

## Re-evaluate the Privacy Risks of Hosting Data in the U.S.

Arabella Hallawell

Leading U.S. telecommunications providers may have given a U.S. intelligence agency millions of phone records. Multinational businesses should re-examine the risks of using service providers in the United States.

### Event

On 11 May 2006, the newspaper USA Today reported that three leading telecommunications providers — AT&T, BellSouth and Verizon — have secretly provided the National Security Agency (NSA) with records of millions of domestic telephone calls placed in the United States. The NSA has neither confirmed nor denied the report. AT&T has also not confirmed or denied the report, but on 17 May stated that it will comply with government requests for assistance only "within the law and under the most stringent conditions." BellSouth stated on 15 May that the company has not "provided bulk customer calling records to the NSA." Verizon stated on 16 May that it has not "provided customer records or call data" to the NSA.

### Analysis

The as-yet-unconfirmed reports of major telecommunications providers allegedly providing a U.S. intelligence agency with huge amounts of information about their customers' telephone usage — seemingly without court orders or other legal authorization — raise serious questions about risk exposure for businesses that use U.S. service providers. Data interception and monitoring practices, and their impact on personal privacy, have become extremely controversial issues worldwide. The European Union (EU) member nations have strong personal privacy protection laws — as well as recent, controversial data retention requirements for EU telecommunications providers — that restrict the transfer of personal data outside the EU. And in a highly publicized case in 2004, trade unions in the Canadian province of British Columbia pressed the provincial privacy commissioner to investigate the outsourcing of medical data to the United States, due to concerns about provisions in the USA Patriot Act.

Whether or not these reports are determined to be factual, businesses with both domestic and international employees and customers — particularly those with significant operations in Canada and the EU — should expect heightened sensitivity about the way they use telecommunications, Internet and other communications service providers in the United States, and be prepared to answer questions about their use of U.S. providers. Providers' responses to requests from government bodies can vary widely. Qwest, for example, has stated that it refused an NSA request for customer records, and in a separate case, Google successfully fought to narrow a U.S. federal government request for large amounts of user search data.

### Recommendations for businesses with international operations

- Ensure that you have a clear understanding of the data interception practices in any country where you do business, and of any service provider you are considering using.
- Determine whether alternative hosting locations are available for EU or Canadian personal data or e-mail, Internet traffic and other communications. Prepare contingency plans for moving such data to alternative locations if it becomes necessary due to regulatory or customer demands.
- Have your legal counsel prepare detailed questions for your service providers, so that you clearly understand how these providers respond to requests from law enforcement agencies and other government bodies — in the U.S. and other countries — for access to, or interception of, personal data.
- Require that all service providers notify you as soon as possible when an interception request has been received.

- Negotiate clauses in all service provider contracts that allow for early termination without penalty if you believe inappropriate access has occurred.

**Analytical Source:** Arabella Hallawell, Gartner Research

## RECOMMENDED READING

---

- "Critical Security Questions to Ask Service Providers" — When choosing an outsourcing or service provider, ask about the security of its network applications, operations and end services. **By John Pescatore**
- "IT Security Directors: Privacy Compliance Best Practices" — IT security directors cannot afford to overlook the increasing, and increasingly complex, demands for privacy protection, especially with European data. **By Arabella Hallawell**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

## 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