

Editorial

Bridget Treacy opens Volume 10, Issue 5, of Privacy & Data Protection

Against a background of numerous UK data breaches, which seem to occur with frightening regularity, we now describe privacy and data protection as “trust” issues. Organisations regularly refer to breaches of consumer trust when they experience data security breaches, or where personal data are compromised in some other way. Perhaps we link privacy and trust to breach because, in a very human way, we lament the loss of privacy or trust when a breach occurs, yet we take them for granted when they are intact.

The European Data Protection Supervisor (‘EDPS’) has recently published an ‘Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy.’ The title may sound theoretical, but it provides a very practical perspective — almost a blueprint — for additional ways of ensuring better privacy and data protection in our digital age.

The essential focus of the Opinion is that technology is developing so quickly that technology companies and consumers simply do not evaluate, in a systematic way, the impact of new technologies on privacy. Once privacy is compromised, it is too late.

The Opinion promotes the proactive adoption of ‘Privacy by Design’ principles. This approach involves a systematic evaluation of the impact of a new technology or new data processing activity on an individual’s privacy during the design stage of the technology, so that privacy is embedded into the new technology from the outset. The concept is not new: it was first proposed by the Ontario Commissioner, Ann Cavoukian in the 1990s, and since been promoted elsewhere, including by the UK Information Commissioner’s Office in 2008.

The difficulty with Privacy by Design, and with the related concept of Privacy Impact Assessments, is that they sound good in theory, but organisations have been slow to embrace them. The benefits of designing privacy into technology from the outset, and the risks of failing to do so, have not been clearly or widely explained to organisations. Those with a culture of privacy are well aware of the issues, but many organisations are not. Ad hoc complaints from consumers that their privacy rights are compromised, regulators’ investigations and audits to assess the privacy credentials of new technologies, all raise awareness of the issues, but rely heavily on self regulation.

In his opinion, the EDPS supports self regulation based on the concept of accountability,

but considers that legislative change is necessary to force organisations to incorporate concepts of Privacy by Design in a proactive way. Arguably, Article 17 of the Data Protection Directive 95/46/EC provides a legislative foundation for incorporating such concepts in that it requires data controllers to implement appropriate technical and organisational measures to prevent unlawful processing. But this provision is somewhat vague.

The EDPS suggests that Privacy by Design should be expressly included in the data protection legislative framework, in a technologically neutral but mandatory way. The general principles then ought to be elaborated on in specific legal instruments within particular industry sectors. Further, Privacy by Design should be a guiding principle of the EU’s digital agenda.

In addition, the Opinion targets RFID technology, social networking and behavioural advertising for specific attention, proposing mandatory privacy settings, restrictions on third party access to individuals’ information and mandatory consent mechanisms.

The Opinion also promotes the extension of the data breach notification requirements contained within the recent amendments to the e-Privacy Directive. Currently, the breach notification requirement extends only to telecommunications and internet service providers, but for some time there has been speculation that when countries implement the amendments, they may well extend the scope of the breach provisions to apply more generally to any breach.

Perhaps the Opinion is a blue print for future regulatory focus on information and communication technologies. The timing may be significant given that the Data Protection Directive is under active review. The proposed measures are by no means radical, but this may increase the likelihood that they will be implemented at some future date.

Bridget Treacy
Partner at Hunton & Williams
btreacy@hunton.com
