International study finds privacy shortfalls in Internet of Things devices

28 September 2016

More than half of Internet of Things devices don't properly tell customers how their personal information is being used, an international study has found.

The study, by 26 data protection regulators around the world, including the NZ Office of the Privacy Commissioner, looked at a variety of devices and considered how well companies building these devices communicated privacy matters to their customers. The study included smart electricity meters, internet-connected thermostats and watches that monitor health.

The report showed:

- 60 per cent of devices failed to adequately explain to customers how their personal information was **collected**, **used** and **disclosed**;
- 68 per cent failed to properly explain how information was **stored**;
- 72 per cent failed to explain how customers could **delete** their information off the device;
- 38 per cent failed to **include easily identifiable contact details** if customers had privacy concerns.

The report also raised concerns about medical devices that sent information via unencrypted email.

The data protection authorities looked at more than 300 devices. Authorities will now consider action against any devices or services thought to have been breaking data protection laws.

The work was coordinated by the Global Privacy Enforcement Network, and follows previous reports on online services for children, website privacy policies and mobile phone apps.

New Zealand's Privacy Commissioner John Edwards said "This study has shown that there's a significant amount of work to be done to protect privacy in the Internet of Things space. As with many quickly-developing technologies, there is a tendency to cut corners in a rush to get a product to market. The GPEN Sweep indicates that IoT providers would do themselves a favour by reviewing their privacy practice and making sure they are compliant with the Privacy Act."

ENDS

For further information, contact Sam Grover 021 959 050

Note:

Results were submitted by the following agencies:

Albania	*Information and Data Protection Commissioner*
Australia	*Office of the Australian Information Commissioner*
Australia, Victoria	*Office of the Commissioner for Privacy and Data Protection(CPDP)*
Canada	*Office of the Privacy Commissioner of Canada*
Canada, Alberta	*Office of the Information and Privacy Commissioner of Alberta*
Canada, British Columbia	*Office of the Information and Privacy Commissioner for British Columbia*
Canada, Nova Scotia	*Office of the Information and Privacy Commissioner for Nova Scotia*
Canada, Ontario	*Office of the Information & Privacy Commissioner, Ontario, Canada*
China, Hong Kong	*Office of the Privacy Commissioner for Personal Data, Hong Kong*
Colombia	*Superintendence of Industry and Commerce of Colombia*
Estonia	*Estonian Data Protection Inspectorate*
France	*Commission Nationale de l'Informatique et des Libertés*
Germany, Baden-Württemberg	*State Commissioner for Data Protection Baden-Württemberg*
Germany, Bavaria	*Data Protection Supervisory Authority of Bavaria*
Germany, Hessen	*Data Protection Commissioner of Hessen*
Gibraltar	*Gibraltar Regulatory Authority*
Ireland	*Office of the Data Protection Commissioner*
Israel	*Israeli Law, Information and Technology Authority*
Italy	*Garante per la protezione dei dati personali (Italian Data Protection Authority)*
Mexico	*Federal Institute for Access to Information and Data Protection*
New Zealand	*Office of the Privacy Commissioner*
Norway	*Norwegian Data Protection Authority*
Singapore	*Personal Data Protection Commission*
United Kingdom	*Information Commissioner's Office*
USA	*Federal Trade Commission*