

Controversial Spanish Internet Law Holds Lessons for Europe

Michal Zdzyslaw Halama, Adriana Blanco

About 200 Spanish Web sites closed to protest a new e-commerce law. Legislators should learn from this public reaction and work with Internet service providers (ISPs) to implement laws in a way that benefits all parties.

NEWS ANALYSIS

Event

On 12 October 2002, Spain's Law of Information Society Services and Electronic Commerce (known as "LSSI" in Spain) became effective. About 200 Spanish Web sites have shut down in protest at the "inquisitorial" nature of LSSI.

Analysis

LSSI applies to Spanish ISPs and commercial Web sites. Under LSSI, electronic transactions are treated similarly to ones in stores: The ISP or Web site must show clearly who is responsible for each transaction and the contact details. LSSI also protects consumers against unsolicited e-mails. Breaches of the law can result in fines of up to 600,000 euros (\$582,000). ISPs and Web sites must register with the government, and ISPs have to monitor sites for illegal content. They also have to retain detailed activity logs for every transaction for 12 months. This controversial requirement (introduced by the Senate at the last moment) aims to combat Internet crime, particularly terrorism. The government says that only a judge will have access to this information, but there are data protection fears.

Some sites have taken preventive measures to avoid fines. However, many have shut down sites in protest — and will try to challenge the law in Spain's Constitutional Court — for several reasons:

- Some see LSSI as giving the government intrusive powers.
- Some believe LSSI aims to control Web content and force editors into self-censorship.
- Others believe parts of the law are unclear.

LSSI resembles laws under consideration in other European Union (EU) countries. Legislators should learn from the public reaction in Spain and from the technical solutions implemented. Much of the concern centers on the need to balance the right to privacy (enshrined in the EU's Data Protection Directive) and freedom of expression — a much wider issue than disputes between ISPs and legislators.

Recommendations:

- Legislators should recognize that regulations cannot control the use of the Web absolutely. They should involve ISPs early in the legislative process and extend time scales to fit with technical and market developments.
- ISPs should not implacably resist new laws. They should investigate the technical options, cost and time scale for implementing the storage of logs for 12 months, and present these to legislators via an industry body.
- Internet users should realize that their Web usage will increasingly be monitored under laws designed to detect crimes already covered by the laws.

Analytical Sources: Michal Halama and Adriana Blanco, Gartner Research

Recommended Reading and Related Research

- "Making Privacy Laws Work in Practice" — Differences in privacy laws across EU countries remain a considerable barrier to compliance. **By Arabella Hallawell**

- "European Data Protection Compliance, Part 1: Principles" — Enterprises must convince individual employees that the data protection legislation applies to them and the way they store and process personal information. **By David Flint and James Davis**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509