you grasp the *spectrum*, not one dot on it.

**SIDE 2/2** APPLY & WRITE · IGOs & interventions · The future · Scholar bank · Case bank · The essay · Presentation · Case study · Argument craft · Integrity

**100% ASSIGNMENT · NO EXAM**

Compiled by **AskSia** · mapped to the MECM90002 curriculum · asksia.ai/cheatsheet/unimeLb-mecm90002

## 11 · IGOs & Interventions W1.1

**Inter-governmental bodies:** UN agencies — **ITU** (1865, spectrum/telecoms), WIPO, UNESCO; thematic — **OECD** (AI Principles 2019, first intergov. AI standard); WTO/GATS (trade lens).

**Soft vs hard law:** soft = non-binding, fast, flexible (OECD AI Principles, guidelines); hard = binding treaty (Budapest Cybercrime Convention).

**4 intervention levels** (Gorwa, platform governance) — a ready essay frame:

- Government** — laws, bans, taxes, infrastructure, co-regulation
- Platform** — moderation, ToS, oversight boards, ad libraries
- IGO** — soft/hard law, summit diplomacy
- Civil society** — petitions, submissions, campaigns, protest

## 11b · Interventions · Examples BY LEVEL

- Govt** — EU GDPR/DSA/DMA · AU Online Safety Act · Pakistan blocking rules
- Platform** — Meta Oversight Board · Community Notes · ad libraries
- IGO** — OECD AI Principles · UN Global Digital Compact · ITU summits
- Civil society** — Digital Rights Watch · AlgorithmWatch · petitions/submissions

## 12 · The Future W1.2

Tech outpaces regulators. Three recurring issues: **algorithmic bias** (facial recognition misreads Black faces 5–10× more — Buolamwini; Noble), **data divides** (Global South as raw-data provider), and **individual data sovereignty** beyond GDPR.

- AI scraping** — Meta trains on Insta/FB data; EU can opt out, elsewhere unclear
- "Ethical coding"** — who supervises the coder? AI built in West/China; Global South a "receiver" → new infrastructure colonisation
- Beyond law** — dynamic consent, usage control, federated identity

## 11c · Soft vs Hard Law KNOW THE TRADE

|          | SOFT LAW           | HARD LAW            |
|----------|--------------------|---------------------|
| Form     | guidelines, codes  | treaty, statute     |
| Binding? | no                 | yes                 |
| Speed    | fast, flexible     | slow, durable       |
| e.g.     | OECD AI Principles | Budapest Convention |

## 12c · Closing Synthesis W1.2

The wrap-up reprises the spine — EU rights vs US market vs Global-South capacity gaps — and warns that **tech keeps outrunning regulators**. Career payoff: these debates feed roles at the OECD, UNESCO, NGOs & platform policy teams.

## 13 · Scholar Bank CITE THESE

**CASTELLS** *network society*

Global "space of flows" erodes the nation-state's capacity.

**ZUBOFF 2019**

Surveillance capitalism — behaviour as raw material for prediction.

**VOLKMER 2014/21**

Global public sphere; deterritorialisation; the "national lens" bind.

**LESSIG** *Code, 2000*

"Code is law" — software architecture governs behaviour.

**BRADFORD** *Brussels effect*

EU rules become global standards via market power.

**FLEW & MARTIN 2022**

Platform regulation; the internet was never "ungoverned."

**PICKARD**

Market failure; platforms vs the public good/democracy.

**HELBERGER ET AL. 2018**

"Many hands" — cooperative platform responsibility.

**GRIMM · SHACHAR**

Sovereignty has no fixed meaning; the "shifting border."

**COUTURE & TOUPIN · KUNER**

5 senses of digital sovereignty; muddy "data transfer."

**GORWA 2019**

"What is platform governance?" — the intervention typology.

**MEJIAS & COULDRY**

Datafication & data colonialism — platforms "colonise" everyday life.

**HEADRICK · THUSSU · SCHILLER**

History — tools of empire, the US "free-flow doctrine," media imperialism.

**MACBRIDE 1980**

Many Voices, One World — the NWICO Global-South critique.

**COULDRY · FLORIDI**

The "mediated centre"; a "good AI society" can't be left to the market.

**GOLDSMITH & WU 2006**

Who Controls the Internet? — territorial law strikes back.

**MUELLER 2017**

Will the Internet Fragment? — sovereignty vs one global net.

**GILLESPIE**

Custodians of the Internet — the politics of content moderation.

## 14 · Case Bank ESSAY-READY

**PLATFORMS & ANTITRUST**

- Cambridge Analytica** — data misuse + microtargeting
- Rohingya v Facebook** (2021) — hate speech & Myanmar; \$150bn suit
- Google EU antitrust** €2.4bn; **US v. Google** 2025 ad-tech monopoly
- EU DMA gatekeepers**; Apple sideloading

**NATIONAL REGULATION**

- AU News Bargaining Code**; under-16 ban (2025)
- UK Online Safety Act**; **EU AI Act**
- France** — Toubon law; Gaia-X; Durov/Telegram

**STATE-CONTROL**

- China** Great Firewall + 2017 Cybersecurity Law
- Russia** "Sovereign Internet" (2019), DPI, MAX app
- Pakistan** PECA; **TikTok v US** (sovereignty vs security)

**GLOBAL SOUTH / INFRA**

- M-Pesa · Ushahidi · Silicon Savannah** (Kenya)
- Brazil X/Musk**; El Salvador Pegasus; Venezuela "Patria"
- Submarine cables**; ITU/INTELSAT/Starlink

**HISTORY (W5)**

- British telegraph empire** - Reuters — ~60% British-owned by 1891
- Marconi** wireless monopoly (Titanic 1912); **ITU** 1865
- McBride Report** 1980 · **WTO/GATS** — "comms as trade"

**PRIVACY & DATA**

- GDPR fines** — Netflix €4.75m · TikTok €500m · X €120m (DSA)
- Optus / Medibank** (2022) — AU breaches, cross-border data
- WhatsApp** policy — transfers data to US & other regimes

**FLUID DATA & INFRASTRUCTURE**

- Cloud** — AWS 29% / Azure 20%; 2025 AWS outage
- Huawei 5G** — banned US/UK/Japan on security
- Datified cars · Alexa** — IoT data harvesting

**RIGHTS & CONTENT**

- Google Spain** — right to be forgotten (2014)
- Meta "Community Notes"** (2025) — self-moderation pivot
- RT/Sputnik bans** — platforms as transnational arbiters

**SIA** → *One vivid case, fully analysed, beats five name-dropped. Pick the case whose tension proves your thesis.*

## 15 · A1 · The Essay 50% · 2500W

Choose **ONE of three** set questions (~20 sources; argue, don't describe):

- National rationale** — why a country still needs its own digital policy in a borderless world
- UN policymaker brief** — what to prioritise when shaping global digital rules
- Platform responsibility** — what duties a global content platform owes

**STRUCTURE**

Intro — hook · context · **thesis** · roadmap  
 Body ¶ — c**laim** · e**vidence** (c**ritical**) · t**heory** · a**nalysis** · l**ink**  
 Concl. — r**estate** · s**ynthesise** · "why it matters"

**Narrow the huge question** to one sharp, defensible scope (one region, one law, one platform) — breadth is the #1 trap.

## 16 · A2 · Presentation 25% · ~3 MIN · 3 SLIDES

Be a **policymaker**: name a specific regulatory problem & pitch an intervention. Slide 1 the case (broad) · Slide 2 the specific issue · Slide 3 the policy angle + first solutions. **Don't read slides verbatim** (mark penalty). Feeds directly into A3.

## 15b · Essay Traps AVOID THESE

- Too broad** — "regulate the internet" can't be argued in 2500w
- Describing** a law instead of arguing about it
- Theory-dropping** — naming Zuboff without using her
- One region** when the question invites comparison
- No counter-argument** — strong essays answer the obvious objection

## 16b · Pick Your Question ALIGN A1+A2+A3

Choose the essay question whose case you can **reuse across all three tasks** — one well-chosen case (a platform, a country, an IGO) can power the essay, the pitch *and* the case study. Pick where you have **real evidence & a clear tension**, not the "easiest" topic.

## 16c · Slide Design A2 TIPS

3 slides, ~1 idea each — keep them **visual, not wordy** (reading text aloud is penalised). One clear problem statement, one concrete intervention, one "why it's feasible." Rehearse to land inside 3 minutes; the pitch is a dry-run of your A3 thesis. Practice once out loud — 3 minutes is shorter than it sounds.

## 17 · A3 · Case Study 25% · 1500W

Develop the A2 idea into a rigorous study of **one tightly-bounded case**. Pick a lane:

- Topic 1** — a company / practice / tech field × a policy dimension (e.g. a platform × misinfo moderation)
- Topic 2** — a country & one national policy — *or its absence* (the gap is the intervention)
- Topic 3** — a specific international policy/body (e.g. the UN Global Digital Compact)

**3-PART STRUCTURE**

1 describe case + why it must change  
 2 define the problem w/ real incidents  
 3 propose a concrete, **targeted** intervention

Graded on: problem & context · intervention design · **critical analysis > description** · writing & citing.

**Case study ≠ essay**: the essay *argues a position*; A3 **diagnoses one case & designs a fix**. Go **deeper, not broader** — figures/tables don't count to the word limit.

## 18c · Evidence Checklist A3

- The **law/policy text** itself (primary source)
- Real incidents** — a fine, a breach, a court case
- 2–3 scholars** framing the debate
- A **counter-view** you then answer
- A **comparator** — how another country/platform handled it

## 18 · Choosing a Case SET YOURSELF UP

- Narrow** — one figure/law/event, never "social media"
- Has a visible **tension** (sovereignty vs free flow; rights vs market)
- 2–3 set scholars genuinely apply
- Concrete evidence you can cite (law text, reports, coverage)

## 18b · Worked · Mini Case THE SHAPE

**Case:** Australia's News Media Bargaining Code.

**Problem:** platform market power starves journalism funding. **Evidence:** Google paid up; Meta "went dark," signed, then exited news (2024). **Intervention:** mandatory bargaining + final-offer arbitration. **So what:** a state forcing platform accountability — but is it durable when Meta can just drop news?

## 18d · "Targeted" Means A3 KEY WORD

Grading rewards a **narrow, feasible, specific** intervention: "regulate Big Tech" fails; "extend the bargaining code's arbitration to AI-training licensing" passes. Name the **actor**, the **mechanism**, and why it's **enforceable**.

Then pre-empt the obvious objection — feasibility & unintended effects — in a sentence.

## 19 · Argument Craft DESCRIPTION → ANALYSIS

**THESIS TEMPLATE**

"While [region/p]latform] appears to \_\_\_ , this essay argues it actually \_\_\_ , revealing \_\_\_ about [sovereignty / rights / the public interest]."

**Description** = what the policy is. **Analysis** = what it means for power, rights, who profits, who's excluded. End each ¶ on a **"so what."**

- Signpost** — topic sentence states the claim
- Critical voice** — "this suggests", "however", "more convincingly"
- Use a **model** (\$4) + a **case** (\$14) + a **scholar** (\$13) in every body ¶

**CRITICAL PHRASES · STEAL THESE**

**Contrast:** however · yet · by contrast. **Analyse:** this suggests · this reveals · which implies · more convincingly. **Engage:** as X argues · extending X · X overstates · against X.

## 20 · Referencing & Integrity DON'T LOSE EASY MARKS

~20 sources: peer-reviewed + policy docs/reports/news. Cite consistently; build a full list.

**AI policy (MPF1310):** work auto-scanned by **Turnitin AI detection**. **OK (disclose):** verify ideas, define terms, locate/summarise sources, non-AI grammar tools. **Not OK:** AI writing sentences/paragraphs, citing AI as a source, AI rephrasing/"improving" or translating your work. Declare any AI use.

## 20b · Source Mix ~20 REFS

Blend **peer-reviewed** (the set readings + beyond), **policy/law** (the GDPR text, an ACCC report), and **quality news** (Guardian, ABC). **Avoid blogs & AI output as sources**. Cite as you write — never reconstruct references at 2am.

## 21 · HD Checklist BEFORE YOU SUBMIT

- Question narrowed to one sharp scope
- Arguable thesis, answered throughout
- Model + case + scholar in each ¶
- Analysis > description; every ¶ has a "so what"
- ~20 sources, cited; AI use declared
- Counter-argument raised & answered
- Each ¶ links back to the thesis
- Within word count

**SIA** → *Read only your topic sentences end-to-end — they should tell the whole argument alone. If they don't, the structure isn't there yet.*