DEPARTMENT OF COMMERCE
WASHINGTON, D.C.

RE: National Institute of Standards and Technology, Developing a Privacy Framework	**)** **)** **) Docket No. 181101997-8997-01** **)** **)**

COMMENT BY THE ARIZONA ATTORNEY GENERAL

This comment is submitted to encourage the National Institute of Standards and Technology ("NIST") to ensure consumer privacy is the chief focus in building its proposed Privacy Framework. Distinct from the U.S. Constitution and those of many sister states, Arizona has an explicit right to privacy guaranteed in its Constitution. Ariz. const. art. 2 § 8. Moreover, as the Arizona Attorney General, I am charged with enforcing Arizona's data breach law. A.R.S. § 18-551 *et seq*. In light of these guarantees and responsibilities, my office's interest is in advocating for privacy-favoring industry standards that, in particular, favor data collection practices that would allow consumers to opt-in instead of opt-out.

Large companies that rely on consumer data must be incentivized to think more seriously about "putting the customer first" when it comes to data collection. Among the largest and fastest growing companies today are those who pioneered the monetization of users' personal data. But consumers often do not know what data is being collected, let alone what such data is worth to others. The status quo—largely comprised of click-wrap consent agreements—does not alleviate this information asymmetry. And the status quo also leaves consumers vulnerable to another consequence of commercialized data collection—data breaches. Recently, my office has been able to provide restitution to consumers whose privacy was violated thanks to multistate settlements with several large companies, such as Uber, over privacy failings. However, after-the-fact settlements are not sufficient to address the problem of data breaches and over-collection of consumer data without consumer awareness and approval.

A robust opt-in requirement for third party disclosure or business use must be the baseline for the Privacy Framework. Before a data collector may use personal information for its own purposes, or transfer it to third parties, a consumer should have to affirmatively consent to such use or transfer. And this requirement must not be satisfied by today's ubiquitous, sweeping, click-wrap model for consumer consent. *See, e.g.*, *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593 (E.D. Pa. 2007) (rejecting clickwrap agreement as invalid contract of adhesion).

Encouraging an opt-in data collection regime will benefit consumers significantly and require companies to more thoughtfully approach key questions, such as why they collect data, what data ought to be collected, how long collected data should be retained, and when it is prudent to anonymize data, especially if doing so will not frustrate the specific purpose for which the consumer permitted the data collection. Operating successfully under an opt-in regime necessitates concentrated efforts by a business towards each consumer. When businesses have to earn consumers' opt-in, they likely will offer an up-front, well-detailed value exchange to the consumer in clear terms: consumers can obtain better features, more value, or even actual payments in exchange for offering over personal data as part of an affirmative opt-in regime. This would be a valuable change to consumers over the status quo of maximum data extraction.

I urge a paradigm shift that recognizes consumers' valuable property interest in their data, and requires adequate procedural safeguards to protect meaningful control over and consent to sharing consumer data, by consumers. Consumers should have more control over their data; NIST should take this opportunity to help shift the current paradigm and empower consumers.

MARK BRNOVICH
Attorney General of Arizona