

State Privacy Laws

Massachusetts recently passed 201 CMR 17 which is titled the "Standards for the Protection of Personal Information of Residents of the Commonwealth"; This important piece of legislature, set to begin January 2010, is a big step in state and local compliance laws. Currently, most state laws are reactive. This means that they require disclosure in the event of a breach, but rarely mandate active or proactive protections. It is interesting to watch these state laws develop. Despite the fact that the PCI DSS has laid out most of the ground work, the states are still reinventing the wheel. If the states simply replace the credit card values with Social Security numbers and PII, the framework is largely there. At that point it is simply a matter of choosing compliance dates and managing the fall out. (Not a trivial task necessarily.) While 201 CMR 17 may be first, it will certainly not be last. We have been advocating clients for some time now to think about compliance several years out when building infrastructure and architecting new solutions. The idea is that if your state does not mandate it today, it will mandate it tomorrow, and being one step ahead will create a significantly reduced compliance effort.