A-Z Guide

SURVEILLANCE

Contents

Overview

Modern technology provides employers with the opportunity to conduct surveillance of their employees in almost every place and activity in the workplace.

The decision whether or not to conduct any sort of surveillance needs to be weighed against considerations involving privacy and the implied term of mutual trust, confidence and good faith.

The Court of Appeal has determined that if, as the result of surveillance, personal information is obtained but it was unsolicited (not asked for) information, then that information is not collected within the meaning of the word “collect” as defined by the Privacy Act 2020.

The Privacy Commissioner continues to hold the view that, in spite of this decision by the Court of Appeal, surveillance does involve the collection of information, even when it is unsolicited, which may be personal information within the meaning of the Privacy Act 2020.

Introduction

Employers have always had the right to monitor employees in the workplace during working hours. The development of technology and the enactment of the Privacy Act 2020 have raised a number of issues in respect of this right.

While there is no legislated right to privacy in New Zealand, except for the right to be secure against unreasonable search and seizure under the New Zealand Bill of Rights Act 1990, there has been the view that a common law action for invasion of privacy is possible in this country. This is a gradually developing area of the law because of the recognised need to balance any right to privacy with the freedom of expression.

In the employment area, the legal limits of surveillance are under constant review; new technology and the innovations in its application demand an ongoing reappraisal of the potential of, and possible need for, surveillance.

In this guide surveillance, both covert and overt, is covered. Some types of surveillance are covered in greater detail in the following **A-Z Guides**:

- **Drug Testing**
- **Medical Examinations**
- **Pre-Employment Checks**

This **A-Z Guide** deals with the issues that arise out of surveillance under the Privacy Act 2020 and the Employment Relations Act 2000.

Definitions

Surveillance, which may or may not be directed at employees, can occur in many different ways. This list is not exhaustive.

Digital

- Cookies
- Global Positioning Satellite (GPS)
- Tracking software
- Web cams

Audio

- Audio recording
- Phone tapping
- Visual
- Security cameras
- Hidden cameras
- Closed Circuit Television (CCTV)
- Speed cameras

Physical

- Bag searches
- Vehicle searches
- Office and locker searches
- Drug testing
- Biological monitoring

Privacy Considerations

The purpose of the Privacy Act 2020 is to promote and protect individual privacy. It seeks to achieve this purpose by establishing principles about the collection, use, storage and disclosure of personal information about identifiable individuals. In all, there are 13 Information Privacy Principles. Not all of these Principles, or all of the conditions each Principle imposes, are discussed in respect of surveillance.

The Act does not just apply to employer organisations; it applies to most private and public organisations and agencies. However, for the purposes of this **A-Z Guide** the discussion refers to employers.

It is important to note that the provisions of the Privacy Act 2020 do not confer on any person any legal rights that are enforceable in a court of law; however, the entitlements conferred on an individual by Principle 6 insofar as it relates to the personal information held by a public sector agency, are legal rights, and are enforceable in any court of law.

It is also important to note is that the Privacy Act 2020 introduces a regime whereby the Commissioner must be notified of privacy breaches. A Notifiable Privacy Breach means a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals or is likely to do so.

Refer to the **A-Z Guides** on **Privacy and Audio Recordings** for supplementary information to this topic.

Principle 1

Principle 1 provides that personal information shall not be collected by any agency unless:

a. The information is collected for a lawful purpose connected with a function or activity of the agency.
b. The collection of the information is necessary for that purpose.

The Privacy Commissioner has held that a policy allowing employee bag searches for security purposes were for a lawful purpose connected with the employer's functions and activities. The function being to ensure the security of its property, its staff's property and staff safety. The Commissioner also found that the searches were necessary to achieve that function.

Principle 3

Principle 3 imposes a number of conditions on the collection of personal information, where it is collected from the individual concerned, that an employer must comply with.

The individual concerned is entitled to know that the information is being collected, and the purpose for which the information is being collected. The employer does not have to comply with this principle if it believes, on reasonable grounds, that:

- The individual concerned has authorised the collection
- The interests of the individual concerned will not be prejudiced by the collection
- Non-compliance is necessary to avoid prejudice to the maintenance of the law
- Compliance would prejudice the purposes of the collection
- Compliance is not reasonably practicable in the circumstances of the particular case
- The individual concerned will not be identifiable

Unsolicited information

The Court of Appeal, in *Harder v Proceedings Commissioner* [2000] 1 NZLR 80, held that information that is obtained by surveillance and that is unsolicited (not asked for, but voluntarily offered) is not "collected", even when it was recorded on tape, and that the information contained in the recorded conversation was therefore outside the scope of the Privacy Act 2020. It held that the way in which in fact the information was recorded did not change the unsolicited nature of the information.

This decision cannot be viewed as justifying or legitimising any covert surveillance; what it states is that in some circumstances, some information that is obtained but is not sought, may not fall within the scope of the Act.

The following example is entirely fictitious and designed to be illustrative only:

> *A fleet of ambulances are fitted with GPS systems. This enables the Emergency Service Command Centre to monitor the position of all ambulances within its region and with the use of visual display technology, see at a glance which ambulances are within a specified radius of any given location. Each GPS unit records information about the ambulance, including the identity of the driver, each time it is activated.*

While activated, the highly sophisticated GPS records information about:

- *The speeds the ambulance is driven at*
- *The fuel consumption*
- *Where it has travelled*
- *How many stops it makes and the time involved in those stops*
- *What electronic devices within the unit are used*
- *How many seats or stretchers are occupied at any time*
- *The payload of the ambulance at any time*
- *The temperature inside the ambulance at any time*

The information is recorded digitally onto a chip in the unit itself and digitally on a backup system in the command centre. This information is retained indefinitely and used for a range of things, including:

- *Analysing the demands made on the vehicles used as ambulances*
- *Assessing the efficiency and economy of each type of vehicle used as an ambulance*
- *Managing the fuel consumption of the fleet*
- *Compiling information about the demand on the fleet*
- *Compiling information about the use and efficiency of devices fitted in ambulances*
- *Monitoring the safety of the ambulances as places of work*
- *Assessing the efficacy of the service within the region*

As a result of the ability of the GPS systems to record so much, and certain, information, the Service records a lot of information about its employees who work in the ambulances. If it sorted the information it records, it could ascertain:

- *The weight of every employee*
- *The performance of every employee in respect of fuel consumption, speed, stopping times, availability*
- *The movement of each employee in respect of an ambulance at a specified time*
- *Limited information about each employee's activities while on duty*

This information is entirely unsolicited; under the findings of the Court of Appeal in *Harder*, none of this information is personal information within the scope of the Privacy Act 2020 because it is unsolicited and therefore not collected.

Hidden cameras in the workplace

It is the view of the Privacy Commissioner that covert video surveillance does fall within the scope of the Act; this view is contrary to the view of the Court of Appeal apparent in the *Harder* decision. The current difference in views could be settled at any time by either a change to the meaning of "collection" in the Act, or a review by the Court of Appeal of its earlier decision in another case.

The Privacy Commissioner continues to hold the view that video surveillance does involve the collection of personal information, because if it is being collected for a lawful purpose associated with the function or activity of the employer (Principle 1), it can be justified under Principle 3. The Commissioner believes that this statement is true whether or not the video surveillance is overt or covert.

In principle, the view of the Privacy Commissioner is applicable to all types of surveillance.

The discussion that follows in respect of the following Information Privacy Principles is based on the Commissioner's view.

Principle 4

Principle 4 prescribes the manner in which personal information must be collected. It states that an employer shall not collect personal information by:

- Unlawful means
- Means that are in the circumstances of the case either unfair or intrude to an unreasonable extent upon the personal affairs of the individual concerned

In the view of the Privacy Commissioner, employers who conduct any covert surveillance should:

- Clearly record the purpose of the surveillance
- Conduct the surveillance only during relevant time periods
- Restrict the surveillance to the least amount of time possible
- Ensure only information relevant to the reason for the surveillance is collected
- Unless there are extraordinary circumstances, do not conduct any surveillance at any times or in any areas where employees would expect complete privacy

If an employer conducted its surveillance, whether or not it was covert, within these limitations, then the surveillance should not (but may) be considered an interference with privacy if challenged.

It would be unlikely for the Human Rights Review Tribunal or Employment Relations Authority (the jurisdictions of these two institutions are not the same) to determine that a manner of collection of personal information was unlawful if it had been covered in sufficient detail in a written, and signed, employment agreement. In this instance, the purpose of the collection, the intended recipients, the intended use and disclosure, and the storage of the personal information should also be covered.

Principle 10

Principle 10 places limitations on the use of personal information. If your organisation conducts any surveillance to collect personal information in connection with one purpose, it should not use the information for any other purpose. However, an employer does not have to comply with this principle if it believes, on reasonable grounds, that:

- The use of the information is authorised by the individual concerned
- Non-compliance is necessary to avoid prejudice to the maintenance of the law
- Non-compliance is necessary to prevent or lessen a serious threat to either public health or safety or the life or health of the individual concerned or another person
- The purpose for which the information is used is directly related to the purpose in connection with which the information was obtained
- The individual concerned will not be identifiable

If your organisation conducts any surveillance and collects personal information in connection with one purpose and uses the information collected for another, it may constitute an interference with privacy under this Act.

In some instances, personal information obtained in connection with one purpose, may reveal information that may support an allegation of misconduct. The use of the information for disciplinary matters may, or may not, constitute a misuse of that information; the use of the information for disciplinary matters may fall into one of the exceptions contained in Principle 10.

The following example is entirely fictitious and designed to be illustrative only:

> *A first-aider working in an organisation asks all of the employees to advise him whether or not they have Hepatitis B so that the first-aider can protect himself, and any other person, from infection if any of the employees who do have Hepatitis B are injured and in need of first aid.*
>
> *Two employees confirm to the first-aider that they have Hepatitis B. The first-aider then tells the individuals concerned that they may not use the communal toilet facilities on the floors they work but must use the toilets on the ground floor which are for use by people in wheelchairs. Then he tells everyone else that the toilets on the ground floor are broken.*

This example shows a misuse of personal information, in respect of Principle 10, that may also constitute unlawful discrimination.

Employment Relations Considerations

Mutual obligation of trust and confidence and good faith

An employer may not engage in activities that are contrary to the implied term of fair dealing, trust, and confidence.
In *Auckland Shop Employees Union v Woolworths (NZ) Ltd* [1985] 2 NZLR 372, the Court of Appeal cited the following extract from an English case with approval:

In our view it is clearly established that there is implied in a contract of employment a term that the employers will not, without reasonable and proper cause, conduct themselves in a manner calculated or likely to destroy or seriously damage the relationship of confidence and trust between employer and employee.

In *Auckland Local Authority IUOW v Auckland Electrical Power Board* [1992] 1 ERNZ 87, the Employment Court echoed with:

It is now clear that there is implied in a contract of employment a term that the employer will not, without reasonable and proper cause, conduct itself in a manner calculated or likely to destroy or seriously damage the relationship of confidence and trust between employer and employee.

If an employer is going to conduct any sort of surveillance, whether or not the primary objective of that surveillance is to obtain personal information, and unless the employer has good reason connected with the purpose for the surveillance, the employer should be open and honest about that surveillance.

An employer may have policies dealing with such matters as:

- Security
- Standard handling procedures
- Drug testing
- Biological monitoring
- Internet, email, and computer usage
- Motor vehicle usage
- Customer service standards
- Stock control

Surveillance

In some circumstances, covert surveillance may be justified and may or may not be included in these policies; however, in most circumstances overt surveillance, with the full knowledge of it and appreciation for it by your employees, will be just as effective at providing the information sought by the surveillance as covert surveillance.

The Court of Appeal considered the duty of good faith in *Coutts Cars Limited v Baguley* [2001] ERNZ 660; and said:

> *We do not see that the new statutory obligation on employers and employees to deal with each other in good faith introduces any significantly different obligation to that the Courts have placed upon parties to employment contracts over recent years. Undoubtedly the duty to deal in good faith will have an impact in additional areas such as negotiations and collective environments, but in the area with which we are presently concerned we consider the law already required the observance of good faith.*

As well as impacting on any surveillance itself, these obligations impact on the use of information obtained by surveillance.

The Employment Tribunal found in *Pillay v Rentokil Ltd* [1992] 1 ERNZ 337, that an employee who had been the subject of secret surveillance by his employer, via the services of a private investigator, had been entitled to resign his employment over a breach of the implied term of confidence and trust.

The Court found that the surveillance itself was not a breach of the contract, but the employer's failure to attempt to put Mr Pillay's mind at rest about any aspect of the surveillance after his car and briefcase had, quite coincidentally, been tampered with; the employer's failure to provide, when sought, a full and frank explanation about the employer's actions in having him followed and watched; and the employer's failure to explain the depth of distrust and suspicion of him and to provide Mr Pillay with the opportunity to explain why that distrust was unfounded.

In *New Zealand Tramways Union (Wellington Branch) v Wellington City Transport Ltd t/a Stagecoach New Zealand* (Unreported) WC 36/02; 19 September 2002; Goddard CJ, the Employment Court found that the relevant employment contract prohibited the employer from using the evidence it had obtained from covert video surveillance in any disciplinary action against the employee bus driver. The contract contained strict timeframes related to the reporting of conduct that it considered warranted further investigation which had been overrun. It stated:

> *The video surveillance of suspected employees is not in itself objectionable. Nor is it particularly novel. There are so many cases in the books of its occurring that to give examples would be a waste of time. The sole question is whether the company has bound itself by contract not to use such surveillance, however sensible it may seem to do so...The [contractual] clause does not contemplate or specifically deal with video surveillance but it clearly contemplates that, whatever means is used to give rise to company concerns about employees' conduct, those concerns, if they are to be acted upon, are required to be notified within a very short time frame...*

These cases show that an employer who uses surveillance technology and captures information that could give rise to disciplinary proceedings against an employee, may not be justified in using that information for that purpose, when all the circumstances of the case are considered.

Conclusion

Whether any sort of surveillance is unlawful, or not, will depend on an examination of the particular circumstances in which it takes place.

Employers are obliged to consider the duty of confidence, trust, fair dealing, and good faith. This term of employment obliges employers and employees to reflect on what is fair and reasonable in the circumstances in determining what surveillance will achieve, how it should be conducted, and how the information that is obtained may be used.

Every decision to introduce surveillance has important implications that should be considered in light of the most current employment and privacy law. If you would like to discuss the option of surveillance for any reason, please contact AdviceLine on 0800 300 362.

Remember

- **Always call AdviceLine on 0800 300 362 to check you have the latest guide.**
- **Never hesitate to ask AdviceLine for help in interpreting and applying this guide to your situation.**
- **Use our AdviceLine employment advisors as a sounding board to test your views.**
- **Get one of our consultants to draft an agreement template that's tailor-made for your business.**

This guide is not comprehensive and should not be used as a substitute for professional advice.

Published: **December 2024**

EMA TERMS AND CONDITIONS FOR THE SALE AND USE OF TEMPLATES

1. The EMA designated as "Seller" herein agrees to sell and deliver to you, the party designated as “Buyer", this digital template subject to the terms and conditions set forth in these Terms and Conditions of Sale.

2. The Seller hereby warrants that the Templates are original, free from any claims or rights of any third party, and do not infringe on any copyright, patent, trademark, or any other intellectual property rights.

3. The Buyer acknowledges that the Templates purchased under this Agreement are for their exclusive use and shall not be distributed, sold, leased, or licensed to any third party without the prior written consent of the Seller. For the benefit of doubt, this includes the use of this material as input into an Artificial Intelligence (AI) engine which may then mean that the integrity of the product - and our material - is compromised.

4. The Seller reserves the right to modify the Templates, their features, and their pricing at any time without prior notice.

5. The Buyer agrees to comply with all applicable laws and regulations regarding the use of the Templates and acknowledges that the Seller shall not be held liable for any violations thereof.

6. The Buyer shall pay for the Templates in accordance with the payment terms set forth in this Agreement. Failure to make timely payment may result in termination of this Agreement and revocation of the Buyer's right to use the Templates.

7. The Templates are provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

8. The Templates are not a substitute for legal advice or are guaranteed to suit your particular circumstances. The Seller recommends that you carefully consider your particular organisations' unique expectations and practices and have the material confirmed by a legal practitioner as suitable for them.

9. This Agreement is governed by and construed in accordance with the laws of New Zealand in which the Seller is located. The purchase is also governed - where appropriate - by the general EMA terms and conditions as located on the EMA Website.