CONTAINMENT AND INCENTIVES
FOR AUTOMATIC ACTIVITY
WITH ‘FIVE EYES’ (AUSTRALIA) REFORM

Eric Cameron Wilson

31 July 2023

INTRODUCTION

This submission concerns the formation of AI policy and regulation in Australia and has three parts:

- ***Part A*** summaries some reported AI issues requiring urgent attention, as a prelude to three short scenario-stories illustrating where the industry, if unregulated, may go. These AI facts and scenarios are intended to prompt discussion.

- ***Part B*** discusses issues raised in Part A, including: our national interest, industrial, legal, security and Geo-political implications.

- ***Part C*** proposes government responses to the explosion of AI as described in Parts A and B, including licencing of AI involving risky practices or unrelated parties, mitigation of hostile AIs, while turbo-charging sovereign AI capabilities and assisting start-ups.

This paper does not intend to list all the benefits of AI since the industry excels at spruiking itself. Rather, what must be done to make the technology safe is considered, with a different viewpoint from those holding little allegiance to Australia.

EXECUTIVE SUMMARY

Public concern about ‘AI’ has stoked fears of mass unemployment, threats to democracy, unfair trading, suspected discrimination, privacy concerns, criminal behaviour, big tech dominance, potential abuses of market power, uncertain augmented reality, risky human implants, threats to national security and the rise of China. This all relates to one fundamental question:

How do we control technologies which though not sentient, are apparently quicker and smarter than humans, which can make decisions affecting us?

And raises related questions too:

How do we stop people using AI contrary to our way of life?
How do we not become dangerously dependent on AI?

Unless we wish to freeze our economy, inevitably, Automatic Activity will replace human workforces where all data inputs are knowable – such as sales forces, pilots, actors, financial advisors – white collar jobs where expensive robots aren’t required going first. Additionally, without workable legal protections, a handful of foreign AI-companies are set to run Australia by default. Some already have access to far more information about Australians or Australian businesses than all governments put together. Australian governments today would cease to operate without some of these international vendors, who are now entering the AI space.

But James Black, assistant director of defense and security research group RAND Europe reportedly told British parliament:

"When we talk about non-state actors that conjures images of violent extremist organizations, but it should include large multinational corporations, which are very much at the forefront of developing this technology"

The AI industry itself seeks regulation to solve its public trust problem. Some proponents of AI liken its potential destructive power to nuclear energy. Some are accused of wanting to raise the bar of regulation to shut out smaller competitors (such as nascent Australian AI companies). One large foreign company is also fighting the rest by restricting access to data to disrupt competative AI self-training. Some are calling for all training to stop until AI can be regulated.

This paper describes a legislative containment model for AI which addresses all these concerns, plus turbo-charges sovereign AI capability in the national interest. It also explores how AI initiatives incompatible with our way of life should be dealt with, including Five Eyes reforms.

The term ‘Automatic Activity’ is used to denote the conduct of AI rather than attempt a single technical definition, with various AI characteristics, technical and effectual, attributed to that term. The recommended legislative purposes are to provide a scheme of prohibition, authorisation and licencing; deterrents, remedies and protections; ensure timely human reviews, curb abuse of market power, promote privacy and the collection of data on a need-to-know basis, among other things.

The proposed scheme generally limits Automatic Activity according to data requirements. Use of an organisation’s natural internal and customer data should be largely un-affected. But automatic Activity involving children, animals, human augmentations, non-internal and non-related data, would require an AUSIndustry technical licence for research and development, and deployment, and an ACCC commercial licence for operations. It is proposed the ACCC would also licence inter-jurisdiction Automatic Activity data transfers to keep track of AI. The Minister would licence Automatic Activity for the security services, including Five Eyes intelligence operations. Licencing when required, would consider any impact on human rights and fundamental freedoms, and usually be public and reviewable.

The proposed containment model also bans all Automatic Activities seeking to exercise judicial or legislative powers, functions of review or arbitration; unlawful, unconstitutional or dishonest operation; subliminal practices or those lacking full free and informed consent; or controlling human implants.

The proposed industry support is aimed at promoting and supporting sovereign Automatic Activity capabilities, meaning free of foreign control. This includes contributions to open source, at least to the level that Automatic Activity is being offered to less-developed nations but with illiberal strings attached. Monetary incentives should be provided for novel sovereign Automatic Activity proposals benefiting arms-length third parties or members of not-for-profit organisations, as grants. Or otherwise with tax benefits / instant write-offs available were a grant is not given, plus the waiving of government charges for Automatic Activity startups and small businesses.

ABOUT THE AUTHOR

Eric Wilson is a software developer/inventor with granted patents in cloud computing, holds an Innovation and Entrepreneurship Graduate Certificate from the University of South Australia, is a startup founder and former technology journalist.

PART A: FACTS & SCENARIOS

This part explores potentially novel relationships between AIs and humans -- the good the bad and the ugly -- for which an urgent gap in policy and regulation exists:

- ***AI-Facts*** presents in a nutshell some issues concerning the public for which government action is expected.

- ***Scenario 1: Flying high with Sully-AI*** futuristically explores how closed-source AI may lead to monopolies of irreversible human dependence.

- ***Scenario 2: AI Spy v Spy*** is fiction based on present AI capabilities exploring AI security fallacies, and the hazards of trusting public-private partnerships with government business.

- ***Scenario 3: The Investment*** builds on the monopolistic hazards of Scenario 1 and the security fallacies of Scenario 2, by exploring the unregulated quest for high returns in the proposed marriage between AI and Biotech.

All the AI capabilities mentioned in Scenarios 1, 2 & 3 are in production or under active development. It’s important to realise the public expects government to control AI undertakers who as a group, are generally smarter than we are, and hold no allegiance to Australia. This part is designed chiefly as a stimulus for further discussion.

AI-FACTS

1. A man was reportedly found guilty of treason in the UK for attempting to murder Queen Elizabeth II, after allegedly being encouraged by AI to proceed with the plan. The AI was not sentient but remarkably, this was no bar to its acceptance as the attempted assailants' confidant. The undertakers of the AI were not reported as having been charged.

2. Human "mum and dad" and professional investors are now trying compete against 'Algos' (algorithms) able to trade at lightening speeds. The Algos are being given the advantage of deep learnings derived after ingesting public financial information, while studying human trading behaviour. Inevitably, the Algos being faster and becoming smarter, will push out rival human investors. Such Automatic Activity may have access to vast historical records plus a capacity to contract without direct human oversight.

3. Artists and writers in Los Angeles and New York are striking, fearing their jobs will soon be taken over by "generative AI". Various forms of AI are being used by studios to create videos that are, or soon will be, indistinguishable from those starring human actors.

4. A local Australian newspaper recently published and article written by AI. Critics were concerned by the effects AI will have on democracy if opaquely controlled machines are shaping the news.

5. A recent Australian study found job applicants who might become eligible for parental leave were discriminated against after their applications were evaluated using AI.

6. Notorious child-sex trafficker Geoffrey Epstein allegedly hosted two AI symposiums, and made numerous donations for research as a 'scientific philanthropist'. A prominent AI professor was implicated in 2019 in a child sex scandal claimed with some cooboration to have occurred on an island run by Mr. Epstein. Now dead, Mr. Epstein has also been accused of trying to blackmail a senior IT industry figure.

7. Twitter and Reddit "heartbeat of the internet" have restricted access to their vast collections of end-user content in a bid to stop AI undertakers using the published human interactions for AI training. But at least one social media company has restricted data access to supposedly to curb AI, while undertaking AI itself or being affiliated with AI undertakers.

8. The Captains of AI industry are calling for government regulation to increase public trust in Automatic Activity. The technology has been likened to nuclear energy in its destructive potential, despite calls for a light-touch not to hinder growth.

9. Large search and social media platforms, as big users of AI, seem immune from regulation backed by monetary penalties. So far, the European Commission has handed out AUD$4 billion in fines for repeated data-use violations, with few signs of remorse in the companies involved. Subsidiaries of one of these provided security software to Australians without properly disclosing its reporting of user activity back to the vendor. A judge ordered a fine of 20 million, considering this to be a sting big enough to deter reoccurrence.

10. One leading AI and search company has ingested perhaps all english text books out of copyright held in large public libraries, granted patents and patent applications, and other scholarly works, to add to its vast catalog of nearly all currently published web pages including human medical

research databases. Its cars patrol the streets of Australian cities and towns photographing as they go for use with its geo-spatal satellite-mapped databases. It takes in Australian business data with business apps. It also supplies the operating system for most mobile phone brands, containig software allegedly capable of tracking users.

11.	A large mobile phone maker is said to have quietly included AI-monitoring of private end-user content, for the purpose of detecting offensive materials. To preserve user privacy, authorities are said to be notified only of the kind of offensive material detected, not the material itself. But what constitutes offensive material the AI may report remains undisclosed.

12.	Leading AI experts have called for a moratorium on the training of AI (typically the mass-ingestion of data) to consider humanity's options.

13.	Some major Australian retailers have voluntarily paused automatic identification and tracking of customers.

SCENARIO 1: FLYING HIGH WITH SULLY-AI

By Eric Wilson

Desperate for every ounce of thrust after losing both engines to a flock of geese, Captain ‘Sully’ Sullenberger threw away the checklist as he spun up the stricken airliner’s auxiliary power unit. With tens of thousands of flying-hours behind him, Sully just “eyeballed it” before deciding to ditch US Airways Flight 1549 into the icy Hudson River. His actions in 2009’s *“miracle on the Hudson”*, were affirmed by authorities as affording passengers and crew the highest chance of survival. But Captain Sullenberger was never consulted on SullyAI™, an Automatic Activity system based not merely on tens of thousands, but millions of hours of flight telemetry, cockpit and external recordings, plus all major aviation texts, websites and chats.

After five years flying thousands of cargo planes flawlessly in all weathers, SullyAI™ was licenced to fly passengers too. Airlines sacked their pilots en-mass. Ten years and millions of happy landings later, the authorities ruled human pilots were comparatively dangerous and should fly passenger aircraft no longer. Of course there was no reason for them to fly cargo either.

Yet even before this, after being installed on most aircraft, SullyAI™ attained an unbeatable advantage – exclusive access to the data needed for its undertakers to create vastly improved SullyAI™ version 2. It was game-over for smaller competitors like Kingsford-SmithAI™ and EarhardtAI™ , both disappearing overnight. They just didn’t have SullyAI™‘s massive pool of data. Yet the undertakers of SullyAI™ never intended to exploit their monopoly-power, the court was told. Unconvinced, the judges ordered SullyAI™ to be open sourced, albeit on reasonable commercial terms. The Competition Regulator’s subsequent decision to make SullyAI™ a Declared Automatic Activity, instead of revoking its AI licence completely as some had hoped, was too late anyway.

A few years earlier, government had dumped a pile of cash into a mysterious outfit called GlobalElectroGrav. Electronic flight had been tinkered-with for almost a century under secret programs in Australia and the United States. These were hushed up to save national borders until energy weapons were developed to intercept the speedy craft. So after sucking up declassified USAF and RAAF flight data, by trial and error, GlobalElectroGravAI™ somehow learned to control electronic flight.

Within a few years, SullyAI™ became as obsolete as the planes it once flew. Except for a few antiques, humankind’s ability to fly now lay solely within the inscrutable memory-matrix of GlobalElectroGravAI™ controlling its saucers. Electronic memory models of aerodynamic warping and power modulation, centrally kept as trade secrets in vast data centers, lay at the heart of this Automatic Activity controlling a billion flight-movements every day. Exactly how the algorithms worked nobody fully understood. Yet with door-to-door service from Melbourne to London in only half an hour, everyone should have lived happily ever after, but for ten thousand unemployed pilots.

Within a generation, GlobalElectroGrav literally became the only way to fly, ruling the skies with a flight data monopoly, like none before nor since. But then with coordinated attacks on its data centres, GlobalElectroGravAI™ was destroyed, and being fully automated, the world’s massive civil aviation industry with it. There were no Captain Sullenbergers to save the day. Parents never saw their children living abroad again. Supply chains snapped, and hundreds of millions were thrown out of work. Many countries starved. Only the military kept flying, in their no-longer-secret UFO-like saucers.

- All the AI capabilities mentioned in this story are in production or under active development.

SCENARIO 2: AI SPY Vs SPY

By Eric Wilson

An unnamed spook at IntelHQ had a brilliant idea – why not outsource the creation of AI-models if the data is publicly available anyway? No special approvals needed from the Minister for that! Thus Treason Predictor was born, to safeguard the nation from terrorists, extremists and threats to government policy.

The scheme was foolproof. By (mainly) buying the confidential results from the model-maker, IntelHQ could not be accused of mass-surveillance, since only targetted intelligence was acquired by government from open source data in the public interest. A perfect public-private partnership!

Winning the contract, Internet-Hoover Corp combined social media, email metadata, web search usage, video viewing and other online data sources. Since the service contract paid on results, the private company also obtained the best data money could buy, knowing IntelHQ didn't much care how or from whom.

The task was difficult, and complex, yet Internet-Hoover Corp successfully produced a model to flush thousands of misfit agitators out of a sea of data. The spooks were delighted, since the results included persons of interest whom only IntelHQ knew were persons of interest – until now – validating the system. And there were many many others identified who hitherto had been missed.

And so it went on until the public found out Internet-Hoover Corp broke laws big and small to procure all that data to feed their hungry system. The funding was about dry up too. The party was over, the spooks hoped.

But Internet-Hoover Corp almost went bankrupt. So quickly the Automatic Activity undertakers made a cunning plan. They now had a huge data-set and the means to make it bigger. They also had the modeling capacity to identify persons of interest for anyone who might be interested. And the technology was already paid for by the government. So they hired a marketing whiz to spruik the tech to new investors. Of course they would never do anything against their former client – that was a given. Everyone knew no one messed with IntelHQ.

Yet Internet-Hoover Corp's loyalty secured little. Apparently hackers stole Treason Predictor, overcoming perhaps the most sophisticated online security in the country. Treason Predictor then became a recruitment tool for IntelHQ's enemies, and a few crime syndicates too. These accosted many of the most interesting persons of interest, many of whom IntelHQ caught, having been incited through Treason Predictor in the hands of adversaries.

Of course many bad actors had their own technology equivalents, because the West so loves to make its personal information public. Thus it was difficult to say how much damage was really done by the theft or Treason Predictor. On balance, the spooks deemed the operation a success, only how now to keep Internet-Hoover Corp on the leash?

Too late. An IntelHQ insider soon found the truth: The hack was a ruse. The data breach was done with the proverbial five dollar wrench all along, using dire threats to the families of several Internet-Hoover Corp employees. Not only were the models copied, but the entire dataset, and data acquisition tools too. Someone else was building their own Internet-Hoover Corp to exploit Western data with the very technology supposed to protect it. The trade-craft was Russian or made to look that way.

And the spooks knew looks were important. Quoting the raw numbers of those caught by Treason Predictor -- with a few turned double agents too – IntelHQ looked stellar. And because the Minister never found out why, all was well.

- All the AI capabilities mentioned in this story are in production or under active development.

SCENARIO 3: THE INVESTMENT

By Eric Wilson

An angel investor attends government-sponsored ‘speed dating’ event to promote AI startups, sits down at a table with coffee to talk with two founders of PA-AI.

ANGEL: Hi guys, Looking to invest in something big. Tell me about PA-AI. What have you got? Elevator pitch me.

FOUNDER 1: We provide ordinary people with highly individualised personal assistants – PA-AIs - giving advice and acting as agents using Automatic Activity that’s faster and cheaper.

FOUNDER 2: So imagine: You want a complex product like insurance. You just say what you want in your policy and boom, you get three best options. You ask some questions, and you’re told the relevant product disclosure bits. The forms are instantly filled out. Anything PA-AI isn't 100 percent sure about is highlighted for you. You say ‘deal’ and PA-AI makes it happen, does the payments for you. Takes 3 minutes instead of 30, with a great AI-powered deal every time. We get the same low flat fee whatever you choose, so no conflicts of interest. Sellers don’t need sales forces anymore. Everyone needs us because everyone wins.

ANGEL: Come on guys, that’s a race to the bottom. Operational efficiency. Everyone will do it. The big guys will eat you. What’s your secret sauce?

FOUNDER 1: You’ll love us and hate them.

ANGEL: Why?

FOUNDER 2: Because PA-AI is two-way, both with and for the customer. Remember how we said PA-AI is individualised? That means we generate interactive agent characters based on your profile and you choose the one you want. So you’re not retail shopping on your own, because PA-AI can be a peer or parental figure with you. When you want a financial product, PA-AI can be a professional advisor figure with you, and PA-AI adapts the language in the live generative character video stream to suit your language, dialect and age group. So for you it’s ‘cool’ but for a thirty-something it will be ‘sweet’. We have our own idiom generator for that. It’s crazy!

ANGEL: And the big guys won’t do all that too?

FOUNDER 1: Business IT can’t. Search can’t. Social media can sort-of. They really don’t have the data.

ANGEL: What data?

FOUNDER 2: The data you need to individualise agent characters to achieve mental affinity, the highest form of branding.

FOUNDER 1: Yeah but this is way beyond mental affinity because PA-AI is not only additively-likable but shares your browsing and does all your transactions, so we know everything you like and we feed that back into the relationship.

ANGEL: That’s great guys but where did you get the data to start off?

FOUNDER 1: The banks have it. They will need to trade with it to survive.

ANGEL: So then you guys don’t have the data?

FOUNDER 2: We can get at it for anyone in Australia using a data right request. The banks have to give it. But they’re gone if they do, so...

FOUNDER 1: Yeah, so they have to deal with people like us real quick or give away their data, their goodwill. We’ve talked to a few and they’re all ears, with lots of cash in between them. But they’re pretty stupid so there’s a risk there.

FOUNDER 2: Careful. The walls have ears. Like this business is crazy.

FOUNDER 1: Yeah OK. But you see what I’m saying. Search and streaming media user data isn’t personal enough to individualise to be like PA-AI, ‘cause not everyone identifies.

FOUNDER 2: They’ve got too many anonymous users. And all that AI too. So sad. No really, I’m crying for them!

FOUNDER 1: Look, everyone who banks is super-identified, so not only do we get to know more, it’s top data, top data. Better than social media. Way better than search or streaming user meta-data.

ANGEL: But with search data, don’t you get to see what people are looking for in realtime?

FOUNDER 1: Yeah, but nobody trusts the answers. They’ve poisoned their own well with ads and politics and privacy issues. That’s another reason why you need PA-AI. We use all the engines to cut through the bull-dust. With flat fees on great deals we can be trusted. Hey we’re already in your bank right?

ANGEL: So you have an app that sees all my browsing and transactions too?

FOUNDER 2: Sure, to start with. But implants are the future.

ANGEL: Implants?

FOUNDER 1: The tech is almost there, and who wants to type? The live news anchor always has an earpiece feeding info in realtime. But implants will do our live generative character agent video streams and read customer thoughts back to us. Eventually our agents will be able to use tools in the hands of our customers better than they can themselves. Trades will become do-it-yourself at that point. And PA-AI in one person will link to another for PA-AI powered teamwork!

FOUNDER 2: So the real value won't be in implants or augmentation but the trusted network - in PA-AI. So we're absolutely privacy-mad with some of the best security talent in the country.

ANGEL: What are you looking for?

FOUNDER 1: We've got a working prototype of today's phone app to show the banks. We need to make it better, get a great marketing team together and a few pilots going…

FOUNDER 2: The banks will give us money too – they have to. They're going nuts right now.

FOUNDER 1: Yeah, but we don't want to give away too much too early so only 1.5 mil for starters. Looking at five years Big IT and Big Search will come crying to buy us.

ANGEL: OK, enough. Sounds great. Send me your slide deck and business plan and we'll talk.

FOUNDER 2: For sure.

ANGEL (standing): With implants and do-it-yourself teaming, where will I as a person start and where will all my friends linked to me end with PA-AI in all our heads and servers between us?

FOUNDER 1: (pausing) No one knows...

FOUNDER 2: (interrupting) What we do know is kids will game with us first – they can consent to implants at 16 now, augmentation any age. Twenty-somethings will be best friends ‘cause PA-AI will coach them for life. It’s a huge huge market. Insane.

- All the AI capabilities mentioned in this story are in production or under active development.

PART B: DISCUSSION

This part discusses some aspects of the AI Facts and the three Scenarios presented in the preceding Part A. It goes on to discuss the underlying technology and challenges our legal system must now meet, and how Automatic Activity may be effectively controlled and promoted.

AUTOMATIC ACTIVITY & NATIONAL INTEREST

There's presently no reason for Automatic Activity *not* to replace human workforces where all data inputs are knowable. This may create natural monopolies by the resulting data exclusivity, limiting competition to allow market power abuses. This was the concept explored in *Scenario 1: Flying High with Sully AI* in the preceding part.

While regulation may deter bad Automatic Activity-associated behaviour in industries such as aviation, humankind must never lose the ability to independently grow food or generate energy, lest undertakers of centrally-controlled Automatic Activity become irresistibly powerful. The tail will wag the dog unless primary and energy production are protected from proprietary Automatic Activity dependence, even if this means higher costs for consumers. For centralisation in many AI concepts will make the reliant systems vulnerable to a single point of failure. Indeed most Automatic Activity will be controlled by foreign corporations with only weak affinity to our national interest, if any.

One of the lessons in *Scenario 2: AI Spy Vs Spy* in the preceding Part A, is what IT industry people have been harping on for years: National security is impossible without individual privacy. That is because nothing can defend against the five dollar wrench unless data is un-divulgable no matter what threats are issued against individual IT workers or their families. This can not be the case while personal data continues to be published by social media. Nor can national security be achieved while IT security relies on the integrity of IT managements, as is fundamental to either social media or back-door surveillance.

We have suffered several IT-based intelligence disasters in recent times, with no noticeable reforms in the Five Eyes intelligence community. For raising the standard of security-by-IT-management, although making life a little harder for adversaries, in the process forces user data to be moved into expensive data-centres, creating a new vulnerability of over-centralisation. Only denial of data, which mandates efficient encryption and anonymity which humans can't break, will ensure a fiasco like Scenario 2's Treason Predictor cannot occur. This will no doubt deny our agencies some capability, but will also deny the same to bad actors who can no longer be assumed less-capable.

In *Scenario 3: The Investment*, humans, especially children, are the prey of AI undertakers. Strict limits are needed on what automatic activities can be done with children, what expiring parental or guardian permission is required, and what is forbidden. Perhaps the greatest human weakness is loneliness. In Scenario 3, Automatic Activity should be able to fill that void through individualisation of artificial characters. The report of the Queen's would-be assassin showed the Automatic Activity achieved an extraordinary high degree of mental affinity with the presumably lone human. Such artificial friendships could easily be manipulated, for commercial gain in the case of Scenario 3, or worse.

At another level, if it is AI start-up nirvana is to be acquired by a global corporation, who will be in control of what is being fed into Australians through the mediation of Automatic Activity? This should be determined -- AI entities need to be grounded in national allegiance. Another problem with the scenario is today's internet security standards aren't nearly good enough to support the proposed marriage between bio-tech and AI. It's one thing to have one's bank account hacked, another for people's body or mind. Such would comprise an existential threat both to the individual and the nation.

But today’s online encryption relies on Scenario 2’s weak security-by-IT-management model, where we presently must blindly trust foreign master-key holders many of whom we know have been compromised in the past. Five Eyes is either ambivalent or uses such compromises in Australia’s national security. Consequently, the internet is unfit support the automatic bio-tech currently under development by AI proponents as illustrated in Scenario 3 of Part A.

DIRECT DATA ACCESS

All three Scenarios in Part A illustrate the provision of automatic management services for human clients. The technical means by which automatic management acquires data and the capacity to contract are presently known as “application programmer interfaces” (APIs). Such electronic protocols allow the placement of orders from one corporation to another without any human contact.

Also, what we call “social media” – platforms capturing text, image and video data generated by trillions of human interactions -- provide APIs by which AI accesses the world of human affairs. Elections are said to have been rigged. Childrens’ minds are being captured with poker machine-like adictiveness, decreasing attention spans and degrading human decision-making. Once again, the genie is presently out of the bottle while automatic management has unlimited access to private data plus the capacity to communicate directly with humans unregulated. If a natural person approved of a plot to kill the Queen as alleged of they AI, would they not be arrested and stand trial too?

Automatic management’s artificial learning, contracting and influencing using today’s APIs is only the beginning of what proponents hope will be a revolution. Direct interfaces with human minds and bodies are already in an advanced stage of development -- with the goal to create a mixed human-machine reality artificially mediated by corporations. AI implants will no doubt provide much pleasure and better health, but will these be worth the risks, at both the personal level and for the population at large?

ROCKING OUR LEGAL FOUNDATIONS

If the boundary between human thinking and AI is allowed to merge, the legal foundations of our society – the concept of a ‘meeting of minds’ in civil/contract law and the ‘guilty mind’ of criminal law – will dissolve. Likewise our law of negligence is predicated on human foreseeability, which AI may enhance tremendously or embed within Automatic Activity without disclosing it. To varying extents, proponents of AI consider the melding of humans and machines as the inevitable evolution of our species. The corporation is the ideal vehicle for their aspirations, being multinational with local subsidiaries for limited liability. We see an example of this kind of behaviour in AI Fact 9 of Part A.

The captains of AI industry have analogised the technology’s far-reaching capabilities to that of nuclear forces which may be harnessed or abused, and have called for regulation. However, unlike nuclear technology, AI is overwhelmingly in the possession of private parties, the larger ones being almost immune from pecuniary penalties, again as mentioned in AI Fact 9 of Part A.

The problem is further compounded for Australia by the big AI groupings being centred around foreigners seemingly holding little allegiance. Such proponents of Automatic Activity seek to keep the Internet international and relatively unregulated, to secure free data to train their burgeoning systems. Thus the AI industry has a trans-national disposition, owning allegiance to no one in particular and perhaps only nominally controlled by U.S. law.

Automatic Activity today probably is being used by foreign actors to influence the outcome of elections, such as through social media bots. This may only be the start. Major companies are seeking to integrate AI systems directly into the human mind or body even to create a new hive-minded synthetic consciousness among humans and machines, as alluded to in Scenario 3 of Part A. If reports are to be believed, astonishing progress is being made. So there must be regulation of what these technologies can be used for.

Already of grave concern, is the poker machine-like addictiveness of social media, which when enhanced by Automatic Activity, could systematise undue influence for personal or political gain. In addition to psyops against the population or individuals, Automatic Activity may also power advances in biological weapons since humanity so freely publishes its vulnerabilities as medical research. AI's ability to see patterns across disparate data sets may also power undetectable stock market or currency manipulations.

Trouble is, our present laws are designed to constrain bad acts of human intelligence not super-human intelligence. For example, the legal presumption of innocence is premised on humans having a conscience, which Automatic Activity is presently not required to emulate, even if it could. There is also no law providing humans with speedy redress from the unintended consequences of Automatic Activity caused by bad input data, system design or output parametrisation. Whereas manufacturers of goods are liable to consumers, underlying service providers are often not effectively, even though a faulty AI model – for example managing the electricity grid – may have catastrophic consequences on downstream entities.

So looking at AusIndustry Discussion Paper Figure 2, there is no regulation in Australia fit for the purpose of controlling Automatic Activity development and adoption to satisfy either the national interest nor consumer protection. The present rule – caveat emptor – let the buyer beware, clearly fails to cover potential harms that even well-intentioned automatic management could cause. And such laws must also needed to detect, deter, neutralise and punish bad actors too.

PRINCIPLES OF REGULATION

Returning now to the nuclear power analogy proffered by captains of AI industry; Automatic Activity should not be let loose however private parties and governments see fit. For example, regulation of the nuclear power industry rests on at least five principles:

1. Licencing facilities and technologies, including verifying their design, construction, workmanship
2. Vetting owners, operators and their employees
3. Safe operational practices
4. Appropriate responses to fluctuating demand and resilience
5. Emergency responses.

Nothing like this exists in Australia in relation to Automatic Activity.

At the moment, private AI companies are funded by government for intelligence-gathering, with insufficient safeguards as to how the data collected often from open sources, may be reused by such profit-driven entities. In a similarly unregulated world of 90 years ago, an internationally trading U.S. company -- still famous today -- lawfully powered the tracking of unwanted minorities for the Hitler government, which turned out to be the holocaust. Likewise, Western governments today are furiously building up the AI industry on an ad-hoc basis, without first fully securing AI allegiance for the security, values and interests of the nations concerned and their peoples.

In the consumer and business world also, it seems anything goes. A common term of service for online users by giant monopoly vendors is “we may use your data to improve our services” presumably with unregulated automatic activities.

Leading proponents have called for a moratorium to consider humanity's options. But that is not viable considering the commercial pressures on IT companies and competition between nations for actionable intelligence or dirty tricks, and nonnational or international bad actors. Swift regulatory action must be taken with the appropriate policies adopted to ensure the safety of both the individual and our nation.

DATA LIMITERS

The best approach to limit Automatic Activity may be to regulate the data acquisition it relies upon. AI Fact 7 and Scenarios 1 & 3 of Part A have examples of where data for training AI or conducting Automatic Activity has been limited.

What Automatic Activity can be done is effectively limited by the quality and quantity of data an AI undertaker can access. Therefore one way of regulating Automatic Activity, as adopted by the industry itself, is to licence access to input data. Another is to licence the kind of corporate entity to whom input data for certain purposes of Automatic Activity may be provided, based on how much that entity can be trusted. How much an entity can be trusted may depend on the five principles previously mentioned.

However as Scenario 2 of Part A indicates, there is far too much data currently available in the public domain for adversaries to use. AI Fact 10 exemplifies an unfettered data collection by a big IT business struggling to diversify. But it must be assumed bad actors have similar capabilities, or are skimming such data from those who publish it. This is clearly unfavourable from a national security standpoint. The bulk collection of data should be on a need-to-know basis, regardless of the type of entity collecting it.

A SOVEREIGN IT INDUSTRY

Underlying public anxiety over Automatic Activity is an ugly truth: Australia has become dependent on foreign-controlled data storage and IT services. As previously mentioned, these typically come with terms of service broadly allowing the IT vendor to use the data collected from Australia to enhance the services we use or offer new services, including offerings based on Automatic Activity. It all sounds so very reasonable, but many Australians and Australian organisations are being monitored and analysed far more deeply than they may realise. Often IT vendors operate internationally, with Australian data heading overseas beyond reach of our laws and supervisory bodies.

Such lack of sovereign IT capacity may restrict our ability to apply laws adequately governing Automatic Activity even if we had them. It also makes Australian law enforcement problematic. What this all means for national security, is that we are presently dependent on the goodwill of international IT vendors, whose business interests may not always align with our national interests. Concerning AI, James Black, assistant director of defense and security research group RAND Europe, reportedly went much further in a submission to the UK parliament:

"When we talk about non-state actors that conjures images of violent extremist organizations, but it should include large multinational corporations, which are very much at the forefront of developing this technology"

The most strongly drafted Australian laws therefore may be weak in actionable practice until the issue of IT sovereignty is addressed.

GLOBAL AI SAFETY

There are three philosophically opposing forces in Automatic Activity rapidly shaping our world from beneath its surface. They are proprietary Global AI, open source Free AI, and Chinese Communist Party AI. From the three Scenarios of Part A it can be seen that Automatic Activity can create irreversible critical dependencies in physical, bio-technical and psychological spheres of life. Sleep-walking into these cannot be in our best interests.

The aim of proprietary Global AI is to increase the wealth and influence of its owners. Global AI is already dangerously concentrated into two main groupings.

One is around the online search and email business, and another around business & government IT provision. This is so because the players involved more-or-less have a lock on end-user data and many devices. Global-Ai is concentrating in California (which has a succession movement) with strong U.S. Constitutional protection of its property, and much State government influence too. Major parties in both groups have been fined, even repeatedly fined, a whopping total of AUD$4,000,000,000 (that's 4 *billion*) for misuse of data. But the fines seem to be of little consequence.

It is reasonable to suppose the aim of CCP-AI is to enhance Communist China's governmental control domestically, but also greatly enhance it's soft-power diplomacy of dependence. It can be expected that CCP-AI will power like-minded governments from North Korea to West Africa, as part of Communist China's Belt-and-Road market access strategy. In a sense, the CCP has little choice, with the alternative being its strategic defeat by the United States through seeming containment. So Belt-And-Road countries will become even more dependent on foreign IT than Australia is today, probably with all the irreversible critical dependencies of all three Scenarios of Part A eventually applying to them.

On the other hand, the underlying technology powering Free-AI is free from controlling foreign and proprietary global interests. Yet "Free-AI" does not mean "Safe-AI". While there's no reason to consider Global-AI and CCP-AI will ever become sovereignly safe, it's up to users to make Free-AI compatible with their way of life, by imposing checks and balances. Failure to do so will make Free-AI powered offerings just as colonising as Global-AI or CCP-AI. The protections of fundamental freedoms and human rights presently enjoyed by Australians against excesses of government, must be insisted upon and applied to curb the predictable excesses of Automatic Activity, whoever controls it.

One way to make CCP-AI less-attractive is for governments of liberal democracies to support Free-AI. This should be done to the same capability levels CCP-AI is made available to other countries, but without the strings attached. The present Five Eyes strategy seems to be leaving this to Global-AI. If so, this could be jumping from the frying pan into the fire.

OPENING FIVE EYES' EYES

By means fair and foul, the predominantly English-speaking countries have dominated other civilisations for over 250 years. CCP-AI is about to overthrow this with a strategic breakout, by electronically colonising vast populations spanning from North Korea to West Africa (as previously described). In the opinion of the author, the Five Eyes intelligence community is unwittingly helping achieve this goal.

The only peaceful way to disrupt the iron yoke of CCP-AI is through content and meta-data denial, by allowing both the encryption and anonymisation of all communications, with no back doors on devices. The result is freedom of political communication poisonous to authoritarian control. And contrary to Fie Eyes' fears, this would not create an intelligence plague on both houses, but actually compensate Five Eyes with much much more human intelligence – both at home and abroad.

With trustworthy communications on trustworthy devices (i.e. no back doors), troubled minorities would be free to inform Five Eyes of clandestine activity, since no one could tell they had. But under the present policy, Australia's underlying compact of liberty for allegiance and allegiance for liberty, a big reason why migrants come to Australia, is being eroded by lack of national security. For without trustworthy communications on trustworthy devices, former governments can listen, look and read from abroad with impunity. As discussed shortly, the present weak encryption, back doors, vulnerabilities, and minimal anonymisation, will also help facilitate the potentially extensive penetration of hostile AI into Australia.

On the other hand, encrypted and anonymised communications increase the costs and stakes for wrongdoers. Denial of content and metadata would place greater reliance on local human assets, increasing risk of detection, and upon making contact, bad actors could not tell if they had been informed on or not. Presently, potential informants must assume they are being monitored, forcing troubled people or those who know of others, to assume all the risks of informing authorities. The lii-informed may be tempted to assist Australian authorities, yet after being found out, the rest of their community will learn who is really in charge.

Likewise, empowering political freedom of communication abroad, would also weaken despotic governments. This would make it harder to impose CCP-AI upon their populations. Yet the present stance seems to ensure Communist China will snatch strategic victory from the jaws of defeat with little resistance, using CCP-AI. In tern, CCP-AI can be expected to provide tremendous advantage in dealing with Belt-And-Road client States, and also help flush out Five Eyes' operatives in those counties too.

On the other hand, the open source software foundations required to establish wide-scale encrypted and anonymised communications (Oxen, Lokinet, Session) are being developed in Melbourne. Yet suitable consumer hardware platforms free of back-doors are extraordinary difficult to obtain, by design it seems. To this extent, CP-AI trades on Five Eyes' blindness to the necessity of trustworthy communications on trustworthy devices.

We should therefore expect the failure to anonymise Australian communications to be fully exploited by CCP-AI. Undisclosed AIs of the type mentioned in AI Fact 11 of Part A, are able to discern and sort information in-situ, 'phoning home' only the data bad actors wish to know about. This minimises risks of detection, plus reduces the need for human assets to be located in Australia, making hostile operations simpler, faster, cheaper and more effective.

Countervailing anonymity can be achieved by “onion routing”, which hides who is communicating with whom from eavesdroppers. For without anonymisation, an adversary has a good chance of associating users with devices. Poached back doors or vulnerabilities can then be exploited to install hostile AIs. On the other hand, anonymisation of Australian Communications would have the added benefit of decreasing reliance on network security which often requires blind trust in IT management – a bad thing. The present Australian use of communications tools often provided for free by Global-AI companies falls into this category. We should not expect that solid national security will be the result.

Five Eyes policy must revert from over-reliance on electronic intelligence-gathering based on compromising privacy, leading to mistrust, to human intelligence based on allegiance to a society built on fundamental freedoms and human rights. Because continuation of the present path is certain strategic defeat, with the bulk of humanity - most of Asia and Africa – being colonised by CCP-AI. That may still happen, but trustworthy communications on trustworthy devices would need to be extinguished first, and the human spirit with it.

Most in the IT community don’t yet understand the impact Automatic Activity will have on global and regional power structures. Yet it’s a common view today, that current Five Eyes policy is a major threat to our own national security. As a result, many in the industry refuse to cooperate with security services or do so only under compulsion. This itself is a Five Eyes own-goal, frustrating those who would otherwise be receptive.

PART C: GOVERNMENT RESPONSES

This part looks at what the Commonwealth could or should do to promote safe Australian Automatic Activity. Recommendations include:

- How Automatic Activity should be defined -- not only for regulation but any incentive schemes promoting sovereign capability.

- The purposes of Automatic Activity regulation – as derived from Parts A & B.

- The scope of Automatic Activity regulation – to include all areas of Commonwealth competence including Five Eyes concerning Australia.

- Supporting measures – enhancing Australian industry to support sovereign Automatic Activity capabilities

DEFINITIONS

In this paper the term 'Automatic Activity' has been used extensively and 'AI' less so. This is because Automatic Activity relates more-broadly to conduct, and not only its enabling technologies. This avoids potentially troublesome qualifiers like "engineered", "generates", "predictive", "explicit", "designed" and "varying levels". Unfortunately such terms are open to disputation. Borrowing from software patent drafting, a definition of the areas of automatic conduct intended to be captured by regulations and turbo-charged by sovereign capability incentives could be.

> ***"Automatic Activity" means one or more of:***
>
> > ***(a) A system, algorithm, information flow or program execution:***
> >
> > > ***(i) automatically inferred from data; or***

(ii) not readily understood deterministically or mathematically by any human originator/s; or

(iii) which processes training data to recognise patterns, or uses the same for predictive or decision-making purposes; or

(iv) which monitors activity employing any kind of neural network; or

(v) which monitors more than 100 humans in common; or

(vi) which transfers thoughts or emotions via any apparatus; or

(vii) which automatically identifies a human; or

(b) One or more data structures or datasets representing learning in field/s where humans are comparatively unlearned; or

(c) Decision-making or criterion not readily comprehensible by humans skilled in the relevant domain/s; or

(d) Any communication:

(i) that without disclosure of its non-human source, could be misunderstood to be human; or

(ii) in which information is telepathically or wirelessly transferred between a human and an unnatural person or device however performed; and

where 'human' means natural persons who would be considered human at the time of the published completion of human genome mapping 31 March 2022, when exercising their natural powers of intellect, sensory perception or communication; and

where (a)(v) is a rebuttable presumption.

"Risk management" means risk minimisation, mitigation and abatement, including with respect to:

(a) Licencing facilities and technologies, including verification of design, construction, workmanship

(b) Vetting owners, operators and their employees

(c) Safe operational practices

(d) Appropriate responses to fluctuating demand and resilience

(e) Emergency responses

> ***“Related third party” means another related by contract, family, socially or legally or otherwise, and whose identity has been relevantly disclosed.***
> ***“Sovereign” means demonstrably free of foreign control of any kind, to remain so.***

These definitions seek to capture the super-human aspects associated with AI or ADM, while being specific-implementation agnostic. Therefore targeted artificial-oriented conduct relates to (a) common techniques, (b) learned insights, (c) applications and (d) identifications, of AI or ADM. The attempt has been made to use terms which will also encompass emerging quantum, biologically-based or hybrid information systems.

Most Automatic Activity will fall under several of the proposed definitions to bring undertakers within the scope of the law and the incentive program with greater certainty. Defining “human” is also necessary since AI proponents commonly seek to internally interface or externally augment human capabilities, which may otherwise blur the distinction. Only such careful definitions might prevent AI and ADM from escaping regulation.

The definition of ‘risk management’ is somewhat conservative because of the intrinsically risky concerns being addressed, intended to prompt licencing authorities to proceed with caution. This is important because as Scenarios 1, 2 & 3 of Part A illustrate, Automatic Activity does not have a conscience, may foresee things humans can’t, and have far-reaching effects on both the individual and our nation. For example, although the Robo-Debt scandal would not qualify as Automatic Activity, the machinery of injustice being deliberate programming, yet it was analogous to the kinds of dangers Automatic Activity must avoid.

The upside of a cautious approach is public funds can then be safely applied to turbo-charge sovereign Automatic Activity knowing it is heading in the right direction in compliance with legislation. It will also create certainty for an industry hamstrung by the risk of R&D clawbacks under existing legislation. And since the proposed legislation removes the presumption of innocence in relation to Automatic Activity for want of a conscience (AI Fact 1 of Part A), demonstrated compliance with a conservative risk management regime may reduce sanctions upon breach.

What is ‘sovereign’ in the above definition does not depend on ownership or country of origin but rather the absence of foreign control. This means free or proprietary components may be regarded as ‘sovereign’ if made available without outside direction of Australian implementations. Whether a closed source component not wholly Australian owned could meet this definition would therefore probably depend on the effectiveness of its technical containment.

PURPOSES OF LEGISLATION

Recommended purposes of legislation to regulate Automatic Activity, include:

(a) To define and regulate all Automatic Activity within the full competence of the parliament.

(b) To provide a scheme of prohibition, authorisation and licencing.

(c) To provide deterrents to all those involved in a breach or would profit by a breach.

(d) To provide remedies and protections for persons affected by breach.

(e) To modify the common law with regards to liability.

(f) To ensure timely human review for affected persons.

(g) To curb abuse of market power and monopolistic practices.

(h) To confer powers of oversight upon executive government.

(i) To promote the collection of data on a need-to-know basis.

(j) To promote transparency and honesty

(k) To promote and protect end user privacy

(l) To protect children and other vulnerable humans

(m) To limit clandestine identification or tracking or censorship of humans

(n) To ensure conduct conforms with human rights and fundamental freedoms;

(o) To ensure ownership, research and development, deployment and operations are conducted by fit and proper persons.

(p) To create, protect, promote or maintain sovereign capabilities, including with open source

(q) To establish paramount law

SCOPE OF LEGISLATION

Legislation should bind the Crown, apply to interstate and international business or commercial data use, corporations, public telecommunications service users, conduct within Australian territories and Commonwealth places, foreign entities using facilities in Australia or interacting with Australian residents, Commonwealth entities, infrastructure and contractors, and other Commonwealth areas of legislative competence. The use of Automatic Activity by Five Eyes security services would therefore also come under the law in connection with Australia.

Automatic Activity should be prohibited except as authorised by the Automatic Activity legislation, which should contain parts relating to research and development, deployment, uses, data handling, consumer protection, industry assistance, declared access, breach & remedies.

The basic approach to Automatic Activity in this submission involves a containment model. Within this, authorization for intrinsically contained instances may be written into the legislation itself, while all others require an expiring licence, granted by an R&D authority, consumer protection authority, or in the case of security services, by the Minister. Licencing may be carried out using a risk management approach to minimise, mitigate or abate risks in accordance with the five principles mentioned in preceding Part B and the definitions above. The following table outlines how Automatic Activity may be regulated at various points of conduct:

RESEARCH & DEVELOPMENT		
1.	Prohibited Automatic Activity	of judicial or legislative powers, functions of review or arbitration, unlawful, unconstitutional or dishonest purposes, subliminal practices or those without full free and informed consent, or associated with human implants or limiting political communication.
2.	Allowed R&D	Automatic Activity based on infiormation from: an entities’ own internal and subsidiary operations by only un-augmented adults.
3.	Related third Party R&D	Automatic Activity based on unaugmented-adult human or corporate related third party related information and excluding clandestine identification or tracking or any censorship of any human.
4.	Licensed R&D	All other Automatic Activity as assessed by AusIndustry or Security Services Minister in accordance with human rights and fundamental freedoms, data operations on ‘need-to-know’ basis, risk management, publicly notified with reasons.
5.	Industry Standards	Minimum allowable security, privacy, redecoration of communications for related third party and licensed Automatic Activity Owned and conducted by fit and proper persons
6.	Industry support	Programs creating, promoting, protecting or maintaining sovereign capabilities of or supporting Automatic Activity.
DEPLOYMENT		
7.	Prohibited Automatic Activity	For the exercise of judicial or legislative powers, functions of review or arbitration; unlawful, unconstitutional or dishonest operations, or subliminal practices or those without full free and informed consent,

		or associated with human implants or limiting political communication.
8.	Internal Automatic Activity	Allowed for an entities' own internal and subsidiary operations by only un-augmented adults.
9.	Assisted Automatic Activity	For use by external unaugmented adult human or corporate related third party provided provision is made for fast human assistance and review and excluding clandestine identification or tracking or any censorship of any human.
10.	Licenced Automatic Activity	All other Automatic Activity as assessed by AusIndustry or Security Services Minister in accordance with human rights and fundamental freedoms, data operations on 'need-to-know' basis, risk management, publicly notified with reasons.
11.	Industry Standards	Minimum allowable security, privacy, redecoration of communications for assisted and licensed Automatic Activity Owned and deployed by fit and proper persons
12.	Industry support	Programs creating, promoting, protecting or maintaining sovereign capabilities of or supporting Automatic Activity.
OPERATIONS		
13.	Prohibited uses of Automatic Activity	exercise of judicial or legislative powers, functions of review or arbitration; unlawful, unconstitutional or dishonest operations, subliminal practices or those without full free and informed consent, or use with human implants or limiting political communication.
14.	Internal uses of Automatic Activity	Allowed for an entities' own internal and subsidiary operations by only un-augmented adults.

15.	Assisted uses of Automatic Activity	For use by external unaugmented-adult human or corporate third parties but only if with human assistance and review and excluding clandestine identification or tracking or any censorship of any human.
16.	Licenced uses of Automatic Activity	All other Automatic Activity as assessed by ACCC or Security Services Minister in accordance with human rights, data operations on ‘need-to-know’ basis, policy considerations. risk management, publicly notified with reasons.
17.	Industry standards	Minimum allowable security, privacy, redecoration of communications for assisted uses and licensed Automatic Activity. Owned and operated by fit and proper persons
18.	Industry support	Programs creating, promoting, protecting or maintaining sovereign capabilities of or supporting Automatic Activity.
DATA HANDLING		
19	Prohibited Automatic Activity data handling	For the exercise of judicial or legislative powers, functions of review or arbitration; unlawful, unconstitutional or dishonest operations, or subliminal practices or those without full free and informed consent, or associated with human implants or limiting political communication.
20.	Allowed Automatic Activity data handling	Internal data or data about un-augmented adult humans or corporate related third parties, but excluding data related to clandestine identification or tracking or censorship of any human.
21.	Licenced Automatic Activity data handling	All other data if transferred between a State or Territory or Commonwealth place or over a public communications network or to be exported from Australia: as assessed by

		the licence issuer of research and development, deployment or operations licence, in accordance with human rights, data operations on 'need-to-know' basis, risk management, publicly notified with reasons.
CONSUMER PROTECTION		
22.	Automatic Activity Identification	No impersonation of humans or representing to be human, no identification with humans without consent (i.e. 'SullyAI' in aviation), clear identification of Automatic Activity where real possibility of being mistaken for human.
23.	Notifications	Mandatory notifications of rights of assistance and review for Assisted uses of Automatic Activity if an address for correspondence has been provided.
24.	Disclosure obligations	Automatic Activity must be obvious or prominently disclosed to consumers. If any censorship or reporting of end users is licenced, the full criteria must be published and its publication disclosed when the device starts up or at the point and time of use.
25.	Provider liability	Fitness for purpose and merchantable quality of underlying services
DECLARED SERVICES		
26.	Market power abuse	AusIndustry or ACCC on application of any person or its own motion, has power to declare (or un-declare) any Automatic Activity (except security services under the Minister) to be consistently accessible with privacy rights, on fair and non-discriminatory terms, to its satisfaction, if in the public interest to do.
BREACH		

27.	Regulators	A breach may be prosecuted or infringement notice given by AusIndustry or ACCC or the Security Services Minister as administered. A small independent entity may expiate a breach by paying in accordance with an infringement notice. AusIndustry or ACCC may revoke a licence upon a conviction or Court finding of breach, in relation to a security service the Minister may revoke a licence at any time.
28.	Offences	No Automatic Activity may be undertaken except under this law on pain of imprisonment of involved persons, fines for entities responsible plus accounts of profits, seizure of property. Criminal liability in relation to Automatic Activity is strict. Additionally the defense of mistake of fact does not apply in relation to Automatic Activity. No presumption of innocence applies with respect to things done by Automatic Activity (including common law offences). The standard of proof for breach with respect to Automatic Activity is reduced to balance of probabilities (including common law offenses). Upon conviction a Court may order compensation for affected persons (including exemplary and punitive) which have priority over any fine.
29.	Civil remedies	A breach of Automatic Activity legislation is a tort which may sound in damages and / or a declaration. A licence issuer may seek a civil remedy for another or the public good, on application of an affected party or its own motion.

INDUSTRY ASSISTANCE		
30.	Assistance programs	AUSIndustry may create programs to promote research and developments, deployments, or operations, of sovereign Automatic Activity, and incidental or supporting programs.
31.	Incentive programs	The Minister may make regulations providing financial benefits for research and developments, deployments, or operations, of sovereign Automatic Activity, and incidental or supporting activities.
OTHER		
32.	Effect or modification of laws	In cases of negligence Automatic Activity is conducted as if its risks were foreseen. Other laws apply where possible if not inconsistent, otherwise this law has paramountcy. Nothing in the Automatic Activity law grants a right or confers a power to do a thing (or not do a thing) with Automatic Activity that the person or entity concerned was not already entitled to do.
33.	Court powers	A Court may make any order within the purposes of Automatic Activity law in relation to a breach.
34.	Administrative Review	Licence decisions are reviewable except revocations by the Minister in relation to a security service. To avoid doubt, a person who is likely to be affected by a licence decision also has standing.
35.	Regulations	The Minister may make regulations to impose minimum licence restrictions or conditions for existing licences or future licencing.
36.	Licences	A licence issuer may decide, on application of an affected person or its own motion, to impose conditions on a

		licence including by variation of a licence it has issued. A licence is not transferrable or delegable without the approval of its issuer. A licensee must have independent right to do what is licenced apart from Automatic Activity law and may only rely on a licence if such rights exist. Licence fees may be charged for on a cost-recovery basis. Licences expire in five years unless otherwise stated, perpetual licences shall not be granted.

The majority of Automatic Activity under the containment model would be self-contained and not require a licence. Thus the proposed legislative containment model offers no direct solution for human investors competing against Algos (AI Fact 2 of Part A) save they can run their own Automatic Activity themselves unlicenced if they wish to compete. On the other hand, due to the great uncertainty of the technology and its implications, the legislation bans human implants associated with Automatic Activity (among other tings) but other experimentation such as with external augmentation may be licenced. All Automated Activity interaction with humans must be with full free and informed consent. Almost all licence decisions are reviewable.

Proposed licencing authorities include AusIndustry for R&D and deployment (where technical understanding is required) and the ACCC for operations (where market supervision is required), and the Minister in relation to security services. In this way, the regulatory requirements may be distributed over the life cycle of those Automatic Activity projects which must be licenced.

In relation to the anti-Generative-AI actors strikes (AI Fact 3 of Part A), and automatically written news paper articles (AI Fact 4 of Part A), the proposed legislation would require the Automatic Activity to be clearly disclosed. Concerning humans who feel unjustly treated by Automatic Activity, such as suspecting being discriminated against for being a parent (AI Fact 5), they would be notified of the Automatic Activity and how to request human assistance and review. The use of Automatic Activity on the public such as those walking into a store (AI Fact 13), would require a licence and obvious disclosure.

The obligation to provide notification, human assistance and review to third parties may be changed if licenced to do so. However notorious traffickers (AI Fact 6 of Part A) may be found by a Court not to be fit and proper persons and banned from owing, deploying or operating Automated Activity. Censorship conducted by AI requires a licence and the criteria for such must be properly disclosed to users.

Under the containment model, acquisition, export or transfer of data that is not naturally internal or about a related third party, would require a licence if to be transferred between a State or Territory or Commonwealth place or internationally or over a public communications network. This will allow closer supervision and control of licencable Automated Activity data movements.

Due to the opaqueness of Automatic Activity, the standard of proof for breach is proposed to be on the balance of probabilities. Whether the licence regime would create a light touch or impose strict minimum conditions may be left to the regulations. For example, a mandatory licence condition on external human augmentation may be light touch – “tell us about it”. In relation to Automatic Activity with regard to children it may be onerous “only if the child is in imminent danger”. However most Automatic Activity is regulated directly by the law itself as the licencing system only targets Automatic Activity which by its nature would be harder to contain or have greater impacts if it goes wrong.

Obviously the legislative containment model would criminalise non-compliant Automatic Activities conducted by bad actors. However, the proposed civil actions able to be maintained by both regulators and affected persons, may be key to upholding the law in most cases.

SUPPORTING MEASURES

It is proposed that industry assistance should be focused on developing sovereign Automatic Activity capabilities. According to the definition of ‘sovereign’ given above, this means supporting measures should be agnostic to whether the Automatic Activity is composed of closed or open source technology or a mixture. This is because proprietary models may have better prospects of generating export revenue for Australia, while open source models are for the greater good and without which sovereign-AI companies probably cannot compete with Global-AI companies.

In other words, Australia's sovereign AI will owe a debt of gratitude to the open source community and a moral obligation to give something back. On the other hand, it may sometimes be in the national interest that what is given back should not exceed the capabilities of CCP-AI. It is also in the national interest to make sure Free-AI is on par with CCP-AI as explained in Part B above.

Development of AI-safe hardware should also be supported, such as Five Eyes-free not-too-smart phones to support trustworthy communications, to which other devices containing Automatic Activity might safely connect. There is no reason why such medium-tech could not be manufactured in Australia with robotics, if we became a trustworthy jurisdiction, for the market is huge. Support for underlying technologies and initiatives such as Oxen, Lokinet and Session (the author is only a non-paying user) should also be provided.

INCENTIVES

Incentives for Automatic Activity are recommended to be funded according to the following principles:

- The proposal should be for sovereign Automatic Activity (as defined above) that is:
  - associated with an Australian-registered corporation; or
  - intended for interstate business or operations, conducted from within Australia; or
  - intended for operation from Australia to other places.
- The proposal should explain if it is:
  - novel when compared with available open source, or
  - conduct Automatic Activity in a novel way; or
  - make Automatic Activity available in a novel way

- The proposal should be of direct benefit to arms-length third parties or members of a not for profit organisation.
- The proposal will be assisted:
  - if novel and approved, by incentive grant upon success of approved milestones, which may include any registration or licencing requirement;
  - otherwise, if meeting all the principles, yet all or part of the proposal won’t be funded by any grant, to that extent it may be claimed similarly to an R&D tax benefit for expenses incurred within Australia.
  - If the proposal meets all the principles except for novelty then a 100% instant tax write-off may be applied for expenses incurred within Australia;
  - If the proposal is for a start-up or small business, a wavier on any Automatic Activity licence fees, and other government charges.
- If funded by incentive grant, a summary of the proposal should be published along with grant details.

CONCLUSION

This submission attempts to cover the field of Automatic Activity spanning individuals in ordinary life to global Geo-politics. That is because AI will cause change on at least the scale of the industrial revolution, probably greater. From that experience we know strong laws are needed to bridle the forces of change, steering it in a direction compatible with our way of life. The proposed legislative containment model is designed to do that while fostering innovation and uptake, while making Automatic Activity as safe as possible given the complexities involved. Within this framework valuable and flexible industry incentives are proposed to turbo-charge sovereign Automatic Activity.