From: Stefan Keller <review@privacydesign.ch>
Sent: Tuesday, October 22, 2019 3:56 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Hi,

many thanks for the opportunity to share my comments on your draft.

I'm grateful to NIST for the excellent material, that you have provided to the community over the years. I'm reviewing your draft through the lens of multinational organizations, that are subject to diverse privacy regulations, including GDPR, other Convention 108(+) derived legal systems, China's Cybersecurity Law, as well as existing and upcoming US state and sectorial privacy laws and regulations, incl. HIPAA and CCPA.

I assumed that your draft would try to establish an overarching framework, so it could be used by multinational companies. - However, I fail to see how a company following this draft, could use it as an enabler to meet the above mentioned frameworks.

Your executive summary emphasizes the "risk- and outcome-based" approach of the Framework (line 100). - This is very different from e.g. GDPR that in general does not allow the impacts to the rights and freedoms of the affected persons to be weighed against the business objectives and mission of the organisation. This is also not what e.g. HIPAA or other existing US privacy laws would allow organizations to do. - I believe you are supporting a dangerous and erroneous expectations here, that company could weigh their business benefits against the privacy impacts to individuals.

You also highlight the need (line 90) to build "customer trust by supporting ethical decision-making". It's unclear to me on which principles this ethical decision-making would be conducted. You are not providing a comprehensive list of privacy principles nor list all the internationally recognized ones. While "accountability" is mentioned, your draft claims that it " occurs throughout an organization, and it can be expressed at varying degrees of abstraction, for example as a cultural value, as governance policies and procedures, or as traceability relationships between privacy requirements and controls."
(line 456ff). This is far cry from having accountable persons, rather accountability seems to be thinly spread throughout the organisation.
Figure 6 seems to further undermine it, by showing Responsibilities on all layer, but not Accountability.

I am baffled why you are pointing out "customers" in your Executive Summary. ID.IMP-3 (Appendix A) rightfully talks of categories of individuals. These includes employees, citizens, patients, students, etc. - A loss of "customer trust" is one of many possible impacts the organization and society can experience. It seems inappropriate to focus just on this one.

I believe that all multinational companies have come to adopt modern principles such as "privacy-by-design" and "privacy-by-default". It pains me that they are not mentioned in this document.

Most importantly, the concept of a Privacy Impact Assessment (as known from GDPR) seems to be missing. This is a major gap, if you try to use your Framework in a global context. - On lines 238-240 you propose "Once an organization can identify the likelihood of any given problem arising from the data processing, which the Privacy Framework refers to as a problematic data action, it can assess the impact should the problematic data action occur." This is contrary to good practices. You don't start with a list of "any given problem", then determine their likelihood and only then the impact. - Rather you'd start with the valuable assets (e.g. patient data, availability) and consider the threats, scenarios, impacts and likelihood from there. Your suggested approach might lead to risks with low likelihood but very high impacts to be ignored.

Figure 3 (line 247) seems to be wrong, as Problems will often have a direct impact on both individuals and organisation. For example, a data loss or loss of data integrity will directly harm the organisation, as well as the affected persons.

In 1.2.1 I would welcome if you could point out that problems related to privacy risks can impact the constitutional and legal rights of US citizens (e.g. ability to vote, to enjoy freedom of expression, etc). To that extent, you might consider adapting the EU langauge around impact to the "rights and freedoms" of the affected persons.

Overall, I am not sure who you see as the target audience for this framework. - Most, if not all, organisations are under very specific legal privacy requirements by now. - If you intend to help future-proof growing organisations to meet with internal privacy regulations and expectations, it would be advisable to align with the frameworks developed by other the privacy regulators of other countries. - If you narrow the audience to organizations focused on the US internal market, then you should align better with CCPA, as the harbinger of other future state legislation.

Regards

Stefan Keller