Smart meter privacy and security

All electricity meters collect information about a customer's electricity use. Unlike the old mechanical meters, Smart meters are digital, two-way communication devices that can display and transmit more accurate and close to real-time usage information.

There are strict guidelines in place for the storage and use of this information, which apply to both electricity retailers and distributors.

How is your privacy managed?

The management of your information is protected under the [Federal Privacy Act 1988](#) (the Act) which regulates the handling of personal information.

More specifically, the Act includes National Privacy Principles (NPPs) that cover the collection, use, disclosure and storage of personal information.

The NPPs provide organisations with a set of obligations that direct them on how to handle your personal information responsibly. These obligations apply to organisations with an annual turnover of $3 million or more, and in some cases to organisations that have an annual turnover of less than $3 million.

What does this mean for you?

In relation to Smart Meter privacy and security, a number of NPPs provide safeguards for your personal information.

Firstly, [energy distributors](#) and [energy retailers](#) must obtain your consent before they can disclose your personal information to a third party. There are a few exceptions to this requirement and these are clearly outlined in the NPPs under '[use and disclosure](#)'. Secondly, distributors and retailers must ensure that the personal information they hold is both accurate and secure from any unauthorised use or access and are required to train their staff in data security procedures and conduct regular audits.

Thirdly, distributors and retailers must have a policy on how to manage your personal information and must make it available to you if you so require.

Finally, distributors and retailers must take reasonable steps to protect your information if their business operations require it to be processed offshore for the purpose for which it was collected.

Further safeguards for you

The Victorian Government does not ordinarily have any contact with customer Smart meter information. However should this happen for any reason (for example if a customer were to provide their data to the Government's online price comparator), the Government must comply with the Information Privacy Act 2000. Following the principles set out in the Act, the Government will protect your personal information, only use it for the reason it was collected and must only transfer it outside Victoria for the purpose for which it was collected. For more information, read the [Government's privacy policy](#).

The [Essential Services Commission (ESC)](#), the independent regulator of the retail energy industry in Victoria, is also committed to data security. The ESC outlines confidentiality obligations in a number of its regulatory instruments relating to energy distributors and retailers.

At a national level, confidentiality of your personal information and security of your smart meter installation and data is further protected under the [National Electricity Rules](#). These rules are set by the [Australian Energy Market Commission (AEMC)](#), which is an independent organisation that makes and amends the rules for Australia's energy markets and for the National Electricity Market, in particular.

How is your smart meter data used?

Smart meters are the property of the distribution businesses, which own and manage the poles and wires that deliver electricity to homes and businesses throughout the state. To find out who your distributor is visit the [Switch On website](#) or call 136 186.

Smart meters can record electricity use every 30 minutes. This data is transmitted intermittently to a local electricity distributor. Five distributors supply Victoria with electricity and are responsible for meter reading and sending retailers the data for billing.

The encrypted data is securely transmitted via relays and access points (some are mounted on electricity poles) and sent to the distributor's management system for reading via a telecommunications network such as the mobile telephone network. Distributors pass the data on to electricity retailers for billing purposes.

Energy retailers buy the electricity from generators and sell it to you. Just as different shops have different deals on the same goods, so too do electricity retailers. To find an energy retail company visit the [Switch On website](#).

Electricity retailers sell electricity and bill customers. They need access to a customer's metering data for billing purposes. Retailers also pay distributors to transport the electricity

to their customer's premises. They work with the local distributor to have electricity delivered to customers through the wires in the street. The primary relationship between a customer and the electricity network is managed by the retailer.

Security of smart meter technology within your home

Smart meters are equipped with security features in order to prevent unauthorised access. They are tamper proof and attempts to tamper with a Smart meter would be remotely detected by your distributor who would contact you in the unlikely event that this were to occur.

The Smart meter is password protected and the wireless link between the meter, distributor and home area network (HAN) is encrypted and cannot be disabled. As additional security, the encrypted wireless link between the meter and the distributor does not use the internet.

When using your energy retailer's [web portal](#) to access and track your energy consumption, you can be confident of the security systems in place to protect your data.

Electricity companies prevent access to metering data by third parties by using firewalls and data encryption. Your distributor or retailer is also required to store personal information in a way that reasonably protects it from misuse and loss and from unauthorised access, modification or disclosure. You must give your consent before your Smart meter data can be provided to anyone else. Furthermore, if your personal data is required by someone else, your retailer or distributor must ensure that this 'third party' complies with the Privacy Act.

With the emergence of [in-home displays (IHDs)](#), which provide real-time information on your energy consumption within the home, the security of your data is still assured. IHDs are securely bound to the meter so that information can only flow to that specific device, so your data remains subject to all the protections outlined above.

For more information

If you require further information on Smart meter privacy and data security, contact your electricity distributor or retailer. You can also view their privacy policy on their website.

Further information on privacy can be found on the [Your Choice website](#), which provides a fact sheet on Smart meters and your privacy.

Privacy Impact Assessment Report

An independent investigation into privacy issues around Smart meters conducted by Lockstep Consulting in August 2011 found no unauthorised disclosures from the collection of personal information associated with the implementation of the Smart meter program.

The Lockstep report found that:

- privacy controls are strong and metering data is suitably protected;
- the security of Smart meters is well designed – all wireless links are encrypted and this cannot be disabled, and there are also strong security governance practices to prevent access to metering data by third parties without consumer consent;
- the industry has adopted good information security standards and practice; and
- in light of the extra data that will be generated as new applications become available, the study made recommendations about ensuring future compliance with the privacy regime.

smartmeters