Upholding information rights

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

Information Commissioner's Office response to the Cabinet Office's consultation on the proposal to amend the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), to enable the future implementation of a national public emergency alert system

The Information Commissioner has responsibility for promoting and enforcing the Data Protection Act 1998 (DPA), the Freedom of Information Act 2000, the Environmental Information Regulations and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken.

The Information Commissioner welcomes the opportunity to respond to this consultation document given his role to help ensure compliance with the DPA and PECR. He also welcomes the constructive engagement his office has had with the Civil Contingencies Secretariat during the development of the proposed emergency alert system.

The Commissioner fully recognises the importance of having an effective emergency alerting system in operation in the UK. He understands the pressing public policy need for a national alert system based on mobile phones but believes there is a balance to be found between notifying individuals of incidents or risks that they may be exposed to, and intruding on their personal space through unwarranted unsolicited text messages. Any approach to address this issue should be proportionate to the aim to be achieved, whilst acknowledging and respecting individuals' privacy rights and it should be supported by compensatory safeguards. We would welcome the opportunity to continue to work with the Cabinet Office, the mobile network operators (MNOs) and emergency responders as they move towards implementation of this potentially life-saving system.

The Information Commissioner has focused his response on the questions and issues which raise data protection and PECR considerations. We have not responded to those questions that fall outside of our regulatory remit.

1. Do you agree with the Government's proposal to amend PECR to allow MNOs to process communications data for the purpose of a Location-Based SMS alert system?

We recognise the importance of having an effective and adaptable emergency alerting system and in principle we would support a specific, targeted amendment to PECR, based on a defined and pressing public safety need. We welcome the proposal that the amendment will allow network operators to send messages on behalf of emergency responders in areas at risk but not for any other purpose and that information about the handsets and their location will be retained by the operators and not passed to the authorities. We also note in particular that public security is one of the areas explicitly excluded from the scope of Directive 2002/58/EC (article 1(3)). This support would be subject to the wording of any provision not being too broad and the trigger for the alerts not being too low.

The personal and ubiquitous nature of mobile phones is such that any widespread establishment contact via those devices has the potential to be intrusive. It is our experience that many members of the public find unexpected contact to their mobile phones intrusive and unwelcome. There is a balance to be found between informing individuals to enable them to safeguard themselves and their property against significant potential harm and respecting their privacy. The potential severity of the harm in any incident is fundamental in assessing the reasonableness and proportionality of contacting individuals via their personal mobile phones. We welcome the proposal that the system will be used in the event of serious emergencies and that the consultation document outlines five major types of incident that are likely to be used, and that alert authorisers will be at an appropriate level of seniority (for example Gold Commander for the police).

The lower the bar is set for triggering use of the SMS alerts, the more difficult it becomes to justify the use of the mobile alerting system from the perspective of the DPA. On this basis, we support the types of incidents outlined in the document and agree they would set an appropriate level of severity for potential harm or damage to trigger an alert. This would act as a built-in safeguard to prevent casual or overly frequent use where there might be viable and effective alternatives.

You also asked for views on the option of doing nothing. As you are aware, we consider that an emergency alert system based on cell broadcasts would be the

more privacy-friendly option and would not require amendments to PECR. However, we understand there are significant obstacles to the use of such a system, particularly the difficulties around the configuration of mobile handsets in the UK. Since the government proposes to proceed with the SMS location-based system, we agree that an amendment to PECR would be necessary to provide regulatory certainty for mobile network operators, as well as members of the public and other interested parties.

2. Are there any costs or benefits associated with any of these options that you feel need to be considered before any final decision is taken?

N/a

3. Do you consider that the regulations pertaining to location data would also require amendment?

The PECR rules on location data are strict. In broad terms, an MNO can only process location data if it is 'traffic data'; if the data is anonymous in its hands; if it has consent of the user; or if it is for emergency calls (where the user/subscriber initiates the call).

The Cabinet Office's preferred emergency alert system is one based on MNOs using location based SMS in which they can identify a geo fence around the affected area and target the users' devices in that particular location. This geographical focus enables the police or government to ask MNOs to send alerts telling users what to do in that particular area eg "close windows and stay indoors". In our view the MNOs would be processing location data in order to use the exact location of the user's device to target messages at individuals in what could potentially be a relatively small area. In this situation the location data is not simply being used to route a message. The MNOs are using the location data to decide which users are to receive what message based on their location. It seems likely therefore that their processing is wider than just managing 'traffic' data and we do not consider therefore that the MNOs can rely on Reg 14(1) in relation to the processing of this location data.

We also do not consider that all MNOs can rely on Regulation 14(2)(a) which states that location data can be processed if the data is anonymous. In the hands of most of the MNOs those users being targeted within a specific location would be capable of being identified because the MNO will hold the mobile telephone number and details of the account holder. We are also aware of some

MNOs' views that they do not have the processes and systems to enable them to anonymise the data and consider it would be counter-productive for them to do so. Additionally, we understand the MNO will need to keep a log as to which users it has contacted for this purpose in order to send any follow up messages about the incident.

Since MNOs cannot rely on the data being either anonymous or traffic data, they are only left with the option of consent. Regulation 14(2)(b) states that location data can be processed if the user has provided their consent to use it for a value added service and the processing is necessary for that purpose. We accept your concerns that there would be significant practical difficulties and disadvantages in trying to establish a national emergency alert system based on consent.

Based on our understanding of the proposals, MNOs do not appear to be able to meet the requirements of Regulation 14 and therefore it is likely that the scheme as currently designed would breach PECR unless there was an amendment to the regulations. If the processing of location data without consent is unlawful under PECR, the MNOs would also not be able to comply with the first data protection principle of the Data Protection Act.

We agree with the findings in the consultation document that alert messages should be geographically targeted so that they do not trouble people unnecessarily. We consider that targeting alert messages on users at risk in specific locations represents a more privacy friendly and proportionate approach than issuing large scale SMS alerts. There are advantages to amending the regulations to ensure that the alert system can be highly targeted. Adopting a less targeted approach would be far less effective and would intrude on the privacy of many more people. Citizens' trust in the system is likely to be undermined if people keep receiving unwarranted, unsolicited text messages concerning incidents over a wide area.

4. Do you consider that these changes would have any other impact on you or your organisation?

Amending PECR should provide greater legal certainty that the law allows the implementation of a national public emergency alert system. This should result in fewer complaints and queries to our office, providing there is a good communication plan in operation so that emergency alerts are within people's expectations.

5. Do you have any other comments about the proposed changes?

You have undertaken aspects of a privacy impact assessment as you have developed your legislative proposals, including consultation with a wide range of organisations and the public. As you move towards the implementation phase, we recommend that you undertake a PIA to ensure that the proposal is proportionate in what it seeks to achieve and that it meets the test of being "necessary" for the development of an effective emergency alert system. A PIA should also help you to explore the privacy risks involved and to identify and build in appropriate procedural safeguards into the system from the outset.

Transparency about the alert system will be very important and we note that the Government has undertaken to ensure there is an appropriate communications strategy in place prior to any system launch.

We have also provided advice on our general concerns around the potential for messages from this system to be spoofed. A message sent purporting to be an alert could cause significant disruption and loss of trust in the system and consideration needs to be given to ways to prevent this occurring. Again this issue should be considered as part of any PIA and could include consideration of further measures to deter or enforce against individuals sending out spoof messages.

A further risk would be the potential for a message to be transmitted fraudulently – that is, without being appropriately authorised. MNOs would need some level of assurance that the received request to transmit a message is genuine – as well as the suggested IP address authentication, it might be worth considering having two-stage input processes before the instruction to send a message is issued, forcing strong passwords for login access, two factor authentication and device restriction.

Retention of data

We welcome the proposed safeguard that MNOs will retain the data and that no details of the handsets that have been sent messages or their locations will be passed to the authorities. We also note that reports on volumes of messages sent, time taken etc would not include information on which users have been sent the messages and no personal data would be provided to the authorities.

The Data Protection Act does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that personal data processed

for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. We recognise that data may need to be retained for a little longer than just to send out the alerts or any follow up or stand-down messages. A relatively short, additional retention period may be necessary for the purposes of assessing volumes of alerts, time taken to send them, to analyse coverage and to deal with any follow-up enquires from the public. If an organisation keeps personal data to comply with a legal requirement or professional guideline, it will not be considered to have kept the information for longer than necessary.

January 2015