Picture credit: Pimloc

TAKING RESPONSIBILITY

Simon Randall *explores the importance of carefully navigating the intersection of biometrics, AI, security, privacy and ethics*

In the past 18 months, the world has gone through a major technological shift. There have been major advancements in emerging technology, with a surge of generative AI developments that have tipped into the mainstream consciousness. These early stepping stones towards GAI (general artificial intelligence) now encompass the ability to generate plausible text, images, audio and video that can fool the best of us. The rapid growth of foundational generative technologies, such as ChatGPT and DALL-E from Open-AI, has spawned an ecosystem of new initiatives, applications and endeavours built on these new capabilities. From new start-up technology businesses to nation states who are racing to have control and oversight of the underlying foundation models in their jurisdictions.

The pace of change in the last 12 months since ChatGPT4 launched has been nothing short of bewildering. Alongside the benefits of general chat agents and generative techniques, lots of new threats have emerged, with governments, organisations and society trying to navigate their way through an evolving understanding of opportunities and risks. As companies race to create more engaging and persuasive technologies, the world has recognised the importance of placing responsible development of AI front and centre.

Two opposing sides have emerged; those for and against AI, in the main driven by a fear of existential threats and separating the academic and private sectors on philosophical grounds. Amidst the frenzy, there is much hyperbole and fear-mongering, but there are also real underlying threats that these technologies open up, especially in the worlds of security and privacy.

It's not a simple problem but there are essential principles that organisations and individuals can use as tracks for charting this new world. Responsible organisations can and should take guidance in the way that they manage and harness AI. There is lots of informed brain power having a debate on these topics across the globe, with a range of policies starting to emerge.

The Bletchley Declaration on AI Safety has seen 28 nations work together to identify, evaluate and regulate the risks of using AI

To understand these principles, it's important to grasp the changes happening from regulatory and technological perspectives. Global leaders have come together to ensure that the AI revolution stays guided by values and protection, and a shared vision has emerged for an AI-empowered world operating under a framework of responsibility and trust.

The mix of regulations worldwide reflects diverse cultural attitudes towards privacy and a race against foreign influence, with the US competing with China economically, militarily, and on AI, the EU emphasising its digital sovereignty and India swinging between a non-regulatory approach and a more cautious one.

India, today's chair of the Global Partnership on AI (GPAI), first said that it would not regulate AI in a pro-innovation decision to move closer to its aim of global AI leadership. However, the country's strong cultural identity and values focused on morality and societal goals have challenged this path, and Modi's call for 'ethical' AI has moved the country towards actively creating regulation through a risk-based approach.

China released measures to regulate specific aspects of AI, ranging from algorithmic recommendations to deep synthesis or 'deepfake' technology and generative AI. This iterative approach is widely regarded as a tactic to maintain space for innovation and competitive edge, and for AI technology to accelerate before regulatory limitations can hold it back.

The West has taken a more risk-based approach. President Biden's latest executive order is a show of his administration's commitment to the security, privacy and safety aspects of AI. In a similar vein, US Senate Majority Leader Chuck Schumer is championing a bipartisan effort to encourage collaborative efforts within the US. These initiatives point to the US administration's concentrated effort on AI regulation, spearheading innovation alongside the establishment of global regulatory norms, ahead of other nations. As Schumer said in April 2023, his country should: "not permit China to lead on innovation or write the rules of the road" for AI.

In November, UK Prime Minister Rishi Sunak convened top government representatives, leading AI executives and prominent figures from civil society. The Bletchley Declaration on AI Safety was created: the world's first joint commitment by 28 leading AI nations to work together to identify, evaluate and regulate the risks of using AI.

This has paved the way for more international cooperation on the use and regulation of AI and spurred governments towards action. However, there is a long way to go and the current patchwork of global AI regulation is not robust or mature enough to properly protect society from risks of a rapidly evolving technology.

The AI Safety Summit paper notes that the computing power used to train the most advanced AI systems has increased by 55-million times over the last decade. That power will increase dramatically. As AI power grows, so do the potential risks that it poses. Threats to security and society are profound because generative AI reduces barriers of entry for malicious actors. Open source and easy to use, it enhances the capability of individuals and increases the effectiveness of cyber attacks and data breaches.

Risks tied to large-scale biometric data sets – such as voices, faces and images – are of particular concern to public data privacy and security. Anyone can now create deepfakes and semi-synthetic content, increasing the risk of fraud, impersonation, sexual abuse images and other abuse of sensitive biometric data.

Biometrics in video footage were once the de-facto standard of evidence. That no longer stands. Truth and authenticity are under the microscope and leaders must act to manage the difficulty of the general public to distinguish between authentic and AI-generated misinformation.

THERE ARE TOOLS THAT ORGANISATIONS CAN IMPLEMENT TO PROTECT THE PUBLIC AND ITS DATA

This comes at a time when visual AI systems are seeing increased mainstream adoption. The global market is booming, with Statista citing a projected growth of 11.10 percent in 2023 and a market value expected to reach $10.9-billion by 2030.

As well as making FRT more powerful, advancements in AI have made biometric tech more versatile. It can now be deployed using cloud-based technology or integrated into edge devices, offering better speed, security and affordability.

Biometrics and AI offer enhanced security by replacing pin codes and passwords, reducing the risk of hacks and data breaches. In law enforcement, it helps identify offenders and locate missing or vulnerable individuals. Use in transportation streamlines travel and enhances safety, and in warehousing and retail, it improves efficiency and security for employees and customers. We are seeing FRT being rolled out for public security and even in many sensitive sectors including education, health and public services.

In healthcare, beyond safety and security, tech advancements are being used to aid diagnoses. Healthcare professionals can use AI, facial recognition and computer vision to pick up on subtle symptoms of rare genetic conditions. Teams at Johns Hopkins Hospital are developing an algorithm to identify alterations in patients' facial characteristics, which could distinguish brain damage caused by a stroke from conditions like seizures or anxiety – speeding up treatment and recovery.

As visual AI systems become more used and more faces, human behaviour and identifying information are collected, the liabilities and risks associated with capturing and managing this sensitive data are multiplying. Data protection must keep up with the intelligence and speed of AI models – in an arms race against bad actors.

Privacy, a fundamental human right, is under threat and the implications of such sensitive data in the wrong hands, whether by design or accident, are profound. Its misuse can spread misinformation like wildfire, change beliefs and ultimately impact global perception and behaviour. In a new report released by Freedom House, a human rights advocacy group,

researchers documented the use of generative AI in 16 countries "to sow doubt, smear opponents, or influence public debate".

Last year, the Biometrics Institute identified seven Ethical Principles for Biometrics to ensure the responsible and ethical use of biometrics. The Insitute's Good Practice Framework also provides crucial guidance to manage risks, including those associated with AI and deepfake technologies.

DATA PROTECTION MUST KEEP UP WITH THE INTELLIGENCE AND SPEED OF AI MODELS

Beneath these welcomed principles, the ethical usage of biometric data and AI hinges on maintaining data integrity and security, necessitating in-built defences against potential vulnerabilities and threats. On an organisational level, effective management of these risks is the only way that businesses and society can fully leverage its benefits.

There are tools and infrastructure that responsible organisations can implement to protect the public and its data, and four fundamental approaches. These pare the backbone of data privacy regulations across the world, including GDPR and the Data Protection Act 2018 in the UK, the Children's Online Privacy Protection Act (COPPA), the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Privacy Act of 1974 in the US.

The first principle is proportionality. Organisations must ensure that biometric data collection is aligned with the necessity of the task. This extends to the duration of data storage. Regular audits can help ensure compliance with this, preventing data overreach.

The second covers clarity and communication. People must be aware they are being filmed and you must inform them of measures taken to protect their privacy. Clearly defining policies and processes for data handling is another principle. This means establishing clear guidelines for data storage, sharing and protection. Well-defined processes for responding to data breaches and other security incidents ensure swift and effective action to mitigate any potential damage.

Finally, comes security. Particularly in the face of emerging AI-powered cyber threats, constant updates and adaptations are needed to counter ever-evolving malicious actors. Whether employing advanced cyber security measures, regular system updates, or staff training, data security measures should be regularly reviewed and updated to reflect technological advancements.

ETHICAL CONSIDERATIONS

The future, both exciting and concerning, can be navigated successfully by responsible organisations and individuals. The world needs to embrace technological advancements and deeply embed ethical considerations into its operational fabric. This means being proactive in understanding the implications of AI and biometric technologies and the regulations surrounding them, engaging in transparent dialogue, and implementing robust privacy safeguards. It's about creating a culture where ethical decision-making is a norm, not an exception.

Keeping to these principles, there is an opportunity to steer the course of technological development to respect and enhance human values. By doing so, organisations can not only mitigate risks but also build stronger, more trusting relationships with customers, employees and the public. This is paramount for the safety and privacy of all, regardless of location or the complexity of the technologies involved. Only then can we move towards a future where technology empowers and protects, in equal measure ●

Simon Randall is the co-founder and CEO of Pimloc, a global privacy and security company specialising in anonymisation technology for visual data. Simon has spent decades working in the tech and security sectors, and advocates for greater legislation and education of all things data.

The current patchwork of global AI regulation is not robust or mature enough to properly protect society from risks of a rapidly evolving technology

Picture credit: Pimloc