Resolution: Workers Privacy and Data

Workers' data is increasingly being created, collected, stored and sold by employers and technology service corporations. This workers data is used by employers to make managerial decisions, and is being monetised by technology companies providing payroll, training and other corporate services. Corporate surveillance and monitoring of workers has gone to new heights during the pandemic, with monitoring now extending to workers' homes and private lives via software, apps and GPS.

Data collected and stored by employers is often personal and sensitive, including home address, tax and bank information, health information, biometric and location data, and more.

The Executive notes that there are very few rights for workers to privacy or transparency in how employers and other corporations use, store and sell data.

The Executive notes that as more data is collected about workers, this data is an increasingly attractive target for hackers. An increasing number of employers and technology providers have personal and sensitive worker data in breaches, including Telstra and NAB in 2022 and the SA Government in 2021 – tens of thousands of workers had their personal and sensitive data breached in these 3 cases alone.

The Executive affirms the following principles about workers' data and privacy rights:

- Employers should be required to protect the data of their employees
- Workers must have right of access to data collected on them, including right to have data rectified, blocked or erased
- Workers & unions must be consulted and agreement reached before introduction of new systems that enable surveillance or monitoring
- Data collected about workers must be minimalised – only what is necessary

- Data collection and processing policies & decisions must be transparent and available to workers and their unions
- Restrictions on collection and use of biometric and GPS/location data
- These rights should be implemented and enforceable via collective bargaining

Moved:

Seconded: