

Fair Information Principles for ITS/CVO

These fair information principles were prepared in recognition of the importance of protecting individual privacy in implementing Intelligent Transportation Systems (ITS) for Commercial Vehicle Operations (CVO). They have been adopted by the ITS America CVO Policy Subcommittee.

These principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social, and cultural change. ITS America may, however, need to revisit them periodically to assure their applicability and effectiveness.

These principles are advisory, intended to educate and guide transportation professionals, policy-makers, and the public as they develop fair information and privacy guidelines for specific ITS/CVO projects. They are not intended to supersede existing statutes or regulations. Initiators of ITS/CVO projects are urged to publish the fair information principles that they intend to follow. Parties to ITS/CVO projects are urged to include enforceable provisions for safeguarding privacy in their contracts and agreements.

- Privacy The reasonable expectation of privacy regarding access to and use of personal information should be assured. The parties must be reasonable in collecting data and protecting the confidentiality of that data.
- Integrity Information should be protected from improper alteration or destruction.
- Quality Information shall be accurate, up-to-date, and relevant for the purposes for which it is provided and used.
- Minimization Only the minimum amount of relevant information necessary for ITS applications shall be collected; data shall be retained for the minimum possible amount of time.
- Accountability Access to data shall be controlled and tracked; civil and criminal sanctions should be imposed for improper access, manipulation, or disclosure, as well as for knowledge of such actions by others.

- **Visibility** There shall be disclosure to the information providers of what data are being collected, how they are collected, who has access to the data, and how the data will be used.
- **Anonymity** Data shall not be collected with individual driver identifying information, to the extent possible.
- **Design** Security should be designed into systems from the beginning, at a system architecture level.
- **Technology** Data encryption and other security technologies shall be used to make data worthless to unauthorized users.
- **Separation** Data collected through ITS applications should be used only for the purposes that were publicly disclosed and should not be aggregated with information from other sources.
- **Secondary Use** Data collected by the private sector for its own purposes through a voluntary investment in technology over and above those data required by law should not be used for enforcement purposes without the carrier's consent.