INTRODUCTION

PRISM International is a not-for-profit global trade association headquartered in the United States and maintaining a European secretariat in Brussels. Our members are companies who provide information management outsourcing services, (including paper and data storage services, confidential destruction services, and document conversion services), to other organizations for profit. The association was formed in 1980.

PRISM International members would not be categorized as either a Telcom company or an Internet service provider. Membership in the organization is voluntary; members join PRISM International in order to gain education, networking and advocacy services.

PRISM International first engaged in the Data Retention Directive (2006/24/EC) following a meeting with MEP Alexander Alvaro in 2007. Based on the feedback we received from that meeting, PRISM International co-sponsored a workshop reviewing progress in implementation of the directive. Our purpose in providing funding for this workshop was simply to introduce an outsourcing option as a means to hold down costs associated with implementing the directive. The more we engage on this issue, the more we realize that concerns regarding privacy and verification of data destruction may be even greater than concerns regarding the cost of implementation. We believe our members may represent a critical catalyst to address both of these concerns.

PRIVACY CONCERNS

Because the directive establishes limits on the length of time data can be retained, citizens of EU Member States have expressed concerns that there is some type of verification of the destruction of data. These types of concerns seem to be increasing with each incident where retained data are inadvertently released. This includes data from governments. MEP Alvaro expressed this concern very clearly in a September, 2008 speech in Plenary where he said, "The Commission and Council are striving, with an incredible amount of activity, to take action in the field of the economic protection of personal data. When we see what is happening in the United Kingdom, Germany and other Member States, where there are cases of loss or theft of personal data administered by public authorities, we have just as urgent a need for action here. This is ultimately more than ever about citizens’ rights, as they are not able to prevent their government behaving in this way. With enterprises, the citizen is still able to choose a different one in case of doubt."

MEP Alvaro’s point regarding a citizen’s choice in case of doubt is key. Even though telcom companies and ISPs use any and all means of verification that they have destroyed data, within the minds of some citizens there is likely to remain some question as to whether this has been done unless the data moves beyond the control
of the organization and is housed with a third party. In this scenario it is possible to imagine a much higher threshold of verification. Moreover, access to this data can also be made more secure by encrypting the data prior to sending it to a third party for storage. Data outsourced in this way is stored by a company who does not have the means to access it (an encryption key). The data owner no longer has physical possession of the data and thus has no means of preserving the data past its point of expiration (without the direct intervention of law enforcement due to an active investigation or legal hold). This type of arrangement works very similarly to a separation of duties control in accounting. There must be cooperation between the vendor and the client in order to act. Aside from the added benefits of data security in this arrangement, we believe the additional layer of verification and transparency of data will probably be of the most benefit to telcom companies and the public.

In our opinion, this reliance upon cooperation among parties provides the greatest assurance that data will be destroyed on schedule and will increase the public trust of telcom companies and improve the overall implementation of the directive. The alternative is unpleasant as MEP Sophiën't Veld noted in a 2005 speech about the Data Retention Directive. “Do the proposals that are now before us make our world a safer place? No, we are, to a great extent, being lulled into a false sense of security, because the proposals are not proportionate. They are ineffective because they are easy to circumvent. They offer insufficient guarantees for the protection of innocent citizens and finally, they offer insufficient guarantees for good cooperation and exchange between the Member States, for that is the key to effective policy, and we still have not seen enough results.”

**COST CONTROL AND VERIFICATION**

Because only a few Member States have decided to reimburse communication services providers, these companies are faced with the real challenge of incurring greater cost to service law enforcement enquiries. Because it is possible for these enquiries to become a financial hardship if the volume increases beyond the capacity of the company to absorb, we strongly advocate for the reimbursement of costs for all telcom companies and ISPs servicing citizens in EU Member States. But Member States have resisted full reimbursement for more reasons than simple budget shortfalls. How can Member States ensure that the costs they are reimbursing are genuine and as low as possible?

Members of the archive, records and information management industry can achieve economies of scale and specialization of tasks that create efficiencies of operation and security. Making use of these service providers decreases the need for investment in infrastructure since private sector facilities for storing and managing information already exist.

Utilization of outsourcing options involves no capital costs and provides third party tracking of costs through non-internal billing to facilitate audit requirements of governments who may be reimbursing service costs of implementing the directive. The outsourcing option provides a transparent cost structure for telcom and ISPs.
CONCLUSION

Public safety is a concern of every government at every level. It is for this reason that the Data Retention Directive was first created. While protecting the safety of citizens, governments are also responsible for preserving the personal rights of each citizen including the right to privacy. Governments who are considering the reimbursement of additional costs incurred by telcom companies and ISPs need the assurance that data retention costs are as low as possible. By involving commercial data protection businesses like those who belong to PRISM International, it is possible to lower data storage costs and reduce the need for infrastructure investment while at the same time provide enhanced data security and independent verification of the timeliness of data destruction. If given an opportunity, data protection companies may be able to play a beneficial role that benefits both telcom and ISP companies and enhances the privacy protections of citizens of EU Member States.