Building a culture of privacy at Hewlett-Packard

Hewlett-Packard is one of the pioneers of a new wave of global companies to see privacy as more than just a straightforward compliance issue. **Barbara Lawler**, chief privacy officer at HP, talks to *PL&B International* about her ongoing efforts to build a culture of privacy within her organisation.

"I first came into privacy for Hewlett-Packard really before CPO was on the map as a job title, or job function," says Barbara Lawler. Starting in the summer of 1999, and later formally appointed as CPO in March 2002, Lawler took up the privacy mantle at HP at a time when data protection was still a relatively low priority issue for businesses. E-commerce was still in its infancy, with all the potential and pitfalls yet to be realised. This was before spam, Internet fraud and privacy breaches really captured the public's attention.

Lawler was given the challenge of building a relatively unknown concept into the business culture at HP and initially, she says, people were simply unaware of the enormity of the project ahead. "I had someone say to me: 'Isn't that [privacy] the little statement you see at the bottom of the web page? What will you do with the rest of your day?' - That was the thinking," she says.

The growth of technology and the Internet has enabled organisations – and in particular marketers – to realise the full business potential of information. But with it comes the responsibility to manage that information appropriately – to *use* people's personal data, rather than *exploit* it. And this is where Lawler comes in.

Unlike many CPOs, who tend to be drawn from legal and compliance backgrounds, Lawler comes at privacy from a business perspective. With over 20 years at HP, her experience is grounded in systems and data management and a range of marketing activities - a background that has helped her to break down the barriers between compliance and business development.

"HP wanted someone who spoke the language of the marketer and could understand what they were trying to accomplish, but could also represent the policy needs and obligations of the company," she says. "Having that long time experience in the company and understanding how things got done through the informal as well as formal structures, was a tremendous help for a function and a subject area that was not just new, but foreign to many people in the company."

She explains that there were two key goals behind HP's decision to be an early adopter of privacy management. One was based around the company reputation. The other, was to view privacy as a key element in upholding the values of the organisation, its brand promises of trust and integrity with its customers.

Lawler says that privacy at HP is more than just about compliance risk or reputational issues, it is something that has been woven into the ethics of the company. It is not just about paying lip service to consumer concerns and demands - HP has taken privacy further by incorporating the concept into its global citizenship framework, sitting it alongside other public policy issues like corporate social responsibility, human rights and fair employment practices.

Developing a privacy framework

One aspect of HP's framework that sets it apart from many organisations is that it splits privacy compliance into two streams, making a distinction between customer and employee data. "When I started we had a fairly long standing employee policy, and there was a working group focussing on calibrating that with the new EU directive," she says. So, one of her first mandates was to develop a framework for customer data that would run alongside the HR policy. "From a customer perspective, this was really a new space so I was chartered to accomplish three things: (1) to build out the implementation framework for the fundamental policy we had around customer data; (2) to do that you need to have a tremendous effort around training and awareness inside the company; and (3) establish the company's approach to privacy as one that sets a leadership example among industry, and within the Fortune 100 as a whole."

Lawler explains that HP laid down a policy framework based on concepts taken from EU data protection principles and BBBonline (the privacy seal provider) requirements. The framework laid down the approach on areas such as consumer notice and choice, data accuracy, access, security and oversight.

This policy was then supplemented by a 'privacy rulebook' which has evolved over time to provide more in-depth guidance on specific areas such as e-marketing, call centre operations, market research and customer focus groups.

A global approach to privacy

Because HP is a global business, its strategy has been to build a standard approach to privacy compliance, adopting the same principles across each of the countries in which it operates. However, Lawler says the global policy still needs to be flexible enough to be able to take into account differences across jurisdictions. "What we allowed for in the rulebook is the need to adapt certain aspects, and that varies from country to country, such as how and when a notice is delivered, what choices are offered, and when and how they are offered."

"It's usually our partners at HP legal that assist us with that. In addition, we have regional-based privacy managers focused on both customers and employees – one for each - that are specialists in these areas."

In Europe, one of the more

complex regions in terms of privacy compliance, Lawler explains that HP's regional managers are further supported by individuals on a country level. It is an approach, she says, that the company is now starting to mirror across other regions such as Asia-Pacific and the Americas.

In marketing terms, HP's approach is to offer its global customers standard choices for marketing – they can choose to receive or opt-out from contact via specific channels such as e-mail, post, telephone or mobile. Additionally, they are also offered a single 'global' opt-out that removes them from all marketing contact.

Lawler explains that although HP's overall standards are global, there is again a need for some country-by-country variation. This is not just because of legal requirements, but also for cultural reasons – for example how customers are communicated to, what language, how often, the style and tone of the message and so on.

She concedes that despite having high privacy standards, recent e-marketing legislation has proved a challenge for HP. This, she says, is mainly because laws such as the US CAN-Spam Act and the European E-privacy Directive contain vague definitions that create confusion for marketers, rather than clarification. "Marketing people, at the end of the day, want to be able to do their project and get the results they're measured on. They want a quick list: a 'what are the five things I need to do to make sure I am compliant, but also meet my business goals."

For employee data HP, again, has an overall global policy, but looking at specific issues on a country-by-country basis is "almost unavoidable" argues Lawler. In Europe, for example, multinationals not only have to contend with different labour laws, but also national variations of what is supposed to be a harmonised set of data protection laws. "It's a real challenge," she says. "It has created a lot of complexity, and takes a tremendous amount of time if you're going to do it well."

Implementing the framework

A key factor in the implementation of HP's compliance programme, says Lawler, is privacy auditing. "We have an internal audit framework that has a fairly detailed, but also layered set of questions, depending upon the kind of audit that is being conducted by the organisation."

She explains that audits of specific business units - such as marketing, for example - will be more rigorous, drilling deeper into core issues such as consumer notice and choice.

On more general country-based audits, where a number of business functions are examined, a more basic audit is carried out, looking at issues such as staff awareness of the HP policy, and whether they have been trained and understand key privacy principles. If the general audit identifies compliance gaps, says Lawler, they will then probe deeper to discover the underlying causes. "Depending on what they find, privacy staff can then go back and engage with those organisations and help them get to a much stronger compliance level."

She explains that auditing is an ongoing process which is tied to the organisation's overall internal audit schedule. "If there's a particular area that needs to be targeted, we partner with internal audit to make sure that privacy is included in the audits where that is likely to be an issue."

Most business units, she says, will be audited every 18-24 months, although higher risk units are hit once a year. And to complement the internal audit process, HP also uses third party auditors to target key areas of the business, examining compliance levels and assessing any gaps that may exist.

> "HP wanted someone who spoke the language of the marketer and could understand what they were trying to accomplish, but could also represent the policy needs and obligations of the company."

Raising awareness

HP is engaged in an ongoing staff training programme to communicate its privacy goals throughout the organisation. "We have some broad general global training for all employees, and then we also find the inescapable need to provide fairly custom-focussed training. What a call centre needs is very different from what an e-marketing group needs."

"Company wide training for privacy was just recently introduced and that will be a requirement every other year for employees," she explains, "with the exception that there are some specific groups that will need to read up on an annual basis - in situations where they have access to sensitive data from a human resources perspective."

As well as raising awareness, Lawler has addressed compliance risks by putting together a series of tools to help build privacy into new projects and procedures. These include templates for privacy impact assessments (PIAs), application development checklists, and implementation tools. She explains that HP is working towards the target of creating a closed loop process whereby every single new project or programme that touches upon personal data is properly assessed against the organisation's privacy policy - a significant undertaking considering the number of small or one-off projects that are created across organisations as large as HP.

To achieve this, HP has appointed full-time privacy managers in each of its core business units, to provide advice and assistance in implementing privacy effectively into their operations and practices.

Outsourcing relationships

Probably the hot privacy topic at the moment is outsourcing and the relationships organisations have with third party processors. "For many companies like HP, these issues aren't new, they just haven't surfaced in the way that they have now," says Lawler. "We have been looking at outsourcing and vendor contracts for quite some time. This was something we started working on in the first year that I came on board."

Moving quickly and ensuring that proper vendor protection was in place was necessary, not just from the perspective of achieving HP's privacy goals, but also to meet its requirements

under the EU-US Safe Harbor scheme, which the company signed up to in January 2001.

Lawler explains that HP employs a mix of vendor agreements depending upon the type of outsourcing relationship. Since late 2000, HP has been incorporating personal data protection agreements (PPDAs) into new contracts and contract renewals. "We also use [EU] model clauses for certain outsourcing arrangements," she says, "where we have multiple data sources moving to multiple locations."

"We've also added some fundamental privacy language to our master service agreement templates." She explains that outsourcing relationships will involving drawing up a 'master' agreement, with several sub-agreements, of which one will include the PPDA. Inserting privacy elements into the master agreement, she says, helps ensure that every vendor agreement contains a basic level of privacy protection, even in low risk relationships where little personal data is involved.

One of the challenges, says Lawler, has been that the procurement process at HP was spread out across the organisation's business units, rather than centralised. This has made it harder to ensure that all procurement departments were getting the right information to put into their outsourcing contracts, although she says that following the HP-Compaq merger (see below) the process has now become more centralised.

Lawler says that organisations do, however, need to go beyond contracts and engage with vendors by reviewing their data handling practices and assessing levels of protection. At HP, she explains, this process will either be done at the vendor selection stage, or once an agreement has been signed and the implementation process is being put in place.

PUBLIC POLICY

Another key element of Lawler's work is based around public policy issues, keeping up-to-date on legislative developments and being the public face of HP's privacy programme. "Right now I probably spend about 25 per cent of my time on these issues," she says. Her policy work involves collaboration with HP's government affairs team to look into privacy developments across a number of regions including Europe, Asia Pacific and Latin America. In addition, she and her colleagues work with industry groups such as the International Association of Privacy Professionals (IAPP) and the European Privacy Officer's Network (EPON). HP also consults with government officials, privacy regulators and other policy makers to "share with them our strategy and our challenges around managing privacy, but also to hear from them what they see as concerns, what they see as most important for a global business like HP."

ONGOING CHALLENGES

One major development over the next two years says Lawler will be to drive forward HP's "design for privacy" initiative, a project aimed at developing a privacy architecture which will ensure that privacy requirements are built into all of HP's products and service offerings.

Overall, Lawler's challenge will be to continue the development and realisation of HP's privacy objectives. "The vision is that privacy will be baked into all our business processes," she says. "But I would say that is a very long-term vision just because of the volatile nature of business in a global company today – processes and business models change on a fairly rapid basis."

Tackling privacy in the Hewlett-Packard - Compaq merger

HP's multi-billion dollar merger with Compaq in 2002 presented a major challenge in terms of merging staff and customer records under one legal entity. One of the objectives was to ensure a seamless merger of the two separate employee databases into one staff directory. The legal problems surrounding employee data and EU data transfer requirements, says Lawler, were eased considerably by the fact that both HP and Compaq were signed up to the EU-US Safe Harbor programme prior to the merger. "That was something that the regulators - both from the European Commission's side and from the FTC - indicated was one of the positive reasons for supporting and approving the merger," she says.

Good labour relations also played its part in smoothing over the transition process. "Because HP in particular had such strong relationships with its workers' councils, we were able to leverage that into getting specific approval from them in advance of day one of the merger, to ensure that we could, with their support and approval, merge those databases and have those available to employees."

On the customer side, Lawler says they decided to take a best practice approach that would maintain good customer relations. "We took on - and this was beyond what we felt was explicitly mandated in any particular data protection law, although you could argue that there were some countries in the EU that would have expected it - a data transfer notification process for approximately 5.7 million pre-merger Compaq customers."

HP decided to take a segmented approach to the customer notification process, depending on whether they were high level enterprise customers, SMEs or individual consumers. The large enterprises, for example, were contacted by their accounts teams at Compaq, while lower level customers were notified via a mix of written or electronic communications. Customers were given the opportunity to opt-out from having their details transferred to the new company in addition to a subsequent notification to revalidate their marketing preferences.

Despite concerns in some quarters that there might be high opt-out levels, Lawler says the project was a huge success. Not only did the project come in under budget and within the deadline, but the opt-out rate only reached around 0.5 per cent. "We thought it was truly worth it," she says. "It showed a lot of respect for those customers and allowed individuals who had strong feelings - either about the merger or about their data being transferred - to have that choice."