ADVANCING SCIENCE FOR SOCIETY: HEALTH, MIGRATION AND TECHNOLOGIES
2025 SUMMIT OF THE S7 ACADEMIES | MAY 6-8 2025 | OTTAWA, ONTARIO, CANADA

ADVANCED TECHNOLOGIES AND DATA SECURITY

DEFINING THE ISSUE

The last two decades have seen a remarkable increase in the number, scope, utility and purposes of both systems for data collection[1] and data processing and archiving technologies, including AI systems, that use data to make inferences or perform actions. According to the *International Scientific Report on the Safety of Advanced AI*, the potential of AI to benefit humankind is counterbalanced by potentially serious risks[2]. Therefore, a multi-level, holistic and human-centric and smart approach to governance and regulation is needed to avoid stifling the benefits of these technologies, while confronting the problems. In the remainder of the document, we use the term *data security* to refer to this interconnected set of concerns.

BACKGROUND

As documented by the panel of the *International Scientific Report on the Safety of Advanced AI*, the tremendous potential from anticipated advances in AI, and the demand for data availability and data quality for legitimate reasons like research in areas critical to the betterment of humankind, are counterbalanced by potentially serious risks due to intentional misuse (e.g., disinformation and other threats to democracy), loss of control, human rights violations, labour market disruptions and loss of livelihoods, and climate / environmental damage. There are high uncertainties on both the magnitude of the potential disruptions and their timeline, but there is consensus on the lack of preparedness in scientific, developer and policy spheres. Following the precautionary principle, it is thus crucial to invest in data security as well as research into how to harness and control advanced AI systems. Social, policy and technological innovations are required at all levels to identify and maximize the collective benefits, and to ensure that guardrails are continually maintained and updated to anticipate, prevent and mitigate risks.

Both specific national and international governance and regulation, and coordination between these, will play an important role in mitigating these risks. Governance and regulatory bodies should outline technical and organisational expectations and guidelines to ensure risks and benefits are properly identified and addressed. They should implement responsive compliance and enforcement regimes that protect people and planet without stifling innovation and economic prosperity. We understand effective governance and regulation as policy innovation are needed, enabling benefits to be shared more equitably across society and providing a framework for innovating responsibly and using technology to meet societal goals. Parties involved in data security include practitioners (e.g., industry and public sector), academic researchers, and the public, whether as individuals or (self-) identified groups.

1 These systems include smartphones, wearable and other personal devices, home and industrial automation, smart meters, medical devices, autonomous vehicles, and public and private surveillance systems.

2 International AI Safety Report (DSIT 2025/001, 2025), https://www.gov.uk/government/publications/international-ai-safety-report-2025

POLICY RECOMMENDATIONS

RECOMMENDATION 1

Because advanced technologies can rapidly become critical infrastructure, it is essential that their management is left neither to corporations that develop them, markets, social adaptation, nor to education and training as a way of transferring all responsibility to people. Corporations, markets and education all play essential roles, but governance and regulation are essential:

a. to protect those who are adversely affected by the differential opportunities and effects of new technologies; and
b. to help ensure that these technologies do not continue to concentrate economic and political power and accentuate existing inequalities.

RECOMMENDATION 2

Regulating data collection and retention is both a regulatory and an ethical challenge. Once data have been collected, two crucial aspects about data-use merit careful regulation: preventing unintended data leakage and ensuring data quality. Emerging regulations such as the *EU AI Act*[3] recognize these concerns but contain gaps. For example, regulations recommend:

a. pseudonymization of data to prevent unintended leakage—although privacy experts have shown that this is often insufficient, and stronger measures like differential privacy are needed; and
b. ensuring that demographic distributions in data used to make useful inferences (e.g., train an AI model) match the population it is intended for—but do not specify how this might be done without violating data confidentiality.

Policymakers should more closely engage with experts, including academics, and members of the public whose data this is, to address these gaps. Two-way communication should guide interpretation of legislation into technical features, such as ensuring that relevant demographic data (e.g., language, age, race, gender) are adequately sampled and secured so that inequities are not further exacerbated. It should also inform directions that academic or industry researchers should prioritise to develop technologies that facilitate compliance by practitioners and enforcement by regulators (e.g., through the invention of data analysis approaches that produce verifiable guarantees).

RECOMMENDATION 3

Given that data-driven systems have entered every aspect of human endeavour, the "threat surface" of such systems has dramatically increased. People from all walks of life are now involved in using and managing these systems. Commissions, omissions, and mistakes by them can lead to security breaches. The number of instances where human error led to ransomware or other attacks against critical infrastructure such as hospitals illustrates the scale of the problem. A broad-based and ongoing effort to bring about security/privacy "literacy" is needed. Policymakers should incentivize the ongoing development of tools and training programs to bring about and continuously improve such literacy, and the development of alternative "backup" systems and procedures to mitigate human errors.

RECOMMENDATION 4

Publics can't be thought of as one undifferentiated group, whether it is "users", "consumers" or "people." Groups and individuals engage with and are affected by advanced data and surveillance technologies in very varied ways, and these have consequences that can range from trivial to vital, from minor changes in convenience like automated home delivery, through invisible forms of discrimination, for example, the embedding of racial and gender prejudice in automated hiring or sentencing, to exclusion from countries as the result of no-fly lists based on categorical suspicion, or even death in the case of AI-based weapons-targeting systems. Considering "data justice"—fairness in the way people are categorised and treated in the collection and use of data—is therefore an essential addition to existing understandings of legal, economic, social and environmental justice.

RECOMMENDATION 5

Specific vulnerabilities also need to be addressed, for example, the very young, the elderly, particularly those with cognitive impairments, and those with illnesses, who may be more likely to fall victim to malicious use of advanced technologies, for example scammers recruiting older people, the use of ransomware against hospitals, and predators targeting children. However, such vulnerabilities should not be used as an excuse for the extension of unjustified and generalised surveillance and restrictions on human rights. When increased security and surveillance are introduced,

3 EU AI Act, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

such measures may contribute to the further marginalisation of the very groups who are already the victims of data injustice.

RECOMMENDATION 6

Regulators will have to incorporate data security considerations linked to emerging technologies into their existing mandates and, as a result, ensure that they develop the required in-house expertise and capacities, communication and coordination. New governance systems and regulatory entities may also be needed at both national and international levels to coordinate enforceable guidelines, standards and best practices across sectors and interested parties when advanced technologies trigger systemic and disruptive changes in society, such as is the case with AI. Data security matters because data and advanced technologies now mediate not just innovation and prosperity but health, education, creativity, the arts, expression, and knowledge.

RECOMMENDATION 7

Clarity is needed when it comes to the responsibilities of each regulator, so that new regulatory entities do not lead to inefficiencies from a more fragmented regulatory landscape. The G7 is one such forum for coordination, but there must also be a much wider discussion that involves existing recognised regulatory bodies (even if responsibilities are contested), for example UNESCO and the International Telecommunications Union (ITU), the nations of the Global South, and non-G7 economic and technological leaders.

RECOMMENDATION 8

We recognise that advanced technologies inevitably raise national security concerns, however it is the responsibility of academies and governments to consider the interests of global humanity and the planet. Cooperation for peace and global security is necessary. We would support the creation of a "CERN for AI" –providing widespread and equitable access to compute power for researchers from around the world, enabling them to build datasets, and also supporting multi-way learning between researchers from the Global North and South.

RECOMMENDATION 9

We recommend that to address the difficulty in training the appropriate experts for regulation enforcement, policymakers should incentivize work done in the open-source model. Such incentives could come in the form of dedicated funding and allocation of resources to support the open-source community in maintaining the software and its integrity. Popular open-source projects have shown that openness and transparency can also lead to strengthened security. However, decisions on allowing or restricting open-sourcing of powerful AI systems must be subject to democratic oversight, and safety regulations that apply to proprietary systems must also apply to open-source systems.

RECOMMENDATION 10

Generative AI models can produce media of impressive quality and are being misused for deception. Such models are also flooding the internet with misinformation, not necessarily deliberate deception but false information which can then in turn go on to be used and recycled again by AI models, leading to both model degradation and further misinformation. Regulations, like the EU AI Act, attempt to address this concern[4]. "Watermarking"—the practice of embedding patterns in AI-generated content which enables them to be identified as such[5]—is one solution, but it is known to be brittle. Watermarks verified by the owners of the AI models may not be enough to stem harms from deceptive AI-generated data, and may not change people's behaviour in terms of the way they interact with data—particularly in highly technology-driven societies. Policymakers should incentivize exploration of different techniques for verifiable data provenance.

RECOMMENDATION 11

Finally, cloud-based, AI technologies such as Large Language Models (LLMs) have a large direct impact on the global climate. For example, the energy use resulting from a ChatGPT query is far higher than from a simple web search. This is not addressed by unevidenced assertions that increasing energy use creates incentives to accelerate the switch to sustainable sources of power. Governance and regulation of data and its processing should be coordinated with policies for environmental and energy sustainability.

4 EU AI Act, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

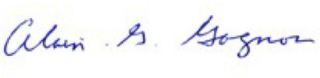
5 https://www.brookings.edu/articles/detecting-ai-fingerprints-a-guide-to-watermarking-and-beyond/

CANADA

The Royal Society of Canada

RSC SRC

ALAIN-G. GAGNON



FRANCE

Académie des sciences

ACADÉMIE DES SCIENCES
INSTITUT DE FRANCE

FRANÇOISE COMBES

GERMANY

German National Academy of Sciences Leopoldina

Leopoldina
Nationale Akademie der Wissenschaften

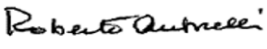
BETTINA ROCKENBACH

ITALY

Accademia Nazionale dei Lincei

ACCADEMIA NAZIONALE DEI LINCEI

ROBERTO ANTONELLI



JAPAN

Science Council of Japan

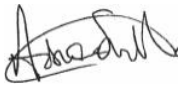
MAMORU MITSUISHI

UNITED KINGDOM

The Royal Society

THE ROYAL SOCIETY

ADRIAN SMITH



UNITED STATES

National Academy of Sciences

NATIONAL ACADEMY OF SCIENCES

MARCIA McNUTT