

## **Chapter seven: enforcement and sanctions, technical standards, and exemptions for national security and law enforcement purposes**

### **The requirements of the Directive**

- Articles 14 and 15
- Recitals 11 and 46 – 47

Article 14 provides that any technical standards on networks or terminal equipment in support of the requirements of the Directive must be introduced in accordance with EU rules, including rules on the free circulation of equipment, on notification of draft technical standards, and terminal equipment standards.

Article 15 allows Member States to make exemptions to the privacy rules set out in the Directive for national security and law enforcement purposes. The Directive now specifies that Member States may adopt legislative measures providing for the retention of data for a limited period for national security and law enforcement purposes. Recital 11 sets out the parameters for Member States' legislation, which must comply with European Convention for the Protection of Human Rights and Fundamental Freedoms, and must be appropriate and strictly proportionate.

Article 15 and recital 47 require Member States to apply the provisions of Chapter III on judicial remedies, liability and sanctions of the Data Protection Directive to national implementation of the Directive, and to ensure that there are judicial remedies and penalties for failure to comply with the Directive.

### **Approach to the Privacy Regulations**

- Regulation 24 (contracts)
- Regulations 25 and 26 (national security and legal requirements)
- Regulations 27, 28 and 29 (enforcement and compensation)

### **Technical standards**

Like the existing Telecommunications (Data Protection and Privacy) Regulations (the TDPP Regulations), the draft Privacy Regulations do not provide for technical standards.

### **Exemptions for national security and law enforcement purposes**

In the UK, the Regulation of Investigatory Powers Act 2000 (RIPA) provides for the terms on which national security and law enforcement agencies may intercept communications and access traffic data (such as a phone operator's records of the time, duration and destination of calls). The Home Office is currently consulting on proposals for secondary legislation under RIPA setting out which additional public authorities might use these provisions. Further information on this is available from the Home Office at:

<http://www.homeoffice.gov.uk/ripa/part1/consult.htm>

The Anti-Terrorism, Crime and Security Act 2001 introduced provisions for the retention of traffic data for national security and law enforcement purposes. The Home Office is conducting a separate consultation on how these provisions should operate: further information on this is available at:

[http://www.homeoffice.gov.uk/oicd/antiterrorism/vol\\_retention.pdf](http://www.homeoffice.gov.uk/oicd/antiterrorism/vol_retention.pdf)

Regulations 25 and 26 specify that communications providers are exempt from the requirements of the Directive if necessary for the purposes of safeguarding national security, or for law enforcement purposes.

### **Enforcement and Sanctions**

The Information Commissioner is the UK body responsible for enforcement of the rights granted under the Directive. The draft Privacy Regulations continue to give the Commissioner the right to take action either in response to a complaint or on his own initiative. In addition, anyone who suffers damage as a result of a breach of the Regulations is entitled to compensation from the person responsible.

### **Issues**

#### **Should network and service providers be required to disclose the source of unsolicited commercial communications?**

How can subscribers, and the ICO, trace the source of unsolicited direct marketing communications which breach the rules (for example, direct marketing calls made to a subscriber who is registered on the Telephone Preference Service)? The current TDPP Regulations allow, but do not require, operators to disclose to anyone with a legitimate interest (including the police) the source of nuisance or malicious calls or faxes, where the caller has withheld their CLI. Network providers are committed to investigate complaints about such calls from their subscribers and currently invest a great deal of time and effort in their nuisance call bureaux.

However, there is a problem under the current regime where nuisance call bureaux trace a call on behalf of a subscriber but find that the source is a call centre or other direct marketer rather than a deliberately malicious or nuisance caller. Although bureaux will normally contact the call centre or direct marketer to pass on the complaint, they are not usually prepared to rely on the current TDPP provisions to disclose the source of this kind of call to the regulatory authorities. The Information Commissioner does have the right, under current provisions, to issue information notices requiring the provision of information to enable investigation and/or enforcement action to be taken for breach of the TDPP rules, among other things, but it is questionable whether these notices may be issued to bodies (such as, in the present case, network or service providers), who have no involvement in the suspected breach. This can leave subscribers powerless to enforce

their opt-in or opt-out rights. All callers are entitled to withhold their CLI under the Regulations, but direct marketers are required to disclose their identity and valid contact details, either on request in the case of a live phone call, automatically on other forms of communication. If they do not comply with this, they will be untraceable without the help of the relevant network operator.

This raises the issue of whether network and service providers should be under a requirement to disclose the source of a call and/or other form of electronic communication which is suspected of breaching the rules on unsolicited direct marketing. Arguably, this kind of requirement would not encroach on the legitimate privacy rights of direct marketers because they are in any case required to disclose their identity and contact details under the Regulations. It would be consistent with the powers available to Ofcom to require information from network and service providers under the Communications Act. This would however clearly place a new obligation on operators with attendant implications for their relationship with their subscribers. We would welcome the views of consultees on whether this form of requirement is justified and if so, how it should be exercised.

**Should the enforcement procedures and sanctions in relation to the rules on unsolicited commercial communications be strengthened? If so, how?**

The current enforcement powers and sanctions for breaches of the TDPP Regulations are those available to the Information Commissioner under the Data Protection Act 1998. Where there is a breach, the Information Commissioner has the power to issue an enforcement notice requiring remedial action to be taken; failure to comply with an enforcement notice is a criminal offence punishable by a fine. If the Information Commissioner needs more information before deciding to issue an enforcement notice, he can, but is not obliged to, issue an information notice. The information and enforcement notices can be appealed against and the effect of the notice is lifted during the appeal, although where the Commissioner considers there are special circumstances he may require the notice to be complied with as a matter of urgency. In such cases the notice can take effect after seven days, even if it is appealed against.

Enforcement of sanctions against breaches of the rules on unsolicited direct marketing communications raises particular challenges. The current structure inevitably involves some time consuming procedures which do not allow for speedy action. This is becoming a particular issue in the fax marketing area, where the falling cost of faxing is lowering the incentive to comply with the regulatory regime. Although enforcement notices have been issued against some operators, no fines have yet been imposed on a company for breaching the terms of an enforcement notice. For legitimate marketers with a reputation to maintain, the threat of an enforcement notice may be a real deterrent; for others it may not be (and is unlikely in itself to create the kind of publicity that spreads subscriber awareness of their rights and the safeguards available to them).

Are there alternative models? The closest parallel are the sanctions that will be available to Ofcom under the Communications Act. In the case of the new offence of persistent

misuse of electronic networks, Ofcom will be able to impose a direct administrative fine of up to £5,000 and/or seek an injunction to ensure that the terms of enforcement notices are complied with. In the case of consumer protection legislation, and where the collective interest of consumers is being harmed, the Office of Fair Trading, Trading Standards authorities and other nominated bodies now have the power to issue “Stop Now” orders; failure to comply with these may leave the offending business liable to contempt of court charges and subject to a fine and/or imprisonment. Alternatively, breaches or repeat breaches could be made a criminal offence, although this would raise the standard of proof required in individual cases. We would welcome the views of consultees on the case for alternatives to the existing regime, and what they might be.

### **Questions for consultees**

Should network and service providers be required to disclose the source of unsolicited commercial communications?

Should new enforcement sanctions be available against breaches of the rules on unsolicited commercial communications? If so, what should they be?