Modern slavery risks in the higher education sector

Surveillance Technology

24-hour monitoring is possible via smart phones, which can collect location, voice, health data and communication history.[1]

US$59.92 billion is the estimated value of the surveillance sector in 2025. This is expected to grow to USD $188.19 billion by 2035.[2]

What is modern slavery?

Modern slavery is a serious violation of an individual's dignity and human rights. Exploitative practices, including human trafficking, slavery, servitude, forced labour, child labour, debt bondage and forced marriage, are all considered modern slavery and are serious crimes under Australian law.

Regulatory Context

Modern Slavery Act 2018 (Cth)

Organisations, including universities, based or operating in Australia with at least AU$100 million in annual consolidated revenue are required to report annually on the steps they have taken to identify and address modern slavery risks in their operations and supply chains. See *Commonwealth Modern Slavery Act Guidance for Reporting Entities*.

Modern Slavery Act 2018 (NSW)

Certain universities in NSW have due diligence reporting obligations under the NSW Modern Slavery Act to ensure the goods and services they procure are not the product of modern slavery. See *NSW Anti-slavery Commissioner's Guidance on Reasonable Steps to Manage Modern Slavery Risks in Operations and Supply-Chains*.

Modern slavery and human rights risks linked to surveillance technology

Forced Labour

Surveillance technologies may enable employers to coerce workers, through monitoring performance, communications, and movement. There are reports of surveillance technologies used to identify and detain ethnic minorities, who are placed into forced labour programs, providing products to global supply chains.

Online Exploitation

Children can be targeted online for labour or sexual exploitation, through grooming, coercion and deception. Digital tools, such as social media, AI, and biometric tracking can be used to identify, recruit, monitor, and control vulnerable victims.

Human Trafficking

Surveillance technologies may support trafficking operations through assisting traffickers to recruit, control and continue to exploit victims. For example, traffickers may use the GPS technology on mobile phones to track and control the movements of victims. Human traffickers are increasingly using social media to contact, recruit and monitor victims.

Why is the sector high risk?

Limited capacity for informed consent. Workers may be unknowingly placed under surveillance without consent or may be scared to refuse a request to monitor their activities.

Surveillance undermines freedom of assembly and free speech. Surveillance can have a chilling effect on political and civic activism through tracking and detaining human rights defenders.

Global regulation is lacking. While there are developments in some regions, e.g., the EU, there is a lack of regulatory frameworks to protect citizens from adverse impacts of surveillance technologies and to safeguard human rights.

[1] Using Smartphones to Collect Behavioural Data in Psychological Science: Opportunities, Practical Considerations, and Challenges, Perspectives on Psychological Science, 2016.

[2] Video Surveillance Market Industry Report 2025-2035: Video Surveillance Market to Triple by 2035, Driven by AI, IP Cameras, and Cloud-Based Security Solutions, Yahoo Finance, 2025.

Modern slavery risks in the higher education sector

Surveillance Technology

THE UNIVERSITY OF SYDNEY

How modern slavery and human rights risks in the surveillance sector may be linked to universities

Procurement *Universities may be linked to modern slavery risks in their supply chains, including in the extraction of raw materials, the manufacturing of components, final assembly of products and in the labour to deliver services on campus.*	
Product, Sector & Geographic Risk	Sourcing surveillance equipment or software without adequate due diligence: • **Facial recognition software for campus safety (**e.g. to unlock devices or entry into secure buildings) may violate staff and student privacy and link universities to third parties involved in human rights harm, such as the use of facial recognition software to track and detain ethnic minorities. • Individual biometric data may be accessed and misused by 3rd parties, presenting a privacy risk to university staff and students. • **Location tracking devices used by universities or their suppliers to monitor employees for safety and performance** have been reported to be misused to coerce workers into excessive hours, enforce rigorous productivity standards, limit union activity and violate privacy *(e.g. cleaners wearing GPS-tracking smartwatches to monitor performance).* • **Surveillance equipment**: Sourcing security systems, CCTV cameras and other surveillance equipment may be linked to forced labour in the manufacturing of electronic components, particularly in China, Malaysia and Taiwan, and forced and child labour in the extraction of critical minerals needed for electronics. • **Limited safeguards of university usage of mobile apps** may expose staff to privacy violations, through the tracking of communications, internet searches and movements by malicious actors *(e.g. spyware installed on phones used to target academics, along with journalists and human rights defenders).*
Teaching & Research *Universities may be linked to modern slavery risks, through their teaching and research activities and partnerships. Risks often intersect with other human rights concerns and counterparty risks related to sensitive technologies, sanctions and national security.*	
Research Development & Application Risks	Research without adequate due diligence of the partner, design or application: • **Biometric data**, including DNA, fingerprint, face and retina scans, provided by third party agencies for research may be collected under coercive conditions or without adequate informed consent, particularly when there are vulnerable groups, such as children, involved *(e.g. journal retracts article on genetic data from China's Uyghur population over ethical concerns the research could be used to enable mass surveillance).* Research with dual academic and commercial use without adequate due diligence: • **Surveillance research used for defence purposes,** such as drones, facial recognition or autonomous targeting using AI, may inadvertently support foreign militaries or enable human rights harm • **Development of surveillance software with a private partner** for commercial use may be misused by a third-party for human rights violations. This is particularly a risk if the intellectual property is owned by the partner company (*e.g. Australian university linked to Chinese government surveillance of ethnic minorities through a research partnership).*
Partnership & Collaboration Risks	**Partnering with companies with links to human rights violations:** • The U.S. has sanctioned several technology firms for development of AI-enabled surveillance software involved in the monitoring and repression of ethnic minorities *(e.g. U.S. sanctions China's largest facial recognition start up).* • Australian universities have faced criticisms for collaborations linked to potential misuse of surveillance technologies for human rights harm.

Modern slavery risks in the higher education sector

Surveillance Technology

Case study

This case study has been developed using publicly available reports. It is intended solely for illustrative purposes and does not represent any specific university, supplier, or partner organisation.

An Australian University entered a high-value research agreement with an overseas technology company to develop advanced video analytics and AI systems for public safety. The project aimed to improve threat detection and emergency response through real-time monitoring capabilities.

Two years into the research partnership, a media investigation revealed that similar technologies used by the partner were being deployed in large-scale surveillance programs, used by foreign governments. While there was no clear evidence the University's research was being misused, the media report raised concerns about the potential use of research outputs for monitoring individuals and restricting freedoms.

The University launched an internal review to determine whether its research contributed to these surveillance practices. The University acknowledged the inherent risks of dual-use technologies and the reputational harm associated with such partnerships. As a result, the university suspended new collaborations with the partner and committed to implementing stronger governance measures, including human rights impact assessments and stricter oversight of projects involving surveillance-related technologies.

Learn more

- The right to privacy in the digital age – United Nations General Assembly, Human Rights Council, 2025.
- Navigating the surveillance technology ecosystem – Access Now, Business and Human Rights Resource Centre and Heartland Initiative, 2022.
- Being monitored at work? A new report calls for tougher workplace surveillance controls, The Conversation, 2025.
- Xinjiang Supply Chain Business Advisory, U.S. Department of State, 2023.
- Electronics Watch

This resource is provided for your general information only and is not a replacement for individual advice that is tailored to your needs. Users of this resource requiring or seeking such advice are responsible for obtaining that advice from their lawyers or other professional advisors. They should do so before taking (or refraining from taking) any action in reliance on any information contained in the resource.

Modern slavery risks in the higher education sector

Surveillance Technology

THE UNIVERSITY OF SYDNEY