

The IIS believes that only focussing on the commonly accepted privacy principle does not ensure that consumers (end users) will trust a business or government organisation that is handling their personal information.

Increasingly, organisations approach IIS for help with privacy on projects involving new technology that consumers are resisting despite the fact that the project complies with privacy law.

Rather than being concerned about compliance with privacy law such as notice or access requirements, research is showing that individuals worry about loss of control over their personal information whether they are dealing with government agencies or the private sector. This could be loss of control they themselves might have over it, or loss of control by the people or entities to which they have given their personal information.

In turn, this concern appears to be driven by uncertainty about whether or not individuals can trust the entities to whom they give personal information, or who have control over it, to look after it and use it appropriately.¹

Research is also showing that whether individuals are prepared to trust an entity often depends on the risks of failure of any sort and who bears that risk when it comes to pass.²

On the other hand when governments or organisations develop new security initiatives they very often focus on managing their own risks without regard for whether or not the initiative might result in a loss of control in other ways, and in the risk being shifted to the individual end user.³

¹ See e.g. Malcolm Crompton's papers "**The Trust Cluster: Dealing Effectively with Security, Privacy, Identity and Authentication at the Heart of Connected Government**"; and "**Respecting people, their individuality and their personal information: The Key to Connected Government, now and in the future**", online at www.iispartners.com/publications.html and www.cisco.com/web/learning/le21/le34/nobel/2005/post/presentations.html

² See "**Trustguide Final Report**", October 2006, UK DTI et al, online at www.trustguide.org.uk

³ "**A Real Remedy for Phishers**", Bruce Schneier, *Wired News*, 6 October 2005, online at www.wired.com/news/politics/1,69076-0.html

The IIS approach of moving away from reliance solely on commonly accepted privacy principles is also based on the emerging view that excessive reliance has been placed on 'front end' mechanisms of end user control such as notice and consent to protect end user privacy.

This approach is based on the excellent but now ageing thinking from the 1960s by privacy pioneer, Alan Westin and does not take into account the realities of the way high volumes of personal information are collected used and disclosed in the current and rapidly evolving IT environment.⁴ It leaves end users bearing the risk in circumstances where they are not equipped, and as research is showing, not willing, to bear it. At the same time, it requires organisations to spend significant time and expense on activities that are ineffective in protecting the real concerns of individuals.

Reliance on consent can also be less effective in the context where individuals may have little choice about providing personal information if they wish to receive essential benefits or services, or interact in other unavoidable ways, such as the payment of tax.

The IIS view is that the combination of lack of concern about end user risk by organisations implementing new systems and the reliance of current privacy approaches on increasingly ineffective front end measures are creating an environment that may undermine end user trust in the online environment.

The IIS approach involves both the management of individual or end user risks and those of the organisation involved. It explores ways of achieving control besides over reliance on notice and consent. It seeks a customer centric approach that gives individual choice in really important or sensitive areas but does not place an unfair burden of control on the individual in other areas.

Having a broader focus on customer risk gives an organisation a clear competitive edge by enabling them to attract, retain and build deeper relationships with more customers.

⁴ See "**The Failure of Fair Information Practice Principles**" by Professor Fred Cate in *Consumer Protection in the Age of the Information Economy*; Amazon reference www.amazon.com/Consumer-Protection-Information-Economy-Markets/dp/0754647099