Is your organisation's data governance capable of managing your technology risks?

BY **DR JOHN SELBY AND ANNELIES MOENS, PRIVCORE**

Technologies that promise to increase capabilities while also reducing costs excite many organisations. To reduce harm to their staff and lower theft rates, two major retailers in Australia (Bunnings) and the United States (Rite Aid) deployed facial recognition technologies to target customers allegedly misbehaving in their stores; however, after significant investment, each later abandoned those implementations when regulators found them to have breached their customers' privacy.

Dr John Selby

Annelies Moens

Using the concept of the OODA Loop, this article explores how misalignment between the risks posed by technologies and an organisation's data governance capabilities contributed to failed technology projects. It also identifies ways for organisations to reduce the likelihood of similar problems in the future.

WHY DID BUNNINGS AND RITE AID ADOPT FACIAL RECOGNITION TECHNOLOGY?

Executives at Bunnings and Rite Aid were responding to a common organisational problem: external threat actors were causing harm to their staff and their profitability. They turned to facial recognition technologies from third-party vendors because they wanted to improve their organisations' abilities to detect those threat actors. They also intended for their in-store staff to be able to respond in a timely manner to prevent further staff harms and thefts, all at a lower cost than alternative strategies (such as hiring more in-store security guards).

THE OODA LOOP

Invented more than 50 years ago by United States Air Force Colonel John Boyd, who wanted to improve decision-making in military conflicts, the OODA Loop has been applied to organisational strategy. It is an iterative process based on four steps: observe, orient, decide and act. Staff within an organisation observe a problem or threat, then consider what options are possible to respond to that problem or threat. Next, a decision is made regarding an action plan, which is then acted upon. Reducing the time it takes to progress through the OODA Loop gives organisations strategic advantages.

While improving the speed within which an organisation can complete an OODA Loop is generally considered to be a positive goal worthy of achieving, when OODA Loops operate at different speeds within an organisation, capability gaps can emerge, which create organisational risks. Enterprise risk planning should, in theory, help organisations keep their OODA Loops synchronised, with advances in capabilities in one area matched by advances in other areas.

In these case studies, two OODA Loops were operating simultaneously within Bunnings and Rite Aid: the first was the loss-prevention/safety OODA Loop designed to prevent physical harms and economic losses. The second was the data-governance OODA Loop, which is meant to identify and control the organisation's data governance risks.

OODA LOOP ONE: LOSS PREVENTION AND SAFETY

Both Bunnings and Rite Aid appear to have sophisticated capabilities in their loss prevention and safety teams, who were motivated to increase the speed at which they could observe, orient, decide and act upon threats.

OBSERVE

For both Bunnings and Rite Aid, executives observed misbehaving customers harming the safety of their staff and stealing products, leading to reduced profits. Each company produced and analysed detailed records for product thefts and customer assaults on their staff.

ORIENT

Senior executives at each organisation oriented by considering whether to hire more security guards or adopt a technology solution, such as facial recognition tools.

DECIDE

After soliciting bids from potential suppliers, those executives decided to implement facial recognition tools supplied by chosen vendors.

ACT

Bunnings and Rite Aid's internal security teams and in-store staff act upon the information generated by those tools to tell particular customers to leave their stores (and, in Rite Aid's case, to verbally accuse certain customers of being thieves). Internal security teams saw the technology as accelerating the rate at which they could complete an OODA Loop to prevent assaults on frontline staff and thefts from those stores. Those executives and staff believed the technology to be a 'win' for their organisations.

OODA LOOP TWO: DATA GOVERNANCE

Unfortunately, it appears that the data-governance OODA Loops for Bunnings and Rite Aid were not as capable or efficient as their respective loss-prevention and safety OODA Loops.

OBSERVE

Neither organisation appears to have had (at the time) data governance systems with sufficient maturity to rapidly observe the existence of an increased privacy risk emerging from adoption of a technology like facial recognition tools.

ORIENT

The standard tools to orient an organisation to such emergent risks, a privacy threshold assessment and a more detailed privacy impact assessment, were not activated to focus the organisation on their increased privacy risk exposures prior to the launch of the technology into their stores.

While Bunnings sought advice from its lawyers, it later chose to claim legal professional privilege over that advice. Consequently, the Australian Privacy Commissioner did not give any weight to that advice when deciding against the company. It is unclear whether Rite Aid sought legal advice.

DECIDE

Decision-making regarding the data governance risks appears to have been severely limited in both organisations. Privacy was mentioned once during a presentation on facial recognition technology by a Bunnings senior executive, and Rite Aid executives ignored vendor disclaimers about the accuracy of their facial recognition tools when signing the technology contracts.

ACT

Each regulator criticised the inability to operationalise privacy risk management effectively within the organisations. Staff training was non-existent or inadequate, particularly for frontline staff. While Bunnings did keep trained internal security staff in the loop, Rite Aid was heavily criticised for providing no staff training and for automatically passing on error-filled decisions by its facial recognition technology to frontline staff without disclosing the technology's confidence scores for those decisions. This led to Rite Aid's in-store staff making nonsensical decisions, such as forcing Black customers to leave stores because they had been (mis-)identified by the technology as Caucasian, blonde-haired thieves.

The regulators criticised both organisations' failure to ensure appropriate data quality for the datasets fed into the facial recognition system (which the vendors stated required well-lit, portrait-style photos to produce accurate results). Inclusion of external datasets (supplied by law enforcement) was similarly criticised. This led to a high rate of false positives for Rite Aid (innocent customers being falsely identified and accused of being thieves/criminals), and an unknown rate of false positives for Bunnings (the data needed to calculate this rate was redacted in the Australian Privacy Commissioner's decision without explanation).

THE REGULATORS CRITICISED BOTH ORGANISATIONS' FAILURE TO ENSURE APPROPRIATE DATA QUALITY FOR THE DATASETS FED INTO THE FACIAL RECOGNITION SYSTEM ...

Notice and consent are the basis for many privacy and data protection regulatory systems around the world. The Australian Privacy Commissioner found that Bunnings staff were unable to produce privacy notices and privacy policies for its customers to read when entering its stores that complied with the requirements under Australian privacy law. The regulator criticised this failure to give adequate notice of the use of the technology, viewing it as undermining Bunnings's claim that the technology was intended to deter misbehaving customers. Rite Aid also chose not to notify its customers that it was using facial recognition technology, and even told its staff not to reveal the company's use of that technology to customers or to the media.

Despite the technology being incorporated into their 'business as usual' practices over the course of several years, neither Bunnings nor Rite Aid appear to have undertaken timely data governance reviews of the performance of their facial recognition technologies.

It was only two years after launching its facial recognition tool across 62 stores that Bunnings's parent company, Wesfarmers, introduced a 'Minimum standards for the use of facial recognition' document. While the regulator accepted that this document contained some useful controls, it criticised the lengthy delay in creating that document. Bunnings was also unable to provide evidence that it was complying with those minimum standards. For example, the company had not documented the contents (or dates) of the training it provided to staff, did not create required documents or reports, and failed to adequately update its privacy policy.

RECOGNISING WHEN SOME OF YOUR ORGANISATION'S OODA LOOPS ARE OPERATING AT DIFFERENT SPEEDS IS CRITICAL FOR SENIOR EXECUTIVES

Rite Aid was criticised for skewing the deployment of its facial recognition tools into stores that serviced predominantly African American and Asian customers. It failed to conduct basic bias and discrimination tests, which form a standard part of technology risk assessments.

CONSEQUENCES FOR BUNNINGS AND RITE AID

Both Bunnings and Rite Aid faced significant media attention, regulator inquiries and public criticism for their implementation of facial recognition technology without complying with privacy regulations. Rite Aid consented to the US Federal Trade Commission's order, including a five-year ban on use of the technology, incurring significant new compliance costs, and deletion of both its facial recognition database and algorithms.

Bunnings has chosen to appeal the Australian Privacy Commissioner's determination that it breached the Privacy Act. The Australian Privacy Commissioner's determination requires Bunnings to publish a statement on its website for 12 months facilitating privacy complaints by members of the public about its actions, to preserve evidence of its actions, and then to eventually destroy its facial recognition datasets.

CONCLUSION

When each organisation was faced with staff safety and theft risks, Bunnings and Rite Aid executives decided to adopt facial recognition technology as a solution. Unfortunately, accelerating their loss prevention and safety capability to manage those risks exceeded their organisations' data-governance capabilities, resulting in adverse regulator findings.

Recognising when some of your organisation's OODA Loops are operating at different speeds is critical for senior executives. Taking a holistic risk management perspective will help organisations to synchronise the capabilities of their different risk-management OODA Loops, reducing the overall likelihood that technology investments will fail. S

About the authors

Dr John Selby *is Privcore's Principal Consultant and Head of Research. He is also an Honorary Fellow at Macquarie Business School's Centre for Emerging Risks. With over 25 years' experience advising clients on technology risks, he focuses on privacy, AI and cyber security issues. An IAPP Fellow of Information Privacy, Selby has published numerous articles and research whitepapers, has won awards, and has designed and taught university courses on privacy, AI and cyber security risk governance and law. He frequently presents at conferences around the world, including AISA's CyberCon.*

Annelies Moens*, a privacy professional since 2001, founded Privcore in 2018. She was the 2023 IAPP's Vanguard Oceania award recipient for demonstrating exceptional leadership and creativity in privacy and data protection.*

This article was based on the Commissioner Initiated Investigation into Bunnings Group Ltd (Privacy) [2024] AICmr 230, which (at the time of writing) Bunnings is appealing, and US Federal Trade Commissioner v Rite Aid Corporation and Rite Aid HDQTRS Corp consent agreement Case No. 2:23-cv-5023.