Data Privacy Guiding Principles

Requirements for meaningful, strong data privacy protections

People's Personal Information Should Remain Private Unless They Agree Otherwise. This is a basic principle of data privacy protection. Unless people voluntarily release information into the public domain, information on who we talk to, what we do, what they purchase – their private lives – should remain private. Should the Washington State Legislature attempt to pass a data privacy law, at a minimum, the following provisions must be included to ensure that Washingtonians have meaningful control over their information, their privacy is protected by law, and strong remedies are available to them when violations occur.

- **Opt-in Consent**: People's information should remain private unless they freely give specific, informed, unambiguous, opt-in consent *before* an entity is allowed to collect, use, and share it. This requires an entity to explain and justify its need for their personal information instead of forcing the individual to navigate complex systems to figure out how to "opt out," which disproportionately burdens those who do not have sufficient time or knowledge — namely, the elderly, the disabled, and those for whom English is not a first language.

- **Protection of People, Not Just Consumers**: All people should have privacy protections, not just when they are acting as consumers.

- **Coverage of All Personal Information**: Protections should cover <u>all</u> personal information, including information collected or generated that can personally identify an individual, not just information called "sensitive." Given aggregation and data mining, any information can be used to reveal sensitive information about an individual. For example, a person's shopping history can expose information about their health and magazine subscriptions can be a proxy for their race.

- **Strong Non-Waivable Privacy Rights**: Strong privacy legislation must guarantee certain minimum rights to individuals, including a right to know and access personal information collected; right to know and access to personal information shared with a third party; right to correction; right to deletion; right to stop the processing of personal information; and the right to data portability.

- **Limitations on Use and Data Minimization**: Entities must be restricted to collecting, processing, and managing the minimum amount of personal information needed to carry out a clear and limited purpose.

- **Limited exemptions**: All types of entities should be required to protect people's privacy and there should not be exemptions for coverage of data when federal laws do not prevent states from providing stronger protections.

M. Lorena González, *Legislative Director* | mlgonzalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington

- **Prohibition of Dark Patterns**: Entities must be prohibited from using dark patterns, which are interfaces designed to confuse and mislead individuals into consenting to things they would otherwise not consent to.

- **No Economic Coercion:** Entities must be prohibited from charging preferential prices, or providing better service, to individuals that permit their personal information to be collected and used, or from refusing services to, or discriminating against those who exercise their privacy rights. Pay-for-privacy provisions worsen the digital divide, which is also a privacy divide and raise racial equity issues. Strong regulations ensure that privacy rights are available to all and not just to those who can afford to pay to keep our privacy.

- **Civil Rights Protections**: Entities must be prohibited from using personal information in a manner that discriminates against people on the basis of race, religion, gender, sexual orientation, gender identity, immigration status and other protected characteristics, ensuring our civil rights are protected online and everywhere.

- **Restriction on Sharing, Selling, and Disclosing Personal Information**: Entities must be required to disclose to whom and under what conditions are they sharing personal information. Moreover, entities must be restricted from sharing information with government agencies without a valid warrant.

- **No Preemption of Other Privacy Laws**: Local governments should be free to provide additional privacy protections to their residents. State and federal laws should be floors, not ceilings, for our privacy rights.

- **Private Right of Action:** People should have the right to take companies that violate our privacy rights to court. Without a private right of action that provides for monetary damages and recovery of attorney fees, people have little practical ability to exercise their rights or enforce protections. Injunctive relief is important, but monetary damages must also be available and meaningful enough that companies will not treat violations as a cost of doing business.