PRISM (Professional Records and Information Services Management) International is a 501(c)(6) trade association headquartered in North Carolina and serving members in more than 60 countries. The members of PRISM International provide paper records management, data protection services, imaging and conversion services and confidential destruction services to multiple clients for profit. Approximately 650 member companies belong to PRISM International. PRISM International also maintains a secretariat office in Brussels.

Since 2008, PRISM International has been actively engaged with members of the European Parliament and European Commission regarding the transposition and implementation of the Data Retention Directive. This directive was put in place as an anti-terrorism measure and was perceived by some telcom companies and European ISPs as an unfunded mandate to retain transactional data beyond the time limit for ordinary business use.

In general terms, the European Union has been more sensitive on issues related to privacy than Americans as evidenced by the European-driven Safe Harbour provisions and recent regulatory action by Germany regarding Google data collection practices. The European Data Retention Directive attempts to strike a balance between the need for individual privacy through limiting retention periods for telcom and ISP transaction data, and law enforcement's need to act quickly to trace the communication channels of terrorists. While the full effect of the directive's transposition has not been felt as yet, (the ISP provisions have not yet gone into effect), the need for balancing individual privacy on the Internet does seem to be an issue of growing concern among Americans. (The recent backlash against the change in privacy settings by Facebook is a recent example).

The following is an excerpt from a white paper provided to the European Commission from PRISM International, which articulates some of the European 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 without a 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."

Thank you for the opportunity to submit these comments.

Respectfully,
James E. Booth
Executive Director

Jim Booth
Executive Director
PRISM International
1418 Aversboro Rd. Suite 201
Garner NC 27529 USA
Voice: +1-919-771-0657
Fax: +1-919-771-0457
jim@prismintl.org