From: Fitzsimon, Leo <leo.fitzsimon@here.com>
Sent: Thursday, October 24, 2019 1:20 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Stoner, Brendon <brendon.stoner@here.com>; Anderson, Andrew <andrew.anderson@here.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments - HERE Technologies

Dear NIST Team:

Attached please find the comments of HERE Technologies on the “NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management”.

Please contact the undersigned or the contacts listed in our comments if you have any questions or need any additional information.

Best regards,

Leo Fitzsimon

Leo Fitzsimon

HERE Technologies

Government Relations – Americas

1250 H Street, NW

Suite 620

Washington, DC 20005

M: +1 202 340 8081

Comments of HERE Technologies on the Preliminary Draft “NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management”

HERE Technologies (“HERE”) is pleased to submit these comments on the Preliminary Draft “NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management”, published on September 9, 2019.

HERE is a global leader in location platform services, enabling people, enterprises and cities to harness the power of location. By making sense of the world through the lens of location we empower our customers to achieve better outcomes - from helping a city manage its infrastructure or an enterprise optimize its assets to guiding drivers to their destination safely.

HERE has a direct interest in this matter, as our customer base includes many of the world’s leading automotive manufacturers, transportation and logistics companies, and government agencies, all of whom demand secure, high-quality handling of the location data we process on our platform. HERE has had a positive experience with NIST’s Cybersecurity Framework (“CSF”) and believes that the proposed Privacy Framework (“PF”) can similarly help entities better manage and reduce their privacy risks.

HERE has the following specific comments, observations and suggestions on the draft Framework.

There are four broad observations on the framework in its entirety:

- Development of informative references similar to NIST CSF that map to specific privacy standards/regulations already in place would improve the end-user experience
- Creation of something similar to the Cyber Resilience Review (e.g., Privacy Resilience Review) could enable organizations to use the framework as a self-maturity tool
- More clarity articulating the incremental value of using this framework versus the other privacy standards/regulations would be helpful; i.e., if I adopt the NIST PF what am I 'getting' that's new?
- Similar to above, it would be helpful to more clearly connect the PF to the CSF, particularly in the Core function, categories, and sub-categories.

Overarching notes applicable to multiple areas of the framework:

- The “Govern” function is a confusing concept in the privacy framework, especially since it is lifted from the “Identify” section in the NIST Cybersecurity Framework (CSF). Privacy can extend well beyond the traditional risk management roles/priorities in a company. There is also confusion with how this ‘Govern’ in privacy interacts with govern in the cybersecurity framework.
- It is unclear if the PF covers “Recover”, if the CSF categories left out of PF also apply here, or the exact mapping of functions (similar to previous point).
- It is still unclear what the relationship of the PF is to the CSF and if they are supposed to be used adjacent, additionally, or in tandem.

Granular points on the framework and appendices:

- There is significant repetition between lines 320-325 and 174-179 where there is opportunity to elaborate on the five privacy framework functions in a new light or reduce redundancy.
- The privacy framework is a self-ascribed risk management tool; however, there is not a clear way to generate an externally viable output from this framework. As this document suggests in various places, it is purposed for iterative improvements. A tool would be something along the lines of a Privacy Resiliency Review similar to the NIST Cyber Resiliency Review. Line 415 drew attention to this point.
- It would be helpful if the framework provided guidance on what to do with privacy risks after identification for proper ownership and treatment (e.g., line 490).
- Anytime a "risk assessment" is used in context for the paper, a specifier as to organizational or privacy risk should qualify the type of assessment. It is used interchangeably in the paper (line 521) and could conflate operational and privacy risks.
- Referencing the privacy risk assessment definition (line 539) earlier in the document could help the users' understanding when reading and applying the framework.
- Table 2, GV.RM-P3 points to "risk tolerance" and should specify "privacy risk tolerance" because it is later referenced as risk associated with the data processing ecosystem.
- It would be helpful to provide guidance on how to integrate with enterprise risk management objectives and proactive risk mitigation techniques when describing privacy risk assessments in the section titled "Conducting Privacy Risk Assessments" (Appendix D). This could further demonstrate the value of an organization utilizing the privacy framework.

HERE is pleased to submit these comments on the Draft Framework and we would be happy to provide additional information or to answer any questions NIST staff might have.

Contacts:

Henri Kujala
Global Data Privacy Officer
HERE Technologies
Henri.kujala@here.com

Brendon Stoner
Head of Governance, Risk, and Compliance
HERE Technologies
Brendon.stoner@here.com

Andrew Anderson
Senior Risk Analyst
HERE Technologies
Andrew.anderson@here.com