From: stephen.campbell@nstillc.com <stephen.campbell@nstillc.com>
Sent: Thursday, October 31, 2019 4:25 PM
To: privacyframework <privacyframework@nist.gov>
Cc: privacyeng <privacyeng@nist.gov>
Subject: Privacy: Positive Versus Negative Rights

Dear NIST,

I have enjoyed examining the draft version of the NIST Privacy Framework and the related document NISTIR 8062. As a security and privacy consultant (and adviser to the Center for internet Security) the biggest thing that jumps out at me is the lack of the concepts of positive rights and associated obligations in the supporting models.

Privacy is a composite right that consists of both negative and positive sub-rights. See https://www.learnliberty.org/videos/positive-rights-vs-negative-rights/. The new framework talks mostly of privacy in terms of the risk of an adverse effect on an individual created either by the classic compromise of the confidentiality, integrity or availability of personal data, or by a "problematic data action". All good stuff. This pertains to the negative sub-rights associated with privacy: freedom **from** embarrassment, stigma, economic loss, physical harm etc. precipitated by a security incident or by a problematic data action associated with the individual's personal data.

But to model privacy we also need to account for an individual's positive rights. Depending upon the regulatory environment these include the right **to** be informed through a privacy notice of the purpose of the data collection and the uses of the data, the right **to** opt in or opt out, the right **to** request the data, have it erased, have it rectified etc. These positive rights impose obligations on the data controller. These obligations also create risks for the controller if the controller fails to carry out the obligations. They have to do with the establishment and maintenance of trust as captured in the design goal of predictability.

One way to include the positive rights and associated obligations into a conceptual model is to depict privacy at a high level as consisting of both negative and positive rights. The negative rights can then be modeled using the privacy risk model outlined in the current documents, such risks consisting only of direct risks to individuals and indirect risks to controllers created by direct risks to individuals. The positive rights can be modeled in terms of obligations. These obligations can be modeled either in terms of the improved trust that successful fulfillment of the obligations can bring about, or in terms of the indirect risks to the controller caused by a failure to carry out obligations tied to the individual's positive rights.

I hope that makes sense. I realize my comment is past the deadline but would appreciate your consideration. Email or call if anything is unclear. I am in the Boston area.

Kind regards

Stephen
774 777 6784