CCTV, videos and photos in health, aged care and retirement living and disability facilities – your rights and obligations

Presented by:

Alison Choy Flannigan
Partner
(02) 9390 8338
alison.choyflannigan@holmanwebb.com.au

4726927.1 19 October 2016

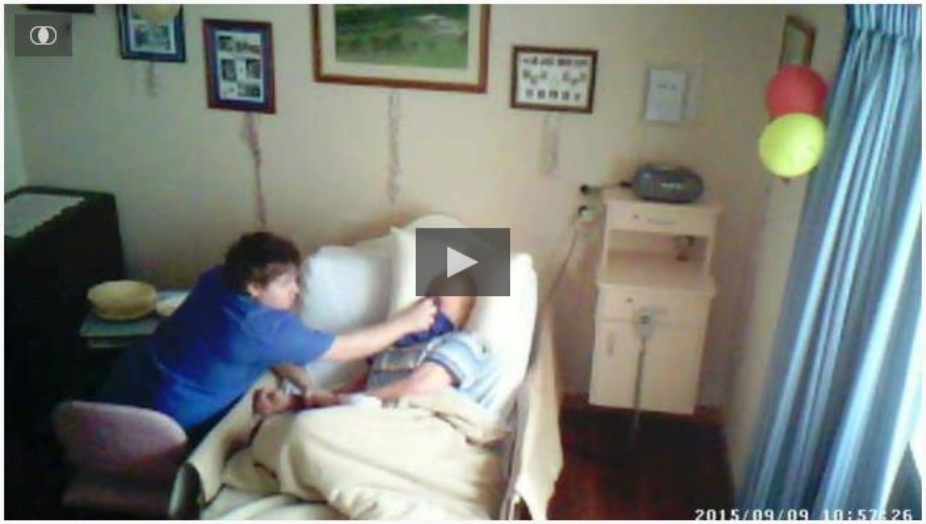
HOLMANWEBB LAWYERS

Introduction

Secret camera captures abuse of elderly man in nursing home including attempted 'suffocation'

7.30 By Andy Park

Updated 25 Jul 2016, 5:08pm



VIDEO: WARNING: THIS VIDEO CONTAINS DISTURBING FOOTAGE. Hidden camera footage shows nursing home staff member appearing to attempt to suffocate man (ABC News)

MAP: Adelaide 5000

A hidden camera in an Adelaide nursing home has captured footage of a staff member appearing to attempt to suffocate an 89-year-old man, prompting calls to legalise the installation of cameras in the private rooms of aged care facilities.

Source: http://www.abc.net.au/news/2016-07-25/secret-camera-captures-nursing-home-attempted-suffocation/7624770

HOLMANWEBB LAWYERS

Introduction

- **CCTV, videos & photos**
  - User Right's Principles
  - Privacy
  - Confidential information
  - Workplace surveillance
  - Surveillance devices legislation
  - Telecommunications and cybersecurity
  - Crimes against publishing indecent images
  - Alternative solutions – conditions of entry, trespass to property
  - Contract
  - Commentary on elder abuse

HOLMANWEBB LAWYERS

Care recipients' rights

- User Right's Principles 2014 (Cth) (residential care)
  - Each care recipient has rights, including:
    - To full and effective use of his or personal, civil, legal and consumer rights
    - To personal privacy
  - Each care recipient has responsibilities, including:
    - To respect the rights and needs of other people within the residential care service and to respect the needs of the residential care service community as a whole
    - To respect the rights of staff to work in an environment free from harassment

HOLMANWEBB LAWYERS

Privacy

- **To whom does the Commonwealth legislation apply?**
  - Commonwealth government agencies and private sector
  - Whilst there are is a small business operator exemption (annual turnover of $3 million or less for a financial year) – this does *not* apply to health information except in an employee record
  - The APPs extend to an act done or practice engaged in and outside Australia by an organisation that has an "Australian link"
    - Australian company
    - Someone who carries on business in Australia
    - Information is collected or held in Australia
    - Websites which offers goods and services in Australia
    - Australia is a country in a drop down menu on the entity's website
  - The Cth Privacy Act applies to **private sector not-for-profit** companies and incorporated associations and committee members of unincorporated associations (s98B)
  - NSW, Vic and ACT State/Territory privacy laws apply to State government agencies and private entities

Privacy

- **Privacy Legislation (private sector)**
  - *Privacy Act 1988 (Commonwealth) – penalties for serious and repeated offences are up to (5 times penalty for individuals – 80W) $1.8 million for businesses and 2000 penalty units ($360,000) for individuals*
  - *Privacy and Personal Information Protection Act 1988 (NSW)*
  - *Health Records and Information Privacy Act 2002 (NSW)*
  - *Information Privacy Act 2002 (Vic)*
  - *Health Records Act 2001 (Vic)*
  - *Health Records (Privacy and Access) Act 1997 (ACT)*
  - *My Health Records Act 2012 (Cth)*

  Note: The Australian Law Reform Commission Report "*For your Information: Australian Privacy Law and Practice*" (ALRC 108)

HOLMANWEBB LAWYERS

Privacy

- **Key concepts**
  - **“personal information”** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

HOLMANWEBB LAWYERS

Privacy - APPs

- **Australian Privacy Principles (Privacy Act)**
  - APP 1 Open and transparent management of personal information
  - APP 2 Anonymity and pseudonymity
  - APP 3 Collection of solicited personal information
  - APP 4 Dealing with unsolicited personal information
  - APP 5 Notification of the collection of personal information
  - APP 6 Use of disclosure of personal information
  - APP 7 Direct marketing
  - APP 8 Cross-border disclosure of personal information
  - APP 9 Adoption, use and disclosure of government related identifiers
  - APP 10 Quality of personal information
  - APP 11 Security of personal information
  - APP 12 Access to personal information
  - APP 13 Correction of personal information

Privacy – Open and transparent

- **Australian Privacy Principles (Privacy Act)**
  - **APP 1 - Open and transparent management of personal information**
  - You must have a clearly expressed privacy policy containing:
    - The kinds of personal information that you collect and hold
    - How you collect and hold personal information
    - The purposes for which you collect, hold and disclose personal information
    - How an individual may access their personal information held by you and seek to correct the information
    - How an individual may complain about a breach of the APPs and how you will deal with such a complaint
    - Whether or not you are likely to disclose personal information to overseas recipients and if so, the countries in which those recipients are located

Privacy – Collection, use and disclosure

- **Australian Privacy Principles (Privacy Act)**
  - **APPs 3, 4, 5 and 6 – Collection, use and disclosure**
  - You must only collect personal information if it is reasonably necessary for, or directly related to, one or more of your functions or activities
  - An organisation must only collect personal information by lawful and fair means
  - You must take steps as are reasonable to notify the individual of the collection
  - Personal information should only be used and disclosed for:
    - The primary purpose of collection
    - A secondary purpose which is related to the primary purpose and the individual would reasonably expect
    - With the consent of the individual
    - For another lawful purpose – As set out in the Act or otherwise

Privacy - Security

- **Australian Privacy Principles (Privacy Act)**
  - **APP 11 Security of personal information**
    - You must take such steps as are reasonable in the circumstances to protect the information:
      - from misuse, interference and loss; and
      - from unauthorised access, modification and disclosure
    - If you no longer need the personal information for any purposes which the information may be used or disclosed and the information is not contained in a Commonwealth record or required to be law or a court/tribunal order to be retained, you must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified

Confidentiality

- Confidential information

  It is a well-settled principle of law that where one party ('the confidant') acquires confidential information from or during his service with, or by virtue of his relationship with another ('the confider'), in circumstances importing a duty of confidence, the confidant is not ordinarily at liberty to divulge that information to a third party without the consent or against the wishes of the confider.

Attorney-General v Guardian Newspapers [No. 2] [1998] 2 WLR 805

Workplace surveillance

- *Workplace Surveillance Act 2005 (NSW)*

Under the Workplace Surveillance Act 2005 (NSW) an employer commits an offence if it engages in the surveillance of an employee without providing written notice at least 14 days before the surveillance commences: section 10.

- The notice must indicate:
  - the kind of surveillance to be carried out (camera, computer or tracking);
  - how the surveillance will be carried out;
  - when the surveillance will start;
  - whether the surveillance will be continuous or intermittent; and
  - whether the surveillance will be for a specified period or ongoing.

Workplace surveillance

- *Workplace Surveillance Act 2005 (NSW)*
- For camera surveillance of an employee, it is only permissible to use cameras for surveillance where:

  (a) the cameras are clearly visible in the place where the surveillance is taking place; and

  (b) there are signs notifying people that they may be under surveillance in that place which are clearly visible at the entrance to that place: section 11.
- Written notice by the provision within a workplace policy is sufficient
- Covert surveillance is permissible in very limited circumstances, for example, for the purpose of establishing whether or not an employee is involved in any unlawful activity while at work for the employer.
- Any employer (including a person contracting for services) conducting surveillance in breach of the Workplace Surveillance Act is liable to prosecution under the Workplace Surveillance Act.
- Surveillance may be undertaken by agreement: section 14.
- Penalties: up to 50 penalty units ($5,500) per breach

HOLMANWEBB LAWYERS

Surveillance devices legislation

- The *Surveillance Devices Act 2007 (NSW)* contains an offence of knowingly installing, using or maintaining an optical surveillance device on or within premises or a vehicle or on any other object, to record visually or observe the carrying on of an activity, if the installation, use or maintenance involves:
  - entry onto or into the premises or vehicle without the express or implied consent of the owner or occupier of the premises or vehicle, or
  - interference with the vehicle or other object without the express of implied consent of the person having lawful possession or lawful control of the vehicle of object: section 8.

Surveillance devices legislation

- This does not apply to the installation, use or maintenance of an optical surveillance device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation.
- This also does not apply if each principal party to the private activity consents expressly or impliedly to the installation, use or maintenance.
- An owner of a private residence is lawfully able to install and record from a CCTV device all activities within their home or vehicle.

Surveillance devices legislation

- There are also restrictions on the overhearing, recording, monitoring and listening of private conversations to which the person is not a party and the use of tracking devices without consent.
- Arguably, in relation to residential aged care facilities, both the resident and the Approved Provider “own” and/or “occupy” those premises and therefore, the consent of both is required. Certainly the Approved Provider occupies common and public areas. The consent of the resident should be obtained for their private room.
- The installation of a secret CCTV recording device in a room of a facility is an offence under the Surveillance Devices Act unless permitted under the Act and can incur penalties for a contravention of up to 5 year imprisonment and fines of $11,000 for individuals and $55,000 for corporations (see s.8).
- The person who installs a camera device is also liable to prosecution under the Surveillance Devices Act.

Telecommunications & cyber security

- The *Telecommunications (Interception and Access) Act 1979 (Cth)* regulates access to telecommunications content and data in Australia.
- The Act makes it an offence for a person to intercept or access private telecommunications without the knowledge of those involved in that communication.
- The *Criminal Code 1995 (Cth) (as was amended by the Cybercrime Act 2001 (Cth))*, division 477 regulate cybercrimes involving computers.

HOLMANWEBB LAWYERS

Crimes

- Criminal laws prohibit the taking or publishing indecent images, for example, the *Crimes Act 1900 (NSW), section 578C* and indecent filming without consent, *Crimes Act 1900 (NSW)*, sections 91K to 91M.

Alternative solutions

- Conditions of entry – Code of Conduct – requiring consent
- Trespass to property
- The common areas of an aged care facility or hospital may be "private property", to which the *Inclosed Lands Protection Act 1901 (NSW)* may apply
- The laws of trespass to property might apply to restrict access to non-residents if the policy/Code is infringed: *Halliday v Neville* (1984) 155 CLR 1, 8; *TCN Channel Nine Pty Ltd v Anning* (2002) 54 NSWLR 333
- There may be an action in nuisance where the activity unduly interferes with the use or enjoyment of land.
- The common law in Australia does not recognise an action such as trespass to person unless the act caused the victim physical harm or psychiatric illness.

HOLMANWEBB LAWYERS

Commentary on elder abuse

- Commentary on elder abuse and videotaping
  - Consider adopting technology as an enabler, for example, offering it as a service to residents and their families, such as life saving tracking devices (with consent)
  - Ensure that your complaints process are robust to avoid Elder Abuse and that residents and their families have a number of alternative people to resolve complaints, rather than resorting to covert video-taping

Social media

Don’t forget that your obligations extend to social media!

HOLMANWEBB LAWYERS

Risk management

- **Checklist**
  - Be mindful of your legal obligations
  - Ensure that you have a privacy policy and keep it up to date
  - Obtain the consent of residents, staff and visitors (preferably written) before video/photography or recording for business purposes
  - If you are monitoring or tracking residents, obtain consent
  - If you wish to engage in workforce surveillance, make sure that:
    - You provide adequate notice to staff
    - Ensure that the cameras are visible
    - That there are signs notifying people that they may be under surveillance in the entrance of the place being monitored
  - Only enter into premises to install, use or maintain surveillance equipment with the consent of the owner or occupier of the premises
  - If you wish to engage in convert monitoring, obtain a warrant from the court, which may be obtained by contacting the police

Risk management

- **Checklist**
  - Ensure that your policies, including employment policies are up to date
  - Adopt an IT policy to ensure staff know their obligations concerning your IT systems and computers, including security and unlawful access
  - Adopt a social media policy
  - Adopt a Code of conduct applicable to employees, residents and visitors
  - Provide training and education of your staff on your legal requirements
  - Consider adopting technology as an enabler, for example, offering it as a service to residents and their families, such as life saving tracking devices (with consent)
  - Ensure that your complaints process are robust to avoid Elder Abuse and that residents and their families have a number of alternative people to resolve complaints, rather than resorting to covert video-taping

Conclusion and questions

alison.choyflannigan@holmanwebb.com.au

HOLMANWEBB LAWYERS