Privacy groups attack Google Gmail

Google has landed itself in hot water with the pro-privacy lobby over plans to introduce a free e-mail service for web users.

Over the last few years, Google has outstripped its competitors to create the world's most popular search engine and it now aims to repeat that success by taking on the likes of Microsoft and Yahoo! in the web-based e-mail space.

The selling point for the new 'Gmail' service, aside from being free, is that users will be given a massive 1 gigabyte storage space. But nothing, of course, comes for free and it seems that the price consumers will have to pay is their privacy. Google's Gmail service will aim to generate revenue by scanning users' e-mail accounts and then delivering targeted advertising based on the contents of the messages.

Concerns have also been raised over Gmail's privacy policy which states that "residual" copies of e-mails may remain on Google's systems even after users have terminated their accounts.

Privacy International has already filed complaints in 17 countries, while officials at Germany's federal data protection authority have voiced concerns over Gmail's compatibility with its privacy law. In the US, a coalition of privacy groups has written an open letter of complaint to Google executives, and Californian senator Liz Figueroa recently announced she is considering legislative action to tackle the privacy issues.

Such has been the public furore over Gmail that Google is reportedly mulling over changes to the service, including the possibility of allowing users to opt-out from receiving advertising. The official word from Google, however, is that the service is still at the testing stage and it is not going to jump into any "rash" decisions.

As to the debate on whether Gmail actually violates any national privacy laws, arguments are still being put forward on both sides. Nethertheless, Google has been dealt a blow in the publicity stakes - a simple lookup on its own search engine makes it painfully clear just how much adverse attention it is receiving.

US study reveals privacy spending trends

A new study carried out by the Ponemon Institute has revealed how US-based multinationals are budgeting for their privacy compliance programmes. Results from the IBM-backed *Cost of Privacy* study have shown that while privacy is becoming a higher priority, it is still taking a back seat to other regulatory obligations. 95 per cent of the 44 respondents to the survey felt that their organisations spent less on privacy than on compliance with environmental regulations.

The study showed that organisations with a more mature privacy compliance setup tend to spend more than those in the early stages. The multinationals studied fell mainly into three categories: (1) the planning/architecture stage (spending an average of $3.9 million), (2) the launch and implementation stage (an average of $6 million), and (3) the operational and ongoing maintenance stage (an average of $14 million).

The study found that organisations in the later stages of their privacy compliance programme require higher budgets in order to carry out privacy audits, implement employee training programmes, obtain website certification and privacy seals, and ensure third party processors meet their legal and contractual obligations.

Interestingly, the study found that technology companies spend the most money on privacy compliance, as opposed to the more heavily regulated sectors such as finance and healthcare services. Transportation and the hospitality industries spend the least on privacy initiatives.

In terms of the budgets allocated to privacy enabling technologies (PETs), the survey found that only ten per cent of companies were using PETs to enhance compliance or mitigate business risks. According to Steven Adler, marketing manager for privacy and compliance at IBM Tivoli, this is because adoption of privacy technologies is still in its early stages. "In general, privacy management is moving from legal policy to an operational IT domain, just like other regulatory compliance issues," he said. "Chief information officers today are just as concerned about building privacy management into IT infrastructure as chief privacy officers are about building effective human policies and training."

The kinds of technology that companies will adopt are likely to fall across a range of privacy compliance areas, from managing marketing and privacy preferences, through to digitising privacy policies and automating internal compliance procedures.

The rise in identity theft, data spillage as a result of viruses and worms as well as the huge problems caused by spam is costing industry dearly. According to Adler, privacy and security-related incidents last year cost the global economy $250 billion in direct damages and lost productivity, providing a huge incentive for organisations to implement robust compliance controls. "The only way to control further damage from these problems is to stem the flow of private information into the public domain, and to do so requires IT investment in privacy technologies to embed sound data management and disclosure control into the IT systems that collect and disseminate that information."

European Parliament wants more say over data transfers

A resolution adopted by the European Parliament in March, has criticised the way in which the EU handles international data transfers and has called for more say in the decision making process.

The resolution focuses on the European Commission's report on the implementation of the EU Data Protection, which was published in May last year.

The Parliament lambasted disparities in the way EU countries' handle data transfers, describing some approaches as "excessively rigid" while others as far too "permissive". It also suggested that the disparity is not only affecting data transfers outside Europe, but also internal data flows within the EU. The Parliament said that the "free movement of personal data is vital for the smooth operation of virtually all Union-wide economic activities; it is therefore necessary to resolve these differences of interpretation as soon as possible, to enable multinational organisations to frame pan-European data protection policies."

While the Parliament broadly supports the European Commission's view that the directive should not be changed, it has called for an amendment regarding the process for assessing whether so-called "third" countries meet the EU's data protection standards. It now wants the power to approve the Commission's "adequacy" decisions.

The proposal reflects the ongoing conflict between the Parliament and European Commission over the transfer of airline passenger details to US authorities. The Parliament has been extremely critical of the Commission's attempt to broker a deal with the US, branding it illegal and threatening to take the issue to the European Court of Justice.

Overall, the Parliament's resolution does provide some reassurance for the business community, accepting that organisations need to be able to operate in a "less complex and burdensome environment". It wants to see unnecessary legal obstacles removed and more choices for exporting data to be made available.

Additionally it has also recognised the value of self-regulation as opposed to excessively detailed legislation and has called for the business community to develop a European code of conduct.

EU issues 2nd warning over spam directive

The European Commission is continuing its pressure on EU countries that have failed to transpose the Privacy & Electronic Communications Directive into national law.

Last November, the Commission issued an initial warning to nine countries including Belgium, Germany, Greece, Finland, France, Luxembourg, the Netherlands, Portugal and Sweden. Since then, only Sweden and Germany have taken the appropriate action (see p.10).

The Commission has now delivered a second warning, sending what it refers to as "reasoned warnings" to the remaining countries. They now have until June to provide a reasonable explanation for not transposing the directive. Failing to respond could lead to prosecution by the European Court of Justice.

Framework on short privacy notices launched in Berlin

A group of 23 companies, privacy regulators and consumer organisations from Europe, North America and Australia met in Berlin on March 23rd and agreed on a framework for providing short privacy notices to consumers.

The meeting was convened by Richard Thomas, UK Information Commissioner; Dr Alexander Dix, Data Protection Commissioner, Brandenburg, Germany; Malcolm Crompton, Privacy Commissioner, Australia; and Martin Abrams, Executive Director, Centre for Information Policy Leadership, US. It followed a resolution on short notices adopted at the Privacy Commissioners' Conference in Sydney last September.

The aim of the meeting was to find a solution for improving the presentation of privacy notices, which tend to be overly long, complex, and cluttered with legal jargon. Although many notices are legally correct, the complexity can cause consumer resentment and make them wary of organisations' data handling practices. From the perspective of privacy regulators, complex notices frustrate their aims of raising consumer awareness and improving compliance with data protection laws.

The agreed framework states that short privacy notices should:

- refer to where more detailed information may be easily found
- contain language that the target group can easily understand
- be part of an information package that complies with relevant laws
- follow a consistent format and layout to increase consumer familiarity and understanding; and
- contain an essential minimum level of information.

Richard Thomas and Martin Abrams will speak on short privacy notices at PL&B's 17th Annual International Conference in July (see the events diary on p.5 for more details).