Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

10 February 2015

Dear Sir/Madam (Data Protection contact at camera manufacturer),

The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The ICO has a wide range of powers to help us to regulate the Data Protection Act 1998 and Freedom of Information Act 2000. The powers, which are not mutually exclusive, can be used in conjunction where justified and enable us to:

- provide practical **advice** to organisations on how they should handle data protection matters;
- issue **undertakings** committing an organisation to a particular course of action in order to improve its compliance;
- serve **enforcement notices** where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct **consensual assessments** (audits) to check organisations are complying;
- serve **assessment notices** to conduct compulsory audits to assess whether organisations processing of personal data follows good practice (data protection only);
- issue **monetary penalty notices** requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010 or serious breaches of the Privacy and Electronic Communications Regulations occurring after 26 May 2011;
- **prosecute** those who commit criminal offences under the Act.

The ICO is committed to improving the public's and industry awareness in relation to privacy concerns, particularly those associated with high risk to individuals. One of our strategies in enforcing the regulations is to improve compliance of organisations, through prevention and education.

Quite often some of the privacy issues that we investigate have an international dimension as it has or may affect citizens in many countries. The ICO is a core member of the Global Privacy Enforcement Network and this enables us to coordinate our regulatory activities with other Data Protection Authorities across the world to address major international privacy issues.

I am writing to you to highlight our concern regarding the insecurity of devices accessible over the internet such as IP Cameras, and to ask for your assistance in helping us to reduce the risk to individuals.

As you may be aware, recent months have seen widespread international press and media coverage of a website using the name "Insecam". Until recently, this website was streaming live video footage from internet connected cameras (IP cameras) in residential and commercial premises around the world, providing access to the private lives of numerous individuals. The cameras featuring on this website were unsecure, in the sense that their owners had failed to change the manufacturer's default password settings. These default settings are freely available online, exposing unsecured cameras to being viewed over the internet without the owner's knowledge, which is obviously concerning.

The types of commercial premises that featured on Insecam included offices, children's nurseries, pubs, garages, convenience stores warehouses, factories and storerooms. These feeds often showed employees and customers, and in the case of nurseries, young children.

Footage of domestic premises included internal and external views of homes, including driveways, gardens, garages, living rooms, bedrooms and kitchens. In the majority of cases, cameras appeared to be being used for the purposes of security. However in other instances, the presence of individuals within the footage suggested some cameras were being used for care purposes. They often featured vulnerable elderly people, children and pets, via cameras pointed at cots, beds and armchairs.

At one stage, Insecam was streaming over 73,000 camera feeds from numerous countries. Alongside the live video footage, the website also

informed viewers of each camera's manufacturer, model, and approximate geographical location. As you will appreciate, this was a major breach of privacy and data protection rights and was extremely concerning for us and many other global Data Protection Authorities ("DPAs") around the world.

We worked closely with other DPA's and sent a joint letter (https://ico.org.uk/media/about-the-ico/documents/1042566/letter-to-the-operators-of-insecam.pdf) to Insecam, and the website is seemingly no longer active. However, for as long as cameras remain configured in this way, the risk to privacy remains.

As a manufacturer of IP cameras, we are contacting you to ask for your assistance in protecting the privacy of individuals by implementing a simple Privacy-by-Design solution whereby the camera users must secure access to the camera before it can be operated.

Our investigation established that the camera users were not aware of the risk associated with not changing the default settings of their devices, and the dangers associated with not doing so. We believe that the relatively simple solution of designing and manufacturing devices that cannot be operated unless the owner or user has first set a secure access code. This would prevent unauthorised access. This can be achieved in a number of different ways including forcing customers to choose a new password during first use or to consider an alternative authentication method.

We would also encourage you to provide increased guidance to customers about ensuring the security of their IP cameras, for example, by advising *how* to change their passwords and *why* they should do this in addition to explaining which the correct set-up process so that customers can easily choose which features they wish to use or access over the internet. This could potentially take the form of increased instructions provided upon purchase of the camera itself, and clear, easy to find guidance on your website.

You will undoubtedly understand the importance and severity of the situation, as well as the potential detriment of such severe privacy breaches, and we hope that you will share our concerns and put in place these changes to help improve the privacy and security of your customers.

Yours sincerely

Original signed by

Stephen Eckersley
Head of Enforcement
Information Commissioner's Office

cc. Brent Homan
Director General, PIPEDA Investigations
Office of the Privacy Commissioner of Canada