

[Hidden Camera and Surveillance Laws Outside of the US](#)

Every country has its own privacy and surveillance laws. You will want to check your local laws regarding hidden cameras and other covert surveillance before installing your new equipment.

This article will give a brief overview of the applicable laws in a few of the home countries of our most frequent international visitors.

Canada

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) generally require a person's consent before video or audio recording them in a commercial or business situation.

The consent can either be expressly given (either orally or in writing) or it can be implied (such as clearly posting notice of the surveillance or advising callers of the recording of calls).

There are specific procedures outlined in PIPEDA which must be followed for a legal recording. If you plan to record calls or conversations with customers or clients, you should consult PIPEDA for its particulars.

PIPEDA also applies to workplace/employee surveillance situations. Pursuant to PIPEDA, an employer must usually advise its employees of any personal information it is collecting from them and why it is collecting the information.

This can include video surveillance, phone monitoring, keystroke recording and email review. An employer should only collect information necessary to the employer's stated purpose in collecting it.

An individual (as opposed to a business) can record conversations with the consent of one party to a conversation. If you are taking part in the conversation yourself, the consent can come from you.

With regard to video surveillance, Canada has passed a video voyeurism law, making it a crime to surreptitiously observe or record a person who has a reasonable expectation of privacy in the circumstances and is or is expected to be nude or partially nude or involved in sexual activity.

You can't legally place cameras in bathrooms or locker rooms. You can't legally set up a camera to record in your roommate's bedroom.

Keep in mind that, in addition to federal laws in Canada, your home province may also have privacy, surveillance and/or voyeurism laws which should be reviewed as well.

United Kingdom

Public surveillance cameras (also known as closed circuit TV - or CCTV) have been in heavy use in Britain for over thirty years. It has been suggested that there are more CCTV cameras in use in the U.K. than anywhere else in the world.

The Data Protection Act of 1998 (DPA) covers use of CCTV surveillance cameras in the U.K. It does not, however, apply to individuals who might use cameras for personal or household uses - just to businesses.

Individuals using such cameras must still make sure that they are not breaking British voyeurism laws by peeping into private spaces - these are similar to voyeurism laws in Canada and the U.S.

The Information Commissioner's Office has issued DPA guidelines for businesses using CCTV monitoring. There must be visible signs indicating that the cameras are in use on the premises and the cameras must be placed in spots which allow the best images but avoid recording people outside of the business premises.

The images recorded must be securely stored and not provided to anyone other than those responsible for the monitoring in the business and to law enforcement. Check with the ICO for any other requirements your business may have regarding video surveillance.

If cameras are used to monitor workers, they must not be installed anywhere deemed private, such as toilets or private offices.

The ICO suggests that workers should generally be told they are being surveilled but says that covert or hidden monitoring may be acceptable if it is an exceptional situation and the employer intends to involve law enforcement in the investigation.

In the U.K., you should also consider whether or not your planned surveillance complies with the Regulation of Investigatory Powers Act (RIPA), which covers the monitoring of electronic communication.

RIPA allows individuals to secretly record conversations for their own use. It only becomes illegal if the recording is made available to someone else.

If the person doing the recording plans to use the recorded conversation in court or plans to disclose the recording in any way, he will have to get consent from the person he is recording. There are a few exceptions to the basic RIPA requirements for businesses.

A business may record a conversation without anyone's consent to provide evidence of a business transaction, to prove regulatory compliance, to prevent or detect a crime, for national security or secure effective operation of a phone network. For any other purpose, the company must get the consent of the person being recorded.

Similar to the ICO's guidelines on the use of CCTV to monitor employees by video, RIPA guidelines suggest the electronic monitoring - email, telephone calls and such - of employees should also be overt and as non-intrusive as necessary to meet the goal of the surveillance.

For example, companies that routinely record phone calls in the regular course of business should provide their employees with a way to make necessary personal calls that are not recorded.

The Home Office and the ICO have issued helpful guidelines and checklists for businesses to use when considering video or other surveillance.

Other European Union Nations

Over the last ten years or so, the European Union (EU) has issued directives to its members regarding human rights and data protection. The result has been legislation in each country which complies with the basic directives. The British laws described above are good examples.

Without investigating the laws of each European country here, it is safe to say that they all have similar laws to the laws passed in Britain regarding monitoring and surveillance.

As always however, you should review the laws applicable in your own country and province and/or consult with a lawyer.

The newest surveillance technology can be a wonderful help in a difficult personal situation. It can also help you keep your business running smoothly and profitably. But it can also be misused and cause you some pretty serious legal headaches if you don't understand the applicable laws before using it.

So, if you've decided to purchase some fantastic new monitoring equipment, take a quick look at your surveillance and privacy laws before you press the "record" button - do your monitoring the right way and you just might save yourself a lot of trouble in the end!

About the Author

Sharon Macdonald is a retired teacher and high-tech security specialist. She is an expert in [video and audio surveillance systems](#) and techniques. See what she recommends to protect your family in her [blog](#)

Source: <http://www.onlineearnings.net>