

# Privacy & Security Law Update

## International Trends

# Enforcement Outside the US

Security breach issues in the US have overshadowed major trends in international enforcement. In 2006, the Spanish Data Protection Authority alone conducted 1,282 investigations and imposed 24.4 million € in fines. Globally, DPAs and other regulators are engaging in rigorous enforcement.

### Process Violations

EU laws impose an array of process requirements, such as data base registration and responding to data subject requests. Companies neglect these tasks at their own risk.

The UK Information Commissioner's Office announced in June that it was investigating employment companies for unregistered databases. The ICO had previously fined Abacus Recruiting 2,000£ for failure to register.



The Irish DPA is fo-

cused on companies who fail to respond to access requests. It announced in May that it would impose 3,000€ fines on companies that failed to respond to access requests promptly and properly.

In France, the CNIL fined Tyco 30,000€ for improper registration and undisclosed data transfers.

Last October, a German court ordered internet service provider T-Online to delete customer IP logs upon request. The court was unpersuaded by the company's arguments relating to cost or the need to retain logs for law enforcement purposes. Separately, the court ruled that a website operator was in violation of the law because its privacy notice did not sufficiently disclose the uses it made of personal information collected.

### Data Collection

Even where a privacy notice is given, data protection laws



restrict data collection to those elements that are reasonably needed by the company to perform the tasks at hand. Companies are regularly subject to enforcement activity for overbroad data collection.

Last year the CNIL imposed a 50,000€ fine on an investigative agency for inappropriate collection of financial data.

In Germany and Canada, authorities ruled that blanket waivers for the release of personal data to insurance companies were unlawful. Individuals may *continued on page 2*

## IN THE SPOTLIGHT... Cross-Border Enforcement

On June 12, the OECD Council adopted a Recommendation to provide a framework for DPA cooperation in the enforcement of privacy laws. This Recommendation is the result of a series of roundtables, organized by the Canadian Federal DPA, Jennifer Stoddard.

The Recommendation follows an October 2006 Report on the barriers to cross-border enforcement. The Report also contains a useful summary of the enforcement powers of national DPAs.



The Recommendation provides a model for DPAs to support and assist each other for

privacy law enforcement. It calls on OECD members to develop domestic mechanisms that facilitate cross-border enforcement initiatives, such as notification, complaint referral, investigative assistance and information sharing.

The OECD has also developed some model forms to assist with cross-border enforcement initiatives, including a formal "request for assistance" template.

The US Federal Trade Commission has participated in the OECD process. The FTC issued a June 14 statement expressing its support for the Recommendation and noting that it had already imple-

mented many of the specific recommendations.

Given the breadth of cross-border data transfers, we will likely see further efforts to reduce jurisdictional barriers to enforcement. Companies should expect their regulators to cooperate to ensure compliance, without regard to geography.

More information about the OECD effort can be found online at [www.oecd.org/sti/privacycooperation](http://www.oecd.org/sti/privacycooperation).



## Enforcement Trends

only be asked to consent to disclosure of information that is needed at the time.

Last month, the Hong Kong DPA ruled that a company violated the law by collecting more information than necessary in connection with a promotion. The company was required to delete the data.

### Targeted Marketing

Most DPA actions stem from a failure to respect marketing preferences. The Irish DPA reported that 38% of all complaints received last year related to unwanted marketing.

The CNIL brought actions against retailers, marketers, and financial services, imposing almost 80,000€ in fines for failure to respect do-not-contact requests. The ICO addressed unwanted faxes.

Last October, an Australian court imposed an A\$4.5 million fine on a company in the first prosecution under the Spam Act. The Communications and Media Authority followed this in July with an A\$149,600 fine on a marketing company for calls to cell phones.

In India, three firms were fined 7.5 million rupees (~\$170,500) in January for unwanted calls and text messages. The

Hong Kong DPA has also aggressively fined companies for unwanted marketing. The fines typically range from HK\$3,000 to HK\$14,000.

**“Fines are the tool that produce respect for individual privacy rights.”**

— Artemi Rallo Lombarte, AEPD

Quoted in *BNA Privacy Law Watch*



### Information Security

The largest fines result from security breaches. In February, the UK Financial Services Authority (FSA) fined Nationwide Building Society 980,000£ after the theft of a laptop containing account holder information. The FSA determined that Nationwide had failed to properly assess its security risks, implement controls, or conduct training.

In December, the Hellenic Authority for Information and Communication Security and Privacy fined Vodafone 76 million € for a breach of the wireless communication security during the 2004 Olympics. Last month, the Authority fined Ericsson 7.36 million € in connection with the same event.

In June, the Spanish Supreme Court affirmed an almost 1.1 million € fine again Zeppelin Television for inappropriate processing of sensitive data and failure to comply with Spanish requirements for security and data processors.

In July, the Japanese Ministry of Economy, Trade and Industry announced that it would fine companies for security incidents as well.

### Looking Forward

The enforcement climate is likely to become even more stormy, as regulators seek additional powers. Companies must allocate compliance resources as needed to meet these challenges. For additional information, please call Peggy at 404-914-1163.

## Working with Data Protection Authorities

International regulators are no different than our US regulators—they want to work with companies and to understand company needs and practices, but they zealously approach their roles as protectors of individual rights and freedoms. With this in mind, here are a few tips for working with your international regulators:

- Never contact a DPA without first talking with your legal department. Depending on the issue, it may be best for the contact to be made anonymously, through local counsel. It is also critical to anticipate the types of questions and concerns that the DPA may raise.
- If you ask a DPA for permission to process data, be prepared to accept “no.”
- All inquiries received from a DPA should be escalated immediately to legal. The legal department can ensure a prompt, accurate response.
- If a DPA shows up unannounced for an audit, you need to cooperate. Remain calm and polite at all times. Ask the inspectors to show you their identification and their warrants. Also ask for time to telephone your lawyers. The investigators likely do not have to wait, but may do so if you are polite.
- The investigators are entitled to search the premises and access documents and systems containing electronic records. Stay with them at all times.
- The investigators may ask questions about your data processing activities and systems. Record the questions asked and the answers given. Keep your answers short, factual and accurate, and do not volunteer information. If you do not understand the question or know the answer, tell the investigator that you will have the appropriate person respond in writing.
- If the investigators want to retain documents, offer to make copies for them. If they insist on taking original documents, make copies for your own records.
- Do not sign anything produced by the investigators unless you have been advised to do so by your lawyer.

International companies may want to document procedures and train employees on how to work with regulators to develop the best possible relationships.

This newsletter is intended for clients and friends of Privacy & Information Management Services—Margaret P. Eisenhauer, P.C. PIMS is a Georgia Law Firm specializing in privacy, security and information management. If you do not wish to receive communications from PIMS, please email [tanya@privacystudio.com](mailto:tanya@privacystudio.com)—we will gladly remove you from our mailing list.

The information contained in this newsletter has been prepared for informational purposes only and is not legal advice. This communication is not intended to create an attorney-client relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. If you are not a current client of PIMS, please do not send us any confidential information.

Privacy & Information Management Services—Margaret P. Eisenhauer, P.C.

4355 Cobb Parkway—Suite J-280, Atlanta GA 30339

Phone: 404-914-1163

[www.privacystudio.com](http://www.privacystudio.com)