

## WTIA Privacy Principles

The following principles have been developed to guide WTIA members and the technology industry of Washington state when using personally identifiable information\* (PII) in products, services, marketing, storage or any other use where an individual or consumer's PII is known.

The loss, misuse and stealing of PII is a global problem that requires serious responses by all types of businesses that collect and use PII. Many state legislatures are proposing and passing laws that require data encryption, notices of data breaches, limitations on behavioral targeting and other measures to protect individuals and consumers from both real and perceived threats.

If businesses do not react or take initiative quickly enough they will face additional liability and limitations on what information they can collect from consumers and how it can be used. In that light, the WTIA strongly encourages our members and the technology industry to adopt the following principles.

**PII is information about people. Any misuse, loss or stealing of PII affects the lives of people. This must be kept foremost in the minds of WTIA members and the technology industry.**

**PII is critical data for business. It must be understood that way from the top of an organization to the bottom. Loss, misuse or stealing of PII should not be tolerated and policies to protect PII must be developed that apply to everyone in an organization.**

**Access to PII within an organization should be limited to those who have a critical need for it. For those within an organization that need access to PII, personal financial information should be segregated from other PII to lessen the opportunity for misuse or stealing of personal financial information.**

**Organizations must be transparent to consumers, customers, clients and employees about what PII they collect, how they use it, with whom it is shared, what protective measures are in place and options to limit disclosure of PII. Privacy policies can serve this purpose but should be written in plain English, be more prominent and must be developed in conjunction with legal, marketing, IT and others who will have access to PII.**

**Consumers may or may not be aware that companies are using behavioral targeting as a means to develop and market products and services. The use of behavioral targeting tools, such as cookies, web bugs, web beacons and others must be disclosed prominently, either within privacy policies or separately.**

**Organizations must closely monitor third party vendors for access to and use of PII. Access to personal financial information and SSNs should be limited only to those where it is necessary. Third party vendors' use of PII should be restricted to only what is contracted and be prohibited from transferring PII to anyone else.**

**New information gathering technologies, such as RFID, must be carefully monitored when deployed. When using new technologies, PII should be collected with a consumer's or individual's knowledge with a convenient means to opt out or opt in.** These principles are by no means exhaustive and may be added to over time as new consumer and data privacy issues arise. While these principles are directed at WTIA members and the technology industry, government and other industries ought to consider adopting these principles as well.

The WTIA will continue to advocate and lobby for market-based, industry self-regulation but may support legislative measures to protect PII if they are not overly restrictive or create undue liability.

\*PII is defined as: Any information that can be traced to a particular individual. Usually a set of identifiable information is identified through an identification block of data, such as a name, mailing address, phone number, social security number, or e-mail address. Personal user preferences tracked by a Website via a cookie are also considered personally identifiable when linked to other personally identifiable information provided by a user online.

Endorsed by the WTIA Board of Directors October 24, 2008