When Marvin Gaye sang ‘I heard it through the grapevine’, few would have imagined that 40 years later victims of identity theft and data protection breaches would be listening to the track in a whole new light. All too often, however, consumers are unaware of the security breaches regarding their personal information until it is too late. The European Commission are keen to change that, and have recently published a proposal for a Directive amending the current position on users’ rights relating to electronic communications networks, processing of personal data and the protection of privacy in the electronic communications sector.

Two of the main proposals are worthy of note. First, there is to be mandatory notification of security breaches resulting in users’ personal data being lost or compromised. Second, the EC are looking to strengthen implementation and enforcement provisions to
ensure that sufficient measures are available at Member State level to combat spam.

The e-Privacy Directive would be amended to require that end-users are notified about breaches of security, and informed about precautions that may be taken in order to minimise loss or harm. Article 4(3) of the e-Privacy Directive would be amended to read:

In case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of publicly available communications services in the Community, the provider of publicly available electronic communications shall, without undue delay, notify the subscriber concerned and the national regulatory authority of such a breach. The notification to the subscriber shall at least describe the nature of the breach and recommend measures to mitigate its possible negative effects. The notification to the national regulatory authority shall, in addition, describe the consequences of and the measures taken by the provider to address the breach.

The Commission’s rationale for this is clear. It recognises in the recitals to the draft Directive that early disclosure could unnecessarily hamper the investigation of the circumstances of a breach.

For ISPs, the anti-spam measures will be of particular interest. Article 13 of the e-Privacy Directive would be amended to allow for, in particular, ISPs to take legal action against spammers. Article 13(6) would read:

Member States shall ensure that any individual or legal person having a legitimate interest in combating infringements of national provisions adopted pursuant to this Article, including an electronic communications service provider protecting its legitimate business interests or the interests of its customer, may take legal action against such infringements before the courts.

Again, the rationale for this is explained in the recitals to the draft Directive. Recital 35 states that electronic communications service providers have to make substantial investments in order to combat unsolicited communications. They are also in a better position than end-users in possessing the knowledge and resources necessary to detect and identify spammers. Email service providers, and other providers, should therefore have the possibility to initiate legal action against spammers.

Those in favour of the reforms argue that a security breach notification law would have the effect of improving awareness of privacy issues, and would force organisations to be more careful with users’ data. In light of the increasingly tough stance adopted by the FSA, this would appear to be a consistent step forward. It would also bring the domestic position into line with the US laws, where most states have similar laws in place already. Indeed, a number of significant breaches have come to light due to those laws.

Others, notably the Information Commissioner’s Office, have taken a less firm stance. The ICO commented recently that the value of such laws would be undermined if every little breach was notified, with the overall effect being to desensitise the public to more serious incidents. The Government has echoed these concerns, and added that such developments may undermine the internet as a business medium.

Given the recent high-profile breaches of security from Government departments themselves, and the increasing impact of identity-based financial crime, it seems more and more likely that the Commission will leave the UK and other Member States with no choice in the matter.

Technology team
Alex Hamer  
+44 (0)20 3060 6449  
alex.hamer@rpc.co.uk

Alexandra Anderson  
+44 (0)20 3060 6499  
alexandra.anderson@rpc.co.uk

Jeremy Drew  
+44 (0)20 3060 6125  
jeremy.drew@rpc.co.uk

Andrew Hobson  
+44 (0)20 3060 6471  
andrew.hobson@rpc.co.uk

Dianne Vander Cruyssen  
+44 (0)20 3060 6456  
dianne.vandercruyssen@rpc.co.uk

Dean Wilson  
+44 (0)20 3060 6377  
dean.wilson@rpc.co.uk

Editors
Alex Hamer  
+44(0)20 3060 6449  
alex.hamer@rpc.co.uk

Alexandra Anderson  
+44(0)20 3060 6499  
alexandra.anderson@rpc.co.uk

London Office  
Tower Bridge House  
St Katharine’s Way  
London  
E1W 1AA  
+44(0)20 3060 6000

South West Office  
Twyford House  
Kennedy Way  
Tiverton  
Devon EX16 6RZ  
+44(0)1884 243377

Technology Update is a summary of recent developments. It should not be regarded as a substitute for advice on how to act in any particular case. For further information please contact one of the editors.  
© Reynolds Porter Chamberlain LLP  
www.rpc.co.uk