SOCIAL CYBER INSTITUTE

SIX POINT INSTITUTIONAL PLAN

FOR REVITALISING AUSTRALIAN CYBER POLICY

Honest Accounting of the Cyber Security Environment

1. Police forces in Australia should improve or create statistical reporting of cyber crime in their jurisdictions to an agreed national standard, including data on successful prosecutions, and annual expenditure on countering cyber crime, and such reporting should be widely publicised. The reporting should include international comparisons.

   TOTAL COST: ~ $ 0.5 million per year per jurisdiction, recurring. Total for Australia: ~ $4 million per year

   JUSTIFICATION: Cyber crime statistics in most jurisdictions in Australia are poorly organised and lack credibility, not least because of a lack of focus on reporting on prosecutions undertaken and their success. Absence of such credible reporting, supported by specialist analysis, is a key obstacle to effective public policy not just for countering cyber crime but for giving the public and governments an honest accounting of the cyber security environment.

Focused Parliamentary Scrutiny

2. Federal and state parliaments should establish dedicated standing committees on cyberspace policy. The focus would be on both countering malicious activity in cyberspace and on pursuing the economic and social potential of information technologies more fully. The policy focus of such committees would be appropriate to their jurisdiction's constitutional responsibilities.

   TOTAL COST: $ 1 million per year per parliament, recurring. Total for Australia: ~ $9 million per year

   JUSTIFICATION: In most parliaments of Australia, existing committee responsibilities do not do justice to the range of complex and intractable policy problems created by malicious activity in cyber space. Ad hoc inquiries on various aspects of cyber policy have not met the need.

Law Reform Review

3. Initiate a comprehensive inquiry by the Australian Law Reform Commission (ALRC) on updating Australian law for the information age and give the Commission appropriate additional funding.

   TOTAL COST: $6 million over two years (just over double the current budget of the ALRC)

JUSTIFICATION: Legal reform for cyber policy in Australia has largely been reactive, and it typically defaults to more power for the governments (less for citizens). The country's laws do not compare favorably to those in leading peer jurisdictions in comprehensiveness, reach and effectiveness. The artificial intelligence revolution is already occurring, and Australian law is inadequate for the challenges that this brings.

Arms-Length Policy Institutes

4. Set up at least three complementary centres for cyber policy research and analysis, all fully funded and all operating **independently of universities, businesses and the government**: one focused on privacy, citizen rights and protection of sensitive personal data; one focused on countering cyber criminality; and one focused on national cyber development strategies, including industry policy, education and international mutual assistance. An alternative to three separate institutes might be a a statutory authority with three offices or divisions similar to the Australian Productivity Commission, with an inquiry and report function as well as a research-and-publish function.

TOTAL COST: $6 million per year per centre, recurring (co-funded by federal and state governments and peak industry bodies—no commercial branding). Total $18 million per year nationally.

JUSTIFICATION: Independent policy research institutes are an essential foundation of successful policy. Policy failures in government and business are costing the economy hundreds of millions of dollars per year, if not billions. No Australian government, state or federal, has recognised adequately the transformational significance on society of the information revolution in the same way that the federal government now recognizes the national security significance of it.

Revitalising Public Agencies

5. The federal and state governments should revitalise existing agencies, such as the Office of the Information Commissioner, the Privacy Commission and AustCyber to ensure they have far more policy effectiveness in leading Australian debate to bring out about positive change. The revitalization process must include strengthening key performance indicators, independent annual evaluation, and opening up such organisations to wider community consultation and participation, including in decision-making.

TOTAL COST: ~ $ 1 million per year per jurisdiction, recurring. Total for Australia: ~ $9 million per year

JUSTIFICATION: The foundations have been laid but there is an appearance of passivity and bureaucratism that could usefully be put aside. The lead organisations need to be empowered for more effective public policy influence.

Re-Invigorating Business Leadership

6. The Business Council of Australia, the Australian Chamber of Commerce and Industry, the Australian Industry Group, the Council of Small Business Organisations Australia, the Australian Information Security Association and the Australian Computer Society, among other community and professional lead organisations could jointly establish a National Cyber Policy Council to give vigorous leadership to urgent upgrade of Australian cyber policy and practice, especially in security. This would be stronger to the extent that the Council's positions were as critical of business practices as those we have seen from the Australian Auditor General in respect of sustained poor government performance in cyber security.

   TOTAL COST: ~ $ 3 million per year co-funded, recurring. Funded by business.

   JUSTIFICATION: Other leading cyber powers have far more robust and diverse public activism from their business sector and practitioners than we have seen so far in Australia. Such activism, with a critical mindset, is essential for bring about a shift in public attitudes. Leading business should give a lead in public reporting of their financial commitments to cyber security and protection of personal data.

14 April 2023