ICO response to the Development of Electronic Monitoring in Scotland

24 December 2013
About the ICO

The ICO’s mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The ICO is the UK’s independent public authority set up to uphold information rights. We do this by promoting good practice, ruling on complaints, providing information to individuals and organisations and taking appropriate action where the law is broken.

The ICO enforces and oversees the Data Protection Act 1998 and the Privacy and Electronic Communication Regulations 2003, as well as the UK Freedom of Information Act 2000 and the UK Environmental Information Regulations 2003, both of which apply to reserved matters in Scotland.
The Information Commissioner’s Office ("the ICO") welcomes the opportunity to respond to the Scottish Government’s consultation on the future of the electronic monitoring service in Scotland.

The Data Protection Act 1998 ("the DPA") regulates the processing by organisations of data relating to identifiable, living individuals. The DPA defines personal data which is more sensitive to include “data consisting of information as to…the sentence of any court”. As such, we are keen to ensure that the future direction of electronic monitoring is developed in accordance with the DPA.

As the regulator of the DPA, our response will be limited to commenting on the proper processing of personal data in relation to a sentence which includes electronic monitoring rather than the advantages or disadvantages of any particular system.
Global Positioning System (GPS) monitoring

The third Data Protection Principle of the DPA states that personal information gathered by an organisation must be relevant, adequate and not excessive. GPS monitoring of offenders should only be undertaken if it is strictly necessary to know where they are at any given time. If the current radio frequency (RF) equipment is sufficient to fulfil the monitoring requirements of the sentence, then that is what should be used. If future electronic tags contain both GPS and RF monitoring devices, it must be possible to disable the GPS equipment for an offender who can be adequately monitored through RF alone. Further, the equipment should be able to be disabled so that offenders are not being monitored during periods when they are not restricted to a curfew. There will need to be a detailed retention and disposal policy in place in order to ensure that the personal data processed is done so in compliance with the DPA. We welcome that a Privacy Impact Assessment will be undertaken and concerns such as these will need to be addressed within that.

The fourth Data Protection Principle requires personal data to be accurate and, where appropriate, up to date. It would be of concern if, as the consultation document suggests, a GPS signal can ‘drift’ and misrepresent the position of the individual through no fault of their own when they are stationary. Procedures would need to be put in place to ensure that decisions are not made in respect of that person based on information that may be inaccurate.

The potential for web-based monitoring, and remote access to that monitoring, must be secure to comply with the seventh Data Protection Principle and prevent it from being inappropriately accessed or disclosed. Any access should be role based and it will be important to ensure that adequate permissions are granted that restrict relevant staff to only having the information they need about the offenders they are responsible for monitoring and not others. A clear and robust remote working policy would need to be implemented in order to ensure that there is appropriate security in place. Staff would need to receive adequate training in how to use the system and this training should cover appropriate use of information and the fact that unauthorised disclosures would be a criminal offence under Section 55 of the DPA.

For the purposes of the DPA, the organisation that sets the parameters within which a particular offender is to be monitored (such as a court or the Parole Board) will be the data controller and therefore responsible for the personal data held by them and any company processing personal data on their behalf. This will include the company managing the monitoring service. In order to comply with the Seventh Data Protection Principle, each data controller will need to prepare a written contract with the data processor that requires the data processor to act only in accordance with the instructions of the data controller.
controller and also requires the data processor to take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of personal data and the accidental loss or destruction of, or damage to, the personal data.

The consultation document considers that the police could be provided with information from the monitoring service in order to rule certain suspects out of their enquiries. This would have to be in response to specific allegations and there would have to be good reason to believe that the specific suspects were likely to have been involved in the crime. In order for this information to be shared in appropriate circumstances, the relevant data controller and the police should enter into a data-sharing agreement which specifies, among other matters, the legal basis for sharing the information held by monitoring service and the purposes for which the information can be used. A similar agreement would be required if information is to be shared with the agencies involved in managing the behaviour of a sex offender. The ICO has published a Data Sharing Code of Practice\(^1\) which should be consulted in order to draft an agreement.

The processing of personal data in any particular case must be the most appropriate way of fulfilling the purpose for which that data has been collected and used. If other methods exist that do not require any or as much personal data to be processed, then that should be pursued instead. Processing in the context of electronic monitoring of offenders should be proportionate to the nature of the crime and punishment and targeted based on risk posed to the breaching of the sentence imposed. Therefore we would not consider that an untargeted use of GPS would meet the obligations of the DPA.

\(^1\)www.ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications#sharing
Further issues

Privacy Impact Assessment

The ICO welcomes the acknowledgement of data protection and human rights issues throughout the consultation paper. In particular we are pleased that the Scottish Government intends to conduct a Privacy Impact Assessment (PIA) on any proposals arising from this consultation. We would welcome the opportunity to work with the Scottish Government to ensure that the PIA is rigorous and supports a policy proposal that balances the rights of individuals to privacy with the need to ensure appropriate punishment and rehabilitation for offenders.

We have recently completed a consultation to replace our PIA handbook with a Code of Practice. We consulted on a draft Code of Practice earlier this year, which can be found on our website at www.ico.org.uk/about_us/consultations/closed_consultations. We intend to publish the final Code of Practice by the end of February 2014 but we do not expect it to differ from the consultation draft in any significant aspect. The Scottish Government should consider using the process contained in the draft Code of Practice to develop its PIA for future electronic monitoring proposals.

Research and analysis of offender journeys

We note from the consultation that the Scottish Government intends to gather more information about an individual’s interactions with the criminal justice system in order to provide more robust data about the relationship between electronic monitoring and reoffending.

Any research that is commissioned would have to comply with Section 33 of the DPA and not be used to support any decisions taken to the particular individuals whose data has contributed to the research. The research should also be conducted according to the Scottish Government’s Guiding Principles for Data Linkage and using the ICO’s anonymisation code of practice where applicable.

2 www.scotland.gov.uk/privacyprinciples
3 www.ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications#anon
Development of Electronic Monitoring in Scotland

For further information on this submission, please contact Dr Ken Macdonald, Assistant Commissioner (Scotland & Northern Ireland) on 0131 244 9001 or email scotland@ico.org.uk.

If you would like to contact us please call 0131 244 9001 or e-mail Scotland@ico.org.uk.

www.ico.org.uk

Information Commissioner’s Office
45 Melville Street
Edinburgh  EH3 7HL