From: Jacob N Shepherd <jns2161@columbia.edu>
Sent: Thursday, October 24, 2019 12:41 PM
To: privacyframework <privacyframework@nist.gov>
Subject: Privacy Framework Comments

Hello,

Please see comments on the Privacy Framework Draft attached.

Best,

Jacob Shepherd

--
Jacob Shepherd
J.D. Candidate, Class of 2020
Columbia Law School
jns2161@columbia.edu
(404) 542-5390

Hello,

For the current working draft, I would like to propose two broad comments:

Formalized ambiguity.

The Data Processing Ecosystem outlined in Section 3.5 seems to contemplate only those entities that have a formal data relationship with the organization implementing the privacy framework. On the other hand, the threat of malicious actors is either implicitly or explicitly considered throughout the framework. What seems to be absent, or at least inadequately outlined, is the vast number of neutral parties accessing data without either malice or explicit permission. There are countless applications currently scraping data from any publicly accessible source, often without the explicit permission of the organization that owns that data.

For example, government agencies routinely put out data that can be pulled as reports through agency data portals. However, those data sets can often also be pulled by utilizing relatively basic web-scraping tools. This is partly enabled by agency practices in which a generic public user ID is created to allow non-validated actors to access the public data tools. While this method brings individuals into the framework of validated access, it also creates a backdoor through which web scrapers can access that data without using the sanctioned reporting methods. While this may not necessarily be problematic in the use of public data, it creates a magnified risk for instances in which data that should be private is made public. It also heightens the risk that determined malicious actors can use information gleaned from the generic login protocol and other public information to access secure sites.

This framework should highlight how organizations can properly interact with those third-party entities that are accessing their public data in benign ways. There are a number of ways this can be achieved – providing a single authorized data access channel, enabling monitoring on all public data page views, or even requiring an internal login for any data access. Whatever methods organizations choose to enable these interactions should be thoughtfully considered and actively chosen.

Deliberative peer review.

Privacy breaches are significant events that can have serious impacts on an organization, let alone on the careers of those responsible for allowing the breaches. Within the governance structure frameworks, some language should be included that speaks to aligning incentives between the organization's privacy goals and the individual responsible party's self-preservation instinct.

Fortunately, other organizations have done the work of pioneering methods by which similar incidents can be actively monitored and reviewed. Most notably, the Federal Aviation Administration ("FAA") has implemented the Aviation Safety Action Program ("ASAP"), a voluntary disclosure program that allows pilots to report safety issues that did not result in major incidents.[1] This program allows the FAA greater insight into the daily practices of the regulated, while creating a framework through which issues that do not rise to the level of actionable

---

[1] *See* Russell W. Mills, Dorit Rubenstein Reiss. "Secondary learning and the unintended benefits of collaborative mechanisms: The Federal Aviation Administration's voluntary disclosure programs." *Regulation & Governance (2014) 8, 437–454.*

violations can be documented and analyzed. Furthermore, it allows private industry groups to gather these instances and publish them in trade newsletters for pilots to read and absorb. Instituting similar programs for privacy concerns and breaches may help to ameliorate any tendency by individuals within organizations to minimize or hide privacy breaches for which they would be held responsible.

Implementing governance structures and processes by which minor data concerns or breaches can be reported and analyzed without fear of repercussion, and by which those learnings can be disseminated throughout the organization, will allow for a more robust privacy framework. In building this framework, NIST should consider suggesting these governance structures as best practices.

Best,

Jacob Shepherd
J.D. Candidate, Class of 2020
Columbia Law School
jns2161@columbia.edu
(404) 542-5390