Navigating the Rise of Workplace Surveillance: Balancing Trust, Privacy and Productivity

As remote work and hybrid models become the norm across many sectors, more employers are exploring workplace surveillance technologies to monitor productivity, protect data, and ensure safety. But with these tools comes increased scrutiny - both legally and culturally - around privacy, consent, and trust.

Why This Matters in 2025

The Office of the Privacy Commissioner (OPC) has expressed concerns regarding the use of monitoring tools in employment settings. The OPC's guidance underscores the importance of balancing employer interests with employee privacy rights. For instance, the OPC advises that requiring employees to keep their laptop cameras on at all times while working from home is likely to be considered unreasonable and intrusive, potentially breaching Principle 4 of the Privacy Act 2020. This principle stipulates that the means of collecting personal information should not be unfair or unreasonably intrusive.

Additionally, the OPC emphasises the need for transparency when monitoring employee use of work computers and accounts. Employers should clearly inform employees about what information is being collected and the purposes for its use. Covert collection of information is deemed unfair unless there is a particularly strong reason for not informing individuals about the monitoring.

These guidelines highlight the OPC's ongoing concern about ensuring that workplace surveillance practices are conducted lawfully and respectfully, safeguarding employee privacy while addressing legitimate business needs.

Surveillance may include:

- Keystroke logging or screen recording
- Monitoring of work emails, web browsing or file access
- Use of GPS/location tracking on work devices or vehicles
- CCTV in the workplace
- Requiring cameras on PCs or other devices to be left on

What Employers Need to Know

Surveillance isn't inherently unlawful - but it must be:

- **Transparent:** Employees must be informed of any monitoring, ideally in writing and in advance.
- **Purposeful:** There must be a legitimate reason for the surveillance e.g. linked to the role or workplace risk.
- **Proportionate:** The level of surveillance must not be excessive in relation to the issue being addressed.
- **Compliant:** Employers must comply with the Privacy Act 2020.

Tips for Employers

- Review your employment agreements and policies - do they mention surveillance or monitoring at all?
- Engage staff early - explain the reasons for any monitoring and give them a chance to raise questions or concerns.

- Focus on outcomes - surveillance should never replace good leadership or regular conversations about performance and expectations.
- Train your managers and staff on their Privacy Act obligations
- Don’t assume third-party providers are compliant - always vet the tools you use and how they store data.

Workplace surveillance can create unintended consequences if not handled thoughtfully - damaged trust, reduced morale, or potential privacy breaches.

Taking a values-based and legally sound approach not only reduces risk, but it also shows your team that you respect their privacy, even in a digitally connected workplace.

021 932 332 marie@tovioconsulting.co.nz www.tovioconsulting.co.nz