MORRISON | FOERSTER

Legal Updates & News

Bulletins

Data Retention: Denmark Is First EU Member State to Implement Controversial Directive

May 2007
by Karin Retzer, Jarno Vanto

Privacy Bulletin -- May 4, 2007

PDF Version

Denmark is the first EU Member State to pass a statute implementing the European Union's Data Retention Directive, which calls on communication network operators to retain certain data for a period of six months to two years. Attorneys from Morrison & Foerster analyze the Danish law and the Directive, noting that certain definitions in the Directive are somewhat ambiguous and that the scope of what must be retained is quite broad. They say the Directive left a number of important decisions for the EU Member States, meaning that companies operating in multiple EU Member Sates must devise country-specific compliance strategies to meet the Directives requirements.

Late last year, Denmark became the first EU Member State to pass a statute implementing the Data Retention Directive (the Directive) of the European Union.[1] The Directive is intended to improve the investigation of "serious crimes," including terrorism, by giving the Member State authorities access to communications data that the communications service providers are required to retain for extended periods of time.

The Danish implementing statute is set to enter into force on Sept. 15, 2007, the required implementation date under the Directive. By then, all Member States should have legislation in place that requires the retention of communications data related to fixed telephone numbers and mobile phone numbers. Similar requirements for retaining Internet communications data must be in place by March 15, 2009, at the latest. While implementing legislation has been introduced (but not yet enacted) in other Member States, including Spain, Germany, and the United Kingdom, significant delays are expected. In a meeting held in Brussels on March 14, 2007, where implementation of the Directive was discussed, the Member State government representatives communicated that only a few have even preliminary drafts currently in their national legislatures.

Under the Danish statute, companies that provide "publicly available electronic communications services or public communications networks" must retain communications data for twelve months for the purpose of detecting, investigating and prosecuting serious crimes and will risk fines for non-compliance. The Danes took the middle ground, for the Directive allows a retention period that is between six months and two years in length.

According to industry sources,[2] even a small telecommunications company may generate 100 million records per day, and storing these records for the maximum two-year period would amount to about 72 billion records. The estimated cost of retaining that information varies from a couple of million euros to over €100 million, depending on the source of the estimate. When the Directive was first contemplated, there were calls for compensating service providers for the resulting retention costs. These were not echoed in the final version of the Directive, leaving the compensation issue in the hands of national legislators. The Danish statute stays silent on this issue, whereas for example the implementing legislation in the United Kingdom allows for discretionary reimbursement of retention costs. Telecommunications companies as well as anyone providing technology and support services to them should be aware of the Directive's ramifications, including necessary adjustments of relevant contracts to address the costs, increased data storage needs, public authority access requirements, and increased data security.

Whether the Directive applies to any given company's activities hinges on whether they operate an "electronic communications network" or whether they provide "electronic communications services." Problematically, these are not determined in the Data Retention Directive itself but in the Directive on Common Regulatory Framework for Electronic Communications Networks and Services[3] (the Framework Directive), which contains five key assessment tools. First, an "electronic communications network" is a *transmission system* that permits the conveyance of signals by wire, by radio, or by electromagnetic means. Second, an "electronic communications service" is a service that is normally provided for a fee and *consists of conveying signals* on networks and includes telecommunications and transmission services in networks. Third, *services that provide content transmitted using electronic communications networks and services are excluded* from the definition of electronic communications services. Fourth, "provision of services" means the establishment, operation, control, or making available of a network. Fifth, electronic communications services do not include "information society services", which are defined in another directive[4] as service[s], normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

Because the definitions are somewhat ambiguous and scattered in a number of directives, diverging interpretations in the Member States are highly likely. Perhaps oversimplified, companies that provide network access would be subject to the Directive, whereas companies that provide content would not. For example, if a company runs a network, such as a cable or wireless Internet connection provider, it would be covered because it makes the network available to its customers. If, on the other hand, a company runs only a Web site, it would not be covered because its customers can access the network irrespective of the company. To stave off uncertainty, some Member State authorities, including Denmark's, provide guidance to businesses on whether the implementing laws apply to specific business activities.

The explanatory memorandum (Memorandum) that accompanies the Danish statute states that companies providing software or computer games over the Internet, search services, video conferencing, e-mail and message services such as MSN Messenger and Lotus SameTime (both also mentioned) are not covered. Also, Internet telephony applications that do not comprise any exchange of traffic with the public numbering plan and the conventional voice telephony services (PSTN) are not covered. This would likely mean that if a call is made using a number allocated to the user in accordance with the public numbering plan and the call is conveyed via the Internet (such as the service provided by Vonage in the United States), the Danish statute would apply. If, on the other hand, the call is made using a service that conveys calls via the Internet without a directory phone number (similar to the service provided by Skype), the Danish statute would likely not apply. Thus, the perhaps unintended effect of the new legislation may be to push users to make calls via providers such as Skype without using traditional public numbers.

Finally, the Memorandum specifically excludes from the scope of the Danish statute electronic communications services that are not "commercial" in nature. In general a service is considered commercial when the purpose of offering it is to generate a profit, but the evaluation is carried out on a case-by-case basis. As examples of such noncommercial services the Memorandum mentions library networks, university networks, hospital networks, and workplace networks. Thus, employers providing e-mail and Internet to their employees would not be required to retain communications data in Denmark. It is unclear if providers such as hotel properties offering e-mails and Internet services to guests are covered by the statute. However, providers of Internet access via a hot spot, such as cafes offering wireless Internet, must retain users' access data and, at the same time, retain data that identifies the geographic location of the hot spot in question.

A Bewildering Array of Data

While the Directive and the Danish statute specifically exclude the retention of any content data, the scope of what must be retained is quite broad.

For calls and messages conveyed over fixed lines and mobile phones, the providers must retain the dialing numbers, the dialed numbers, the forwarded numbers, the names and addresses of the subscribers or registered users, message receipt confirmation, and the time of the beginning and the end of the communications. The identity of the utilized communications device (IMSI and IMEI numbers) and network cells in which the mobile phone was used at the start and end of the communication, as well as the precise geographical location of the cellular tower(s) used throughout the communication must also be retained for cellular phone communications.

With regard to e-mail, the physical address of the subscriber or registered user, the IP address of the subscriber or registered user, the user ID of the intended recipient, and the date and time of the log-in and log-off of the e-mail service must be retained. Additionally, for Internet access the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether static

or dynamic, the Internet service used, and the DSL line must be retained.

Providers of wireless Internet connections must also register the exact geographical or physical location of the network access point used, as well as the identity of the communications device. Importantly, any personal data so retained must be processed in accordance with the EU Data Protection Directive[5] and the Directive on Privacy and Electronic Communications and must be destroyed at the end of the retention period.[6]

Finally, Article 15 of the Directive gives the Member States an opportunity to submit a declaration on postponing the application of the Directive to Internet access, Internet telephony, and Internet e-mail until March 15, 2009. Such declarations have been submitted by Austria, Belgium, Cyprus, Czech Republic, Estonia, Finland, Germany, Greece, Latvia, Lithuania, Luxembourg, The Netherlands, Poland, Slovenia, Sweden, and the United Kingdom. Article 15 presents another conundrum to companies since it mentions "Internet e-mail." As discussed above, Denmark specifically excludes web-based e-mail from the scope of its implementing statute. Presumably then, "Internet e-mail" in the Directive would mean an e-mail service that is bundled with Internet access, therefore allowing Denmark to exclude web-based e-mail from the scope of the implementing statute. Once other implementing statutes are enacted, this should become clearer.

Human Rights Concerns

The process of drafting the Directive was characterized by complaints from a number of countries and organizations accusing the Directive of lacking a legal basis, of being a grave threat to human rights and civil liberties, and of being unconstitutional in many EU Member States. The debate continues unabated at the implementation stage in countries such as Germany, Ireland, and The Netherlands. For example a group in Germany has presented a class action suit to be presented to the Federal Constitutional Court in case a statute implementing the Directive is adopted in Germany. The German draft bill has been particularly criticized for going beyond the Directive as it would, if passed, ban anonymous services and anonymous e-mail accounts as well as give authorities access to the retained data in connection with any crime committed using telecommunications networks, including copyright infringements.

While prevention and investigation of terrorism was one of the stated motives for enacting the Directive, how Member States define a "serious crime" has raised the ire of civil liberty advocates throughout the EU. What constitutes a serious crime defines the limits within which the national authorities can access the retained data. The broader the definition, the more instances there are for national authorities to access the data. The Danish statute omits the definition while a fairly broad definition is found in a related statute. This related statute[7] allows government to access the retained data in investigating crimes, including treason; assisting a criminal escape penalty; avoidance of military service; causing disturbance in public services (mail service, telegraph and telecommunications service, data processing systems, water, gas, electricity or heating systems); crime of threatening to commit a criminal act and therefore causing a serious fear for someone's life, health, or welfare; crime of extortion; or a crime where an illegal alien travels or stays in the country without authorization or documentation or works without authorization.

Open Issues

Because the Directive has left a number of important decisions for the EU Member States, companies operating in multiple EU Member States must devise country-specific compliance strategies to meet the Directive's requirements. For example, the Directive gives Member States an option to choose a period of retention within the range of six (6) months to two (2) years. While a number of countries have yet to draft or publish implementing legislation, it is already apparent that there will be significant variation among the Member States on the length of the retention period. As opposed to 12 months in Denmark, the current Dutch draft law for example, contains a retention period of 18 months. Moreover, the Directive gives Member States the power to extend the maximum retention period for a limited time and under "particular circumstances," subject to the Commission's approval. Finally, it is up to the Member States to decide what constitutes a "serious crime" as well as which public authorities may access the retained data.

For the affected parties to voice their concerns, the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament, and data protection authorities. The purpose of the group would be to obtain advice and to encourage the sharing of best practices. The Commission will submit its first review of the application of the Directive to the European Parliament and the Council no later than September 15, 2010.

Conclusions

The Danish statute has quite fluently transposed the Directive into national law. The main purpose of the Directive, having communications data available for law enforcement authorities, will likely be achieved while many uncertainties in how a "publicly available electronic communications service" is defined have been successfully avoided. However, the tricky part is how the statute and related statutes will be applied upon their entry into force. The bulk of the questions will be raised then, and Denmark as well as other Member States will have to prove the critics of the Directive wrong.

This article appeared in the April 30, 2007, issue of *BNA's Privacy & Security Law Report*, and is reprinted by permission. http://www.bna.com/.

Footnotes

[1] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[2] See, e.g., http://www.logicacmg.com/United_Kingdom/400005132.

[3]Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[4] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services.

[5]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[7] Administration of Justice Act, Retsplejeloven.