Spam laws stifle global marketing

Governments seeking to find a legal solution to the spam epidemic have created a complex and disparate landscape that global marketers will find difficult to navigate. By **Alan Pedersen**.

Over the last year there has been a flurry of new spam laws, hastily drawn up by governments in their belated attempts to rally against the rising tide of unsolicited junk e-mail.

A study published in April by law firm White & Case has shown the extent to which nations are now trying to combat what has fast become a major threat to the integrity of online business. Of the 22 jurisdictions selected for their commercial status, 19 have, or are planning, some kind of spam legislation. Arguably these efforts have been to little effect - spam levels are on the increase and show few signs of abating. Recent figures from MessageLabs revealed that 76 per cent of e-mails sent in May were spam, a 9 per cent rise from the previous month.

What isn't in doubt is the impact these laws have on genuine marketers, especially those whose reach extends beyond national boundaries. To keep on the right side of the law, multinationals are having to factor a host of varied and complex laws into their cross-border campaigns. "If you're trying to do global marketing it requires that you meet the toughest restrictions," says David Bender, a New York-based lawyer and general editor of the White & Case study. The tougher the restrictions, the greater the squeeze on marketers' ability to fully exploit the data they hold, a situation Bender thinks could force global businesses into a strategic rethink.

Opting in or out?

A huge problem is the number of new laws requiring businesses to obtain opt-in consent from consumers, but Bender points out that this style of approach is far from being a global standard. "In the United States, opt-out is generally good enough, but not in the EU," he says. While 13 of the jurisdictions in the White & Case study advocate an opt-in system for e-mail marketing, the rest either favour an opt-out approach or offer no protection at all.

Not all opt-in rules are the same either. Some jurisdictions - most notably in the EU - provide exemptions for companies marketing to existing customers. Others, like Australia and Hungary, do not.

The situation is further complicated by the lack of consistency in dealing with 'legacy' marketing data collected under the old regulatory systems. The UK provides transitional relief, allowing companies to carry on as before. Sweden and Italy, on the other hand, take a harsher line which necessitates the expensive and time consuming process of collecting the appropriate opt-in permissions from existing contacts.

Added burden

If it were just a matter of opt-in *vs.* opt-out, the life of the chief privacy officer would be that much simpler. Unfortunately, spam laws are littered with a mix of additional rules and regulations which in the context of cross-border marketing makes it more likely for mistakes and oversights to creep in.

White & Case's study shows that 13 out of the 22 jurisdictions require businesses to include an valid e-mail address for opt-out requests. 9 jurisdictions impose the additional step of including a postal address.

Many laws require companies to identify advertising e-mails, but again they vary in their approach. In the EU the rules apply only to promotional offers, competitions and games. In South Korea and the US, businesses have the responsibility of flagging up all advertising content.

As well as keeping abreast of new laws, chief privacy officers have to keep an eye on changes to existing legislation. Despite only coming into force in January this year, there is already a "groundswell" of opinion calling for changes to the US CAN-SPAM Act. If the government cedes to consumer demands, Bender believes the US may implement a "more rigorous statute" along the lines of California's spam law, which operates an opt-in system and allows individuals to file their own private lawsuits.

Regulatory failings

It is debatable how much attention companies are paying to the new rules. Bender suspects there is considerable "flouting of the law" as they struggle to keep pace with global change and weigh the cost of compliance against the risk of enforcement action. There is little real incentive to jump through hoops because national regulators currently lack the muscle and experience in dealing with what are relatively new laws. "Enforcement agencies have so few resources that it's going to take time before they begin enforcing the law to the degree where a lot of companies are going to begin saluting it," says Bender.

If the regulators do eventually get their collective acts together, it could signal significant changes to the way global companies carry out their marketing campaigns. "The more the laws are enforced, the more likely we are going to see fewer global [marketing] programmes," says Bender. "Unless the laws move towards each other."

United in disharmony

But while global regulators have signalled interest in finding a common line, they appear to be a long way from delivering. If or when they do, the chances of an effective solution look slim, especially when you consider how the EU has failed to fully coordinate its pan-European fight against spam. The European Commission laboured hard to reach a consensus over its 'harmonising' spam directive, only for its member states - at least those that could be bothered to implement it - to then deconstruct the text and draft enough local variations to make pan-European marketing a truly complicated affair.

For a copy of the White & Case survey: www.whitecase.com

Airline data deal heads towards European Court

A controversial EU/US data transfer agreement may land the European Commission in court. **Vanessa Smith Holburn** reports.

Those in favour of the May 28th agreement between the European Commission and the US Department of Homeland Security (DHS) have described it as a 'milestone', yet others say it is a 'stillborn child'. Did the European Commission get it wrong when, after over a year of negotiations, it issued an 'adequacy finding' allowing the transfer of Passenger Name Record (PNR) data between the two continents?

United opposition

Politicians and consumer advocates clearly think so and, since the initial demand that all international airlines provide the American government with full electronic access to computer systems, many have campaigned against what they believe are blatant violations of the EU Data Protection Directive, which restricts the transfer of data to countries where local data laws are not considered adequate.

Alongside campaigns organised by the European Digital Rights Association, the Dutch MEP, Johanna Boogerd-Quaak, spoke out about the controversial transatlantic arrangement, and like many other Parliament members urged the Commission not to agree to American mandates.

And it is true that such protests resulted in concessions being made, such as a reduction in data retention from 50 years to three and a half, as well as a refusal to hand over diet and health information. However, following a meeting on June 16th, disgruntled Parliament political leaders still recommended the case be taken to the European Court of Justice (ECJ) in an attempt to gain an annulment.

A decision from the EU President to take that recommendation further following a meeting with the Parliament Conference of Presidents is currently pending. Any challenge in the ECJ would likely be based on the fact that procedure of assent was not followed and on violations of EU data protection legislation.

If the ECJ were asked to decide and then found the agreement was not legal questions of blame could arise, with violations effectively occurring since March 2003. The airlines are very much in the crossfire, with passengers potentially holding them liable for failing to get their consent.

Fighting a lost cause

But the signs don't look good for anyone planning such a case. A district court judge recently dealt an all-American blow to class action lawsuits against Northwest Airlines, which had shared passenger information with NASA, with the dismissal based on low consumer expectation of privacy and lack of evidence of harm done. Attention could instead turn to national governments and a Pandora's box of culpability.

Clearly the issue is a political hot potato, with European and US relations already strained and other countries considering a similar deal with the States. But in the real world, is it likely consumers would refuse to travel over data privacy concerns, or that airlines would pay extortionate per-passenger fines threatened by the US for non-compliance or ground flights in defiance?

True, the willingness to bow down to American demands sets a dangerous precedent for European lawmakers, but in reality it may end up as a theoretical example of the complexities of international law, which most leave well alone for fear of the fallout. Indeed, the most likely outcome seems that it could perhaps put possibly inadequate data protection back on the agenda in America.

Author: Vanessa Smith Holburn is a journalist specialising in IT and media law.

US/EU Passenger Name Record (PNR) agreement

- The agreement will exist for 3½ years after implementation, with renegotiations due after 2½ years.
- The US Customs and Border Protection (CBP) department will retain data for 3½ years, unless that data is associated with an enforcement action.
- The CBP will have access to 34 Passenger Name Record (PNR) data elements collected in reservation and departure control systems.
- Data identified as 'sensitive' (such as dietary habits) by the EU and CBP will be filtered by the CBP.
- CBP must only use collected data for preventing and combating terrorism and related crimes, transnational crimes of a serious nature - such as organised crime - and to deal with flight from warrants or custody relating to such crimes.
- There will be no bulk sharing of PNR data, and when data originating in the EU is transferred outside the US, the EU will be informed.
- The Transportation Security Administration (TSA) may use EU PNR data for testing the CAPPS II computer terrorist screening system only after it is authorised to begin testing domestic data.
- Each year the EU and the US Department of Homeland Security (DHS) will meet to review the implementation of the agreement.
- A direct access channel between EU data protection authorities and the DHS Office of the Chief Privacy Officer has been established to deal with concerns of European citizens.