INTERNATIONAL
newsletter
ISSUE NO 70 October/November 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
Glenn Daif-Burns
glenn@privacylaws.com

ISSUE 70 CONTRIBUTORS

Clare Goodman and Mark Watts
Bristows

Laura Linkomies
Privacy Laws & Business

Lilly Tarranto

Merrill Dresner
Privacy Laws & Business

Dr Jan-Peter Ohrtmann
Bird & Bird

Christopher Rittweger and Ilana Saltzman
Baker & McKenzie

Peter Fleischer
Microsoft

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

Technology and privacy - a sticking pendulum

Speaking at a recent Riley Information Services conference in Ottawa, Marc Rotenberg, Executive Director of the Washington-based Electronic Privacy Information Center (EPIC), voiced his concern about the distorted "pendulum swing" with technological surveillance. In times of war, he argued, the legal pendulum swings in favour of increased state powers, but the pendulum swings back in peacetime. However, he saw no pendulum swing back with regard to technology. It would be very difficult to imagine circumstances, he suggested, when surveillance cameras would be taken down once they have been installed. Technological infrastructure is difficult to dismantle.

If this view is correct, we can expect technology to serve as a one-way ratchet twisting ever tighter around the neck of privacy, but never slipping back. Not a pretty prospect. However, one ray of sunshine enters this otherwise gloomy picture. The same technological wizards who drive consumers to distraction with "improved" products that are not compatible with earlier versions of those products may also flog new surveillance technologies with no or little "backwards" capability. Just as consumers will one day find no means to view their old videotapes, surveillance-happy governments may have trouble making previously acquired information useable. In some cases, the companies making a particular technology may long ago have disappeared into the mists of the volatile technology sector. Sometimes a little obsolescence is a good thing.

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.

Sign up to PL&B's e-news service

We would like to remind readers of our free e-mail news service providing up to date coverage on the latest international and UK privacy developments. The service is available to all *PL&B* newsletter subscribers. To sign up, please send your request by e-mail to glenn@privacylaws.com.

JetBlue privacy breach, continued from p.1

protecting both the security and the privacy of our valued customers." To reassure passengers, he announced that the company had retained the services of Deloitte & Touche "to assist us in making sure that we have in place all of the procedures to assure that such a mistake never happens again."

On September 22nd, the Washington-based Electronic Privacy Information Center (EPIC) launched a complaint with the FTC alleging that JetBlue and Acxiom had engaged in deceptive trade practices by disclosing consumer personal information to Torch Concepts. The complaint further alleged that the disclosures occurred without the knowledge or consent of the affected consumers, and in contravention of public assurances that the personal information collected would not be disclosed to third parties. EPIC asked the Commission to investigate and to prevent JetBlue and Acxiom from violating the Federal Trade Commission Act, as EPIC alleged.

JetBlue's privacy policy, found on its website, stated in part that "[t]he financial and personal information collected on this site is not shared with any third parties...." EPIC argued that ConsumerReports.org had relied on this privacy policy in August 2003 when it awarded JetBlue a favorable e-rating for Privacy and Security and Customer Service.

The EPIC complaint alleged that Acxiom had provided additional information to Torch Concepts on about 40 per cent of the passengers whose personal information Torch Concepts had obtained from JetBlue. EPIC alleged that information Acxiom provided to Torch Concepts included gender, home specifics (owner/renter, etc.), years at residence, economic status (income, etc.), number of children, Social Security number, number of adults, occupation, and vehicle information.

The EPIC complaint also reproduced parts of Acxiom's US privacy policy from its website, including the following assurances: "Acxiom respects the privacy of every individual about whom we have information...Acxiom recognizes that individuals should be informed about how information about them is used and have choices about the dissemination of that information... Notices should be provided that explain the collection, use and distribution of personally identifiable information. Most importantly, individuals should have the choice to opt out of the use of their data in marketing campaigns if they so desire."

THE ACTIONS OF THE DOD AND ITS CONTRACTOR

The three senators who approached Donald Rumsfeld for an investigation of possible Privacy Act violations by the DoD and Torch Concepts argued that the Privacy Act applies to contractors working for the federal government. They argued that the Act's criminal penalties would therefore apply to employees of the contractor as if they were employees of the federal government. They argued further that the DoD had an affirmative obligation to ensure compliance with privacy laws by Torch Concepts.

> "It was a well-intentioned attempt to assist the Department of Defense in a national security matter…[H]owever, in hindsight we realize that we made a mistake."
>
> - **David Neeleman, CEO, JetBlue**

The senators noted the apparent absence of any Privacy Act notice published by the DoD for this data-mining system. The notice must describe what information about individuals the system will contain, and it must describe how an individual can gain access to the information. They also suggested that passenger information was shared with others, which might violate the Act.

The Senators acknowledged that after September 11th there was a need to "consider anew" how to undertake the difficult balance between the public's interest in improved security versus the fundamental commitment to personal privacy. "However," they wrote, "the best way to win support for effective homeland security systems is by reassuring Congress and the public that agencies have appropriately considered the impacts on personal privacy, as required by law."

The senators asked for detailed information on several aspects of the case:

- the nature of the US Army's contract with Torch Concepts

- the nature of the information collected by Torch Concepts and the number of individuals whose information was collected; and

- whether the DoD complied with the Privacy Act requirement to publish a Privacy Act notice; whether it allowed individuals to gain access to information pertaining to them; whether the DoD or its contractor disclosed personal information to any other person or entity, including another federal agency; and what steps were taken to ensure that the destruction of these records complied with the Privacy Act, the Federal Records Act, or other applicable laws.

The Department of Homeland Security has also stepped into the fray, according to the *New York Times*. The Department, which had assumed responsibility for airport and airline security, will attempt to determine if government officials violated privacy laws in helping coordinate the data mining project.

RAISED EYEBROWS IN THE EU?

The JetBlue fracas must surely have heightened the fears expressed over recent months by EU bodies about attempts by US government agencies to compel the transfer of airline passenger information to US authorities. Now the EU has to worry about "voluntary" information sharing by airline companies with US agencies. JetBlue's predicament has also highlighted the danger of ignoring important privacy considerations, even while attempting to be a good corporate citizen. JetBlue's CEO argued that the company's action was well-intentioned and an attempt to assist in a national security matter. Even that, it seems, may not be enough to cast aside publicly stated commitments to protect privacy.