From: T D <tarana@gmail.com>
Sent: Thursday, October 24, 2019 11:35 PM
To: privacyframework <privacyframework@nist.gov>
Subject: Comments to NIST Privacy framework

Hello,

Apologies for missing the 5pm EST deadline.

Please find my comments attached for your consideration.

It can't be easy taking in all this (at times, contradictory) feedback! Just wanted to say - THANK YOU for making this such an inclusive process and **no worries at all** if the feedback is too late or has already been considered and a different path taken.

Best,
Tarana

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial /Technical)
1	N/A (Individual)	Tarana Damania (tarana@gmail.com)				Much is still evolving in the field of privacy and NIST has recognized the need for the framework to flex to different organization privacy values. However, it might be worthwhile building a framework upon privacy principles that have been the foundation of regulations such as GDPR and the CCPA. This will make it easier for organizations to leverage a single framework to keep track of compliance and regulatory risks while still being outcome-focussed. While the Fair Information Practice Principles (FIPPs) or OECD privacy principles might be pushing the boundaries of their applicability and be considered “outcomes”, a 2020-version of the FIPPs that includes considerations such as: Our vulnerabilities to each other, Manipulation, Automated processing etc. might be beneficial.	Consider basing "current" and "future" states on general principles	General

2	N/A (Individual)	Tarana Damania (tarana@gmail.com)				General observation - Intended audience / Privacy-team considerations - Think the framework will likely work best for Security teams or independent 3rd-line-of-defense assurance teams / consultants that need to confirm general privacy risk coverage and might be more difficult for privacy professionals to leverage. Privacy professionals that are part of privacy / product counsel or product / feature design teams will likely need more granular privacy considerations (e.g. a privacy impact assessment, privacy considerations in launch questionnaires, key elements in a privacy by design program etc.). For e.g. Privacy harm coverage - privacy harms can we quite unique as documented by Daniel Solove in his taxonomy of privacy. E.g. data could already be public, but if aggregated or made more readily available, could result in "Aggregation" or "Increased accessibility" harms and legal risks. Harms resulting from disturbing an "individual's ability to retreat", "expectation of solitude" would fall under the "Invasions" category of privacy harm. NIST would not capture these risks since the framework's focus is on "unintended consequences of data processing", and in the case of "invasions" there oftimes is no data being processed. Some e.g.'s might include:Excessive phone notifications, or app	N/A	General

						notifications when the operating system Do-Not-Disturb option has been enabledRobocallers dialling random numbersPsychological experiments where users might experience a manipulated version of an app without their knowing / consent, even if the data involved is irrelevant / non-sensitive		

3	N/A (Individual)	Tarana Damania (tarana@gmail.com)				General observation - Importance of a framework for risk assessments - As part of NIST's future privacy roadmap, i recommend providing additional privacy risk assessment guidance to organizations. We are familiar with the concept of risk being a factor of impact and likelihood (or “loss magnitude”, probability of a “threat actor” being able to exploit a “vulnerability” using the FAIR risk model components). However, translating those concepts to privacy risks (experienced by individuals) is not intuitive and warrants its own separate discussion.	Please consider prioritizing a risk assessment methodology	General

4	N/A (Individual)	Tarana Damania (tarana@gmail.com)				Minor suggestion - Consider expanding coverage of CT.DP-P6. For e.g. Data processing is limited to that which is relevant and necessary for a system/product/service to meet mission/business objectives AND is restricted to data elements for which the organization has a legal basis for processing of the data (e.g. consent, legitimate interest etc.) - This could for e.g. address the unintended privacy harms that recently occurred from the review of smart speaker recorded conversations by authorized 3rd party vendors hired by the speaker manufacturers. In some cases, consent was buried in pages of T's and C's, in others, it was missing. CM.AW-P1, CM.PP-P1 in combination might address this, but might be worthwhile clarifying.	Expand CT.DP-P6. to include ....AND is restricted to data elements for which the organization has a legal basis for processing of the data (e.g. consent, legitimate interest etc.)	Technical