5. Privacy issues

The use of social networks will inevitably involve the processing of personal data and thus engage privacy and data protection laws.

Is social media compatible with privacy?
New technology has challenged traditional concepts of privacy for well over a century. Samuel Warren and Louis Brandeis' seminal 1890 paper on "*The Right to Privacy*" grappled with the prospect of "*numerous mechanical devices*" and "*instantaneous photographs*" creating a world in which "*what is whispered in the closet shall be proclaimed from the house-tops*". Social media, smartphones and other wearable technology, such as Google Glass, has brought this threat to life.

In the intervening hundred years, the law has evolved to provide generalised rights to privacy or specific data protection laws or both.

New technologies are also redefining social attitudes to privacy. Many users disclose significant amounts of personal information about themselves on social media. Indeed, for many, the very purpose of social media is to provide an endless stream of information about themselves from the trivial, to the intimate to the tragic. However, and perhaps counter-intuitively, users remain very concerned about their privacy and want to keep tight control of their information[43].

Ground rules for compliance
Operating in this fluid environment with both changing technology and changing privacy expectations is challenging, not least because the legal framework in the European Union was adopted in 1995. This predates social networking as we now know it and even the widespread use of the internet.

However, the purpose of these laws is to protect an individual's privacy and put them in control of their information. With this principle in mind, you should consider the following guidelines:

> **Don't be sneaky**: Individuals have a right to know what you are doing with their information. The normal way to provide this information is through a privacy policy but these can be problematic, not because they say too little but because they say too much[44]. Think about other ways to get your message across.

> **Don't be creepy:** Make sure you are using an individual's data for a proper purpose. Data protection laws typically only permit use of personal information for certain statutory purposes, such as with consent. They also impose general requirements not to process that information in a disproportionate manner. Often this comes down to a question of the reasonable expectations of the individual, which in turn depends on what you have told them you will do with their information.

> **Put users in control**: Wherever possible, give individuals the opportunity to make informed choices about how their data will be used. Informed consent that will normally ensure use of the individual's information complies with privacy and data protection laws. This is important for marketing activities, which often specifically require user consent.

Key points

> Trust is important. Individual expectations are an important part of privacy laws so don't be sneaky or creepy.

> Be open and transparent with individuals about how you are using their information.

> Do not just rely on privacy policies. Think about other ways to get your message across.

> Wherever possible, give individuals choices about how you will use their information.

> Make information security a priority.

> Use anonymised information wherever possible.

[43] The *Information Commissioner's Annual Track 2013*, which measures the awareness of the Data Protection Act amongst the general public reveals that protecting personal information is the second most important social issue. Its survey reveals 88% of the public consider it of social importance, very slightly behind unemployment (89%) but in front of preventing crime (87%) and education (84%).

[44] For example, see The Cost of Reading Privacy Policies, Aleecia M. McDonald & Lorrie Faith Cranor, I/S: A Journal of Law and Policy for the Information Society Volume 4, Issue 3 which estimated that it would take an individual around 244 hours a year to read all of the privacy policies of the sites they visit during that year, slightly more than half the time actually spent online

[45] Article 29 Working Party *Opinion 03/2013 on purpose limitation*, Working Paper 203, April 2013

> **Think about security:** One of your key duties under data protection legislation is to keep personal information secure. Cyber attacks against organisations are increasingly common, not least because personal information is a valuable asset for criminals for use in identity fraud. This has risen up many regulators' enforcement agenda with a number of high-profile casualties. For example, Sony's PlayStation Network was hacked in 2011 leaking around 77 million customers' details. Current estimates suggest the breach has cost Sony $1.25 billion from lost business, various compensation costs and new investments.

> **Watch out for sensitive personal information:** Additional controls apply to the use of information relating to an individual's racial or ethnic origin, religious beliefs, political opinions, trade union membership, health, sex life or criminal record. The general rule is that this sort of information should only be processed with the individual's explicit consent.

Big Data

Social media generates huge volumes of information. Facebook alone generates 500 terabytes of data a day, including 2.7 billion new likes and 300 million new photos. This is fertile ground for Big Data analysis.

To the extent that this involves personal information, it will be subject to privacy and data protection legislation, a question European privacy regulators grappled with earlier this year in its Opinion on purpose limitation[45]. For the regulators the key distinction is whether the analysis is just intended to detect general trends and correlations (for example, sentiment analysis) or is intended to support measures in respect of an individual.

Unsurprisingly, the former is unlikely to be objectionable so long as there are proper safeguards in place. The regulators stress the need for "functional separation" such that the output of this analysis cannot be linked back to an individual.

In contrast, if the analysis could be used to support measures in respect of an individual, then greater care will be needed. The regulators have an antipathy for profiling, e.g. direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research, and suggest it would "almost always" require specific, informed and unambiguous consent. The legitimacy of other uses will depend on the circumstances but, to a large degree, will depend on whether the new Big Data analysis is compatible with the purpose of the original social media posting.

Future of data protection regulation

The European Union intends to deal with many of the challenges raised by social media through its proposed General Data Protection Regulation. A draft of the regulation was issued by the European Commission in January 2012 and is now being debated by the European Parliament and European Council, with the European Parliament voting through its draft of the regulation in October 2013.

The regulation contains a number of provisions that are relevant to social media. For example, it contains restrictions on "profiling" that are likely to require consent for many types of profiling, mirroring the position already advocated by many European regulators.

It also contains a "right to be forgotten". This provides enhanced rights to ask that personal data be deleted. It is intended to deal with the problem that the internet may reveal information about individuals that is unfair, out of date or just plain wrong.

However, this right is nuanced and is subject to a number of carve outs, such as where it would conflict with another person's freedom of expression. This will make it difficult to apply in practice. For example, while it should be easier for an individual to remove material they have posted about themselves, forcing someone else to remove information they have posted about the individual will involve a harder tussle between competing fundamental rights.