INTERNATIONAL newsletter
ISSUE NO 68 May/June 2003

EDITOR & PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

ASSOCIATE EDITOR
Eugene Oscapella
eugene@privacylaws.com

NEWS EDITOR
Alan Pedersen
alan@privacylaws.com

NEWSLETTER SUBSCRIPTIONS
Shelley Roche
shelley.roche@privacylaws.com

ISSUE 68 CONTRIBUTORS

William B Baker
Wiley Rein & Fielding

David E Case & Yuji Ogiwara
White & Case

Carol Leland
A&L Goodbody

Kate Brimsted
Herbert Smith

Laura Linkomies
Privacy Laws & Business

Nancy E Muenchinger
Denton Salès Vincent & Thomas

Vanessa Smith Holburn
Freelance Journalist

PUBLISHED BY
Privacy Laws & Business
5th Floor, Raebarn House
100 Northolt Road, Harrow
Middlesex, HA2 0BX
United Kingdom
Tel: +44 (0)20 8423 1300
Fax: +44 (0)20 8423 4536
Website: www.privacylaws.com

The *Privacy Laws & Business* International Newsletter is produced five times a year and is available on an annual subscription basis only. Subscription details are at the back of the newsletter. While every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given. No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior permission of the publishers.

Design by ProCreative +44 (0)20 8429 2400
Printed by Direct Image +44 (0)20 7336 7300

ISSN 0953-6795

"comment"

Flexing consumer muscles in the name of privacy

Consumers in many western nations rely on government-made rules to limit intrusions by sometimes over eager private sector organisations. But what can consumers do when there are no rules, or when the rules fail to protect, or are perceived to be failing? Worse yet, what can consumers do when governments themselves are involved in the plunder of personal information, encouraging or compelling private sector organisations to act as their agents?

Privacy advocates have long argued that good privacy policies and practices mean good business. Consumers, they maintain, will stay away from those organisations that do not respect privacy. That is, consumers may individually boycott businesses that do not respect their privacy.

Two stories in this issue of *PL&B International* highlight the next step in the evolution of the boycott. The personal boycott ("I won't shop there anymore") is evolving into the potentially much more powerful organised boycott ("Here's what this company is doing to your privacy. Let's all show our disapproval by boycotting the company").

We discuss the actions of one Texas businessman, angered by the collaboration between a US air carrier and the US government in collecting personal data (p.11). The strongest action that individuals can take to assert their privacy rights, he said, may be to withhold their custom. But his actions went beyond a simple personal boycott. He launched a website campaign which received over six million "hits" within two months.

The impact of organised boycotts may be difficult to measure, but the prospect of six million "hits" at a website discouraging individuals from dealing with a business is surely enough to make anyone take notice - and perhaps rethink their approach to privacy issues.

Eugene Oscapella, Associate Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B Newsletters

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Alan Pedersen on Tel: +44 208 423 1300, or by E-mail: alan@privacylaws.com.

India privacy law, continued from p.1

EU-US THREAT

Despite phenomenal growth rates, Indian vendors are facing threats to their livelihoods. US attempts to resuscitate its flagging IT sector has led to the introduction of a number of state bills which aim to restrict outsourcing to developing countries like India. But NASSCOM believes that EU restrictions on data transfers pose a greater obstacle, and appear to be the reason why India is choosing to model its proposed law on the EU directive. Speaking to India's *Financial Express* in May, Kiran Karnik said: "This Act will take into consideration the minimum requirements set by the European Union…The threat from [the] EU is greater than it is from the US, and this Act will help us retain our position in the EU markets."

Companies locating their processing operations in developing countries are not having an easy time, says Suzanne Innes-Stubb, a lawyer at White & Case. "The current EU law makes it very difficult for multinationals to transfer data around the world, because if there isn't an adequacy finding by the European Commission, then they have to find a different solution."

The problem, she adds, is that there are a whole host of complex solutions depending upon the type of transfer taking place. "There isn't a standard approach that businesses are taking. You find some that are going for [the European Commission's] standard contractual clauses, while others prefer to have a more individualised approach - but that doesn't necessarily seem to be acceptable with all EU member states."

Daniel Cooper, attorney at Covington & Burling, says that businesses using the standard clauses have had mixed results, and for some it has been an unhappy experience. "There are some elements there that any business would be uncomfortable with," he says. "It increases your level of exposure to third party claims in particular, whereas an ordinary contract really doesn't have that effect because you don't give people third party rights to enforce their terms."

The problem with non-standard contracts is that companies could be exposing themselves to legal action should the contract fail to meet national privacy standards. This is a problem compounded by the fact that divergences between EU member states' approach to international transfers is creating an uneven playing field for businesses. "Some jurisdictions are more industry-friendly on data transfers," says Cooper. "Take for instance the UK where you are pretty much, as an organisation, allowed to make that [adequacy] assessment yourself." Then there is Spain, which takes a much tougher line, requiring prior authorisation before allowing data transfers to developing countries (see p.20).

But despite potential legal pitfalls over non-standard contracts, Cooper says that many businesses have "decided that the risk of their contact being determined to be inadequate is one they are going to take in order to facilitate the transfer."

> "The threat from [the] EU is greater than it is from the US, and this Act will help us retain our position in the EU markets."
>
> **Kiran Kirk, president, NASSCOM**

FINDING ADEQUACY

The solution to multinationals' problems would be for India to get an 'adequacy finding' from the European Commission. This would stimulate more trade with India by removing restrictions placed on data imports into the country.

The question is, though, if India does seek an adequacy finding, how long is it likely to take? To date, only four countries have been deemed by the Commission to be providing an adequate level of privacy protection - eg. Switzerland, Hungary, Canada (but only companies subject to the federal law) and the US (for companies signed up to the Safe Harbor scheme).

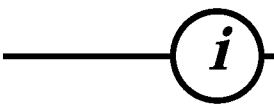
Unfortunately, getting an adequacy decision from the Commission is not a quick process. Despite the fact that the EU Data Protection Working Party published a favourable assessment of Argentina's privacy law in October last year, eight months on it is yet to be given formal approval. However, the Commission has recently indicated that Argentina could be granted adequacy within a matter of weeks.

Stewart Dresner, chief executive of *Privacy Laws & Business* who has worked with the Commission on adequacy reports, says few countries have been granted adequacy "because the European Commission does not have the resources to deal with many countries at once." He adds that it is a time-consuming process, requiring initial research by the Commission, reports from outside consultants, an opinion from the Working Party, possible amendments to the legislation being assessed, and final approval from the EU Article 31 Committee (a group made up of representatives from EU member states).

If India does seek an adequacy finding, it will have to join the back of a fairly substantial queue of countries, including Guernsey, the Isle of Man, Australia, New Zealand, Japan, and South Korea. And with the process generally taking around 18 months, even if India does manage to push its law through before the New Year, it will be mid-2005 at the earliest before a finding comes through.

India may also have to battle for position with other countries pushing for an adequacy finding, but its strong trading ties with Europe could work to its advantage and push it higher up the Commission's agenda.

Even without an adequacy finding, Daniel Cooper says a new privacy law represents a step in the right direction for India and a boost for multinationals. "The ideal situation would be a law that would provide adequate protection in the eyes of the European Commission," he says. "But even short of that, having an effective data protection law would certainly go a long way to easing some of the fears of European regulators that once data is transferred out of the EU, effective control of that data might be lost."



WEB LINKS: India's Department for Information Technology: www.mit.gov.in

The National Association for Software Service Companies (NASSCOM): www.nasscom.org