

Press Release

11 November 2010

New laws that raise privacy issues should undergo further scrutiny, says Information Commissioner

New laws that impact on privacy should undergo post-legislative scrutiny, Information Commissioner, Christopher Graham, said today in an update report to Parliament on the state of surveillance.

The Commissioner recommends that there should be a legal requirement to make sure all new laws that engage significant privacy concerns undergo post-legislative scrutiny to ensure they are being implemented and used as intended by Parliament. The report also makes the case for the use of 'sunset clauses' where legislation poses a high privacy risk.

[The report](#), presented to the Home Affairs Select Committee today, also makes a number of recommendations for the private sector, particularly that the privacy implications of new technologies are considered before they are launched rather than being an afterthought. Other recommendations include the use of robust privacy safeguards as well as the more wide-spread adoption of privacy enhancing technologies. The report was requested by the Home Affairs Committee as one the recommendations arising from its inquiry into the surveillance society.

The report includes research findings by the Surveillance Studies Network, a group of academic experts in this field. This gauges how far

privacy safeguards have kept pace with developments in surveillance and concludes that more still needs to be done.

Information Commissioner, Christopher Graham, said:

“Many of the new laws that come into force every year in the UK have implications for privacy at their heart. My concern is that after they are enacted there is no one looking back to see whether they are being used as intended, or whether the new powers were indeed justified in practice. One example of this is the use of covert CCTV surveillance by local councils to monitor parents in school catchment area disputes under powers designed to assist in crime prevention and detection.

“The report I’ve presented to Parliament today clearly makes the case for government departments to build post-legislative scrutiny into their work as a key way of ensuring the successful delivery of the new transparency and privacy agenda.”

ENDS

If you need more information, please contact the ICO press office on 0303 123 9070 or visit the website at: www.ico.gov.uk

Notes to Editors

1. The report is available on the ICO website here:
http://www.ico.gov.uk/~media/documents/library/Corporate/Research_and_reports/surveillance_report_for_home_select_committee.ashx
2. The Information Commissioner’s Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
3. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.
4. For more information about the Information Commissioner’s Office, subscribe to our e-newsletter at www.ico.gov.uk. Alternatively, you can find us on Twitter at www.twitter.com/ICOnews

5. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
 - Fairly and lawfully processed
 - Processed for limited purposes
 - Adequate, relevant and not excessive
 - Accurate and up to date
 - Not kept for longer than is necessary
 - Processed in line with your rights
 - Secure
 - Not transferred to other countries without adequate protection

6. The Data Protection Act (1998) does not cover the acts of interception of communications or 'hacking' of personal information. The interception of communications falls under the Regulation of Investigatory Powers Act (2000) which is regulated by the Interception of Communications Commissioner.

7. The ICO has legal powers to ensure that organisations comply with the requirements of the Data Protection Act. In using its regulatory powers, the ICO considers the nature and severity of the breach which has occurred. Dependent on circumstances, the powers the ICO has at its disposal include:
 - serving information notices requiring organisations to provide the ICO with specified information within a certain time period;
 - serving enforcement notices requiring organisations to take specified steps in order to ensure they comply with the law;
 - issuing monetary penalties of up to £500,000 for serious breaches of the Data Protection Act;
 - conducting audits to assess whether organisations are processing personal data in accordance with good practice;
 - reporting to Parliament on data protection issues of concern;
 - prosecuting those who commit criminal offences under the Act. The ICO prosecutes individuals and organisations for specific breaches of the Act such as the illegal trading of personal data and non-notification.