INTERNATIONAL newsletter

ISSUE NO 73 May/June 2004

EDITOR & PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

ASSOCIATE EDITOR
Eugene Oscapella
eugene@privacylaws.com

NEWS EDITOR
Alan Pedersen
alan@privacylaws.com

NEWSLETTER SUBSCRIPTIONS
Glenn Daif-Burns
glenn@privacylaws.com

ISSUE 73 CONTRIBUTORS

Vanessa Smith Holborn

Ian McGill, Karin Clark, Banjo McLachlan
Allens Arthur Robinson

Alexander Brown, Patrick Martowicz, Alberto Ferrario, Catherine Jakimowicz, Frank Depaepe, Berthold Hilderink
Simmons & Simmons

Florence Raynal, Fabrice Naftalski, Dr Stefanie Hellmich
EY Law

Tim Beadle
Marketing Improvement

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. Whilst 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

US addresses offshore privacy - but who is the real threat?

Outsourcing of data processing operations treads a delicate line. Companies and governments may want to reap the reduced processing costs that come from outsourcing to lower wage countries, while countries such as India want to make outsourcing from wealthy western countries an attractive option (See *PL&B International*, March/April 2004, p.1).

Meanwhile, some politicians from outsourcing countries, and some workers' organisations, are trying to paint outsourcing as a threat to the privacy of their citizens, perhaps using this as a smokescreen for their real concern - the protection of data processing jobs in the outsourcing country. US Presidential candidate, John Kerry, has made it clear that he is concerned about the loss of US employment caused by outsourcing of jobs, which could of course include data processing jobs. At the same time, US Senator, Hillary Clinton, recently co-sponsored a bill in the US Senate to impose restrictions on exports of US personal data in an apparent bid to protect the privacy of American citizens.

This issue of *PL&B International* examines the relationship between privacy and jobs in the outsourcing debate as well as some of the risks companies face when using offshore service providers (see p.24). It also reports on a new twist to the outsourcing issue. British Columbia's (BC) Information and Privacy Commissioner is now investigating concerns that outsourcing the processing of personal data about BC residents to "US-linked" companies may result in that data being subject to access under secret warrants, complete with "gag" orders to prevent them publishing the fact that access was obtained by the US government under the US Patriot Act. Just how far the Patriot Act can extend jurisdiction over personal data originating from other countries may become a major issue for the large numbers of organisations that either outsource or transfer data to the US.

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 E-mail: alan@privacylaws.com.

US outsourcing, continued from p.1

before such information is transmitted.

The bill also provides that business enterprises will be liable for damages arising from the improper storage, duplication, sharing, or other misuse of personal data by the business enterprise or by any of its foreign affiliates or subcontractors that received such information from the business enterprise.

The Chairman of the FTC would be tasked with developing regulations through which the regulator could enforce the bill and impose financial penalties for violations.

Questions raised

The bill poses several unanswered questions. Given the inadequacy of US privacy legislation (in the eyes of EU member states, at the very least), by what standard will the FTC determine whether another country's data protection standards are adequate? The bill states that the EU directive's standards are adequate, but what will be the standard of adequacy for non-EU countries? Will the EU directive be considered the minimum standard, or will the FTC accept a lower standard?

It is also not clear whether the bill contemplates the use of contractual measures to secure an adequate level of protection for the personal data of US citizens processed offshore. Contractual arrangements are often proposed as a viable alternative to data protection legislation. However, the bill will consider a country as having "adequate privacy protection" only if it has been certified as having a legal system that provides adequate protection for personal data. The requirement that the legal system provide the protection may (although it is not absolutely clear) preclude reliance on contractual measures to protect the data of US citizens. Countries that do not yet have general data protection legislation - India among them - could see their outsourcing industries crippled if the bill comes into law before they have adequate (at least in the eyes of the FTC) data protection laws in force.

Even before the SAFE-ID Act was introduced, the US-based Privacy Rights Clearinghouse raised privacy concerns in March through a submission to two California Senate committees examining business and trade policy issues. The issues it raised include:

- What recourse does an individual have if his/her personal information is handled improperly by an overseas company? Most countries to which data is being transmitted have no data protection laws on the books.

- If a US law or regulation is violated, will the appropriate US regulatory agency send investigators to the offshore company to conduct an investigation?

- If an employee of an overseas company observes improprieties and wants to report this, who can he or she contact to file a complaint? And will that individual be protected by US "whistleblower" laws?

- If an individual becomes a victim of identity theft and is able to trace the illegitimate access to his or her personal information back to an overseas company, can that individual attempt to take legal action against that company for its negligence?

- How would California's law (SB 1386) requiring that individuals be notified of security breaches involving

Continued on p.25

Personal Data Offshoring Protection Act of 2004 (HR.4366)

Introduced before the US House of Representatives on May 13th by Democrat Edward Markey, the Personal Data Offshoring Protection Act contains similar provisions to the Clinton SAFE-ID 'companion' bill (see p.1). Key points:

- Offshore outsourcing permitted in countries with "adequate privacy protection". Customers must be given prior notice and right to object.

- Businesses prohibited from outsourcing to countries without adequate protection, unless consumers are notified and consent.

- Federal Trade Commission (FTC) to certify adequacy of countries' privacy laws. Countries failing to meet standards set out by US federal/state laws will not be certified. Countries whose laws have been approved by the European Commission will be deemed adequate, unless the FTC determines otherwise.

- Enforcement carried out by the FTC. Individuals and state authorities can bring civil actions with maximum financial penalties of $30,000 (€25,000).

Further information: www.house.gov/markey

Increasing Notice of Foreign Outsourcing Act (S.2481)

Introduced on June 1st, the bill put forward by Senators Bill Nelson and Diane Feinstein proposes changes to existing healthcare and financial privacy regulations. Key points:

- Organisations must inform individuals that personal data is being processed overseas and alert them to any security risks.

- Organisations must have certification acknowledging that appropriate safeguards have been taken.

- Service providers to be bound by Federal privacy/security standards and contracts must include a right to audit and monitor compliance.

- Offshore service providers must notify any security/privacy incidents.

Further information: http://billnelson.senate.gov