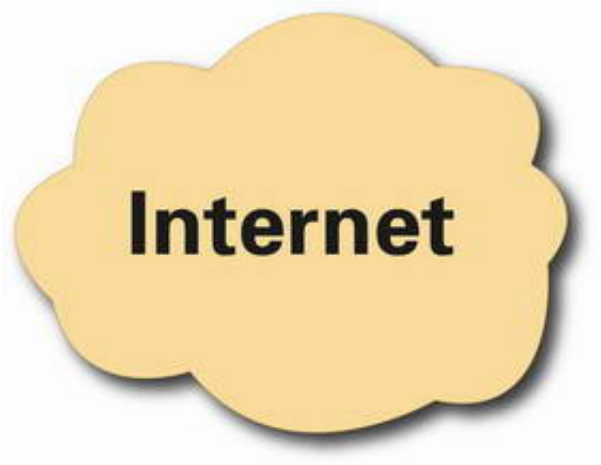
The Web: Europe's cyber privacy declines

December 21 2005



The European Union is no longer the online privacy sanctuary that it once was, as government officials there are enacting a new Internet monitoring law in the aftermath of last summer's London train bombings, experts tell United Press International's The Web.

The EU Parliament last week adopted a privacy directive -- promulgated by the United Kingdom in June -- by a 378 to 197 vote. The directive requires all Internet and telephone traffic to be monitored and stored for up to two years to prevent further terrorist acts on the continent. Civil libertarians here in the United States have previously cited Europe as a model for privacy when arguing against the USA Patriot Act and other domestic data search tools.

The directive requires that all incoming and outgoing messages be retained, as well as Internet Protocol addresses of senders and recipients, short message service, also known as text messaging activity, as well as log-in and log-out times on accounts.

"All the people who thought that Europe was a haven of privacy need to think again," Jim Harper, director of information policy studies at the Cato Institute in Washington, told The Web. "Europe is making great strides toward building a corporate-government surveillance axis with this mandate. This untargeted, general warrant to search the population is probably appealing to law enforcement interests."

There are some protections in place with the new law, which goes into effect next year. The directive will not require the recording of the content of all communications, simply the traffic patterns. What is more, only "competent authorities," as determined by the EU, can access the data. Those who access the data will not be able to see the entire database at once but must limit their search to queries about specific terrorist subjects and actions. There will still be huge costs for data storage.

"The common idea that the cost of data storage is rapidly becoming zero is plainly wrong when you are talking about terabytes of data. It will cost tens or hundreds of millions of dollars to securely store the data in usable form," said Harper. "Europeans will end up paying a great deal more for communications so their privacy can be undone."

An attorney in London told the Web that the debate over the new directive has been, thus far, "Byzantine," but will likely continue. "The European Parliament had previously been an opponent of data retention legislation," Maury Shenk, a partner in the London office of Steptoe & Johnson, told The Web in an e-mail messages.

Now, Internet service providers who have a presence in Europe are going to have to grapple with a number of technical and legal issues, Shenk said. First, they have to determine whether their services fall under the jurisdiction of the law. Next, they have to determine what their data-retention obligations are. Then they will have to create a plan to comply with the regulations. "The concerns that service providers have are that compliance costs -- for network modifications and new hardware and software -- could be extremely large," said Shenk. "Early planning may help reduce or otherwise address those costs."

Another issue is storage access and storage speed, experts said. Organizations often end up paying much more for storage than they had budgeted, because of the need to access the data quickly. Some experts -- at the security and compliance analytics firm SenSage, based in San Francisco -- do not think that relational database software, popular for database management, can handle the new legislative requirements. Data compression may emerge as a technological requirement for ISPs to keep with the law.

Another technological solution -- one being advocated by the firm American Document Management, based in Ft. Lauderdale, Fla. -- is to store all data, from paper documents to voice mails -- on secured Web sites, a spokeswoman told The Web.

There are other problems to be worked out too in Europe. "I understand that the directive may conflict with national laws, such as the German Constitution," said Harper of Cato. "There will be many more interesting twists and turns before it is put into full effect. Hopefully, for the sake of Europeans, it never will be. This shows how European law serves the interests of governments and bureaucrats much more than the European people. The error of entrusting privacy protection to government officials is becoming startlingly clear there."