

# The right to disconnect from work—and employer surveillance—is growing globally. Why is NZ lagging?

August 21 2024, by Amanda Reilly and Joshua A.T. Fairfield

---



Credit: Pixabay/CC0 Public Domain

A new law giving Australian workers the "[right to disconnect](#)"—to refuse contact from their employers outside their working hours (unless that refusal is unreasonable)—comes into effect this month.

The legislation is a response to growing awareness of the health and safety costs of stress and overwork associated with constant connectivity. A number of [other countries](#), including France and Belgium, have also recognized such a right, or are considering doing so.

But New Zealand is not. Its regulation of working time is comparatively rudimentary compared to [more comprehensive regulation](#) in other countries, although the Minimum Wage Act limits working time to 40 hours a week unless the parties agree otherwise.

New Zealand should consider the right to disconnect for workers. But this needs to go beyond limits on when employers can actively contact workers. The government also needs to tackle employers' ability to use newly developed technology to spy on, track and record everything workers do in their time off.

Constant surveillance is now a core feature of algorithmic management software. This gathers data from work-from-home laptops, biometric scanners, workers' smartphones, AI searches of social media, worker-driven vehicles, and even internet-of-things-enabled employee badges.

These devices don't necessarily stop recording when the worker leaves the workplace or stops work for the day.

## **Harms of 24/7 spying**

Workers who are subject to 24/7 surveillance cannot truly disconnect from the workplace. [Research](#) has shown the perception of [constant surveillance](#) is bad for mental health and well-being. Misuse of this

information by spying bosses, [nosy co-workers](#), bullies or stalkers unquestionably harms workers.

Moreover, the data gathered from workers' homes, smartphones, vehicles and biometrics can be commodified and resold to third-party data brokers.

These brokers are largely unregulated and operate well outside New Zealand's borders or control. This means there are few real limits on who could purchase and use this information.

## **New Zealand lags in worker protection**

New Zealand law does little to protect workers from these privacy invasions and [employer](#) demands.

Not only does the law barely limit working time, the protection provided by the Privacy Act against intrusive data collection is more limited than is generally understood. While [other countries](#) specifically regulate privacy in the context of employment, New Zealand does not.

Instead, under the generic principles of the law, New Zealand employers may collect personal information [where necessary for a "lawful purpose"](#) connected with workers' functions or activities.

Employers don't have to make sure employees know and explicitly consent to their data being collected. They just have to take "reasonable steps" to make sure workers know why it's being collected and who will receive it.

Information can be used for purposes other than that for which it was originally collected, provided the individual consents. Information may also be disclosed to third parties on the same terms.

## Global standards for workers

All of this falls behind the emerging global standards for worker privacy protection. The European Union's General Data Protection Regulation ([GDPR](#)) does not allow employers to rely on employee "consent" to surveillance practices. This framework recognizes the [economic power](#) that employers have over workers.

The EU is also [looking to ban](#) the processing of certain sorts of personal data for "platform workers" (Uber drivers, for example), including a prohibition on collecting data while the worker is not working.

New South Wales and the Australian Capital Territory require active notice of filming and sound recording when workers are working at home, and do not permit passive covert surveillance without a court order. In [Portugal](#) the law expressly forbids permanent connection either through images or sounds.

The United States has begun consideration of the [Stop Spying Bosses Act](#), which would prohibit employers from collecting after-hours data. And [California](#) has put in place some specific regulation around workers rights regarding their workplace data.

New Zealand's weak penalties for interference with privacy stand in stark contrast to the penalties levied by the French Data Protection Agency. Amazon France was [recently fined €32 million](#) for breaches of the GDPR.

## Opportunity is knocking

New Zealand's government has a range of other employment law reforms on its agenda, including reform of occupational health and

safety law, reviewing access to personal grievances, and changing the legal definition of "employee."

But the right to disconnect does not appear to be a priority.

New Zealand can benefit from watching other countries as they respond to rapidly changing technologies. When the time is right, the government should implement rules giving workers a true right to disconnect and privacy outside the workplace.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: The right to disconnect from work—and employer surveillance—is growing globally. Why is NZ lagging? (2024, August 21) retrieved 21 August 2024 from <https://phys.org/news/2024-08-disconnect-employer-surveillance-globally-nz.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.