Google

National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

January 14, 2019

Re: NIST Request for Public Comments on Developing a Privacy Framework, Docket Number 181101997-8997-01

Google appreciates the opportunity to provide comments in response to the National Institute of Standards and Technology (NIST) Request for Comment on Developing a Privacy Framework.[1] Google recognizes the longstanding leadership of the US Commerce Department in promoting data privacy policies enabling continued innovation and, in particular, the Department's open and consultative processes for developing policy and technical frameworks. We specifically appreciate the opportunity for stakeholders to participate in the workshops hosted by NIST to further refine the Privacy Framework and be part of this transparent and public dialogue.

As we noted in our comment to NTIA on Developing the Administration's Approach to Consumer Privacy, promoting a comprehensive, balanced, and practical approach to privacy will improve privacy and security protections, build user trust, and promote continued societal and economic benefits made possible by the free flow and innovative uses of data.[2] We appreciate NIST's ambition to develop a Privacy Framework that will be a tool to help organizations take a "prioritized, flexible, risk-based, outcome-based, and cost-effective approach"[3] to privacy risk management. Complex, prescriptive privacy requirements can require considerable resources. Practical guidance, like what NIST proposes with this Framework, can support organizations not only while developing an initial privacy program, but also in sustaining that program as an organization grows and operates in a dynamic regulatory environment.

In this request for comment, NIST is soliciting feedback on a wide range of topics—several of which were discussed at the first workshop—to inform the development of the Framework. We have focused our comments on a few areas where we felt our experience has given us unique insight or where we wanted to emphasize our support for a particular idea. We also address some of the issues raised in, or absent from, "An Introduction to Privacy Engineering

[1] Developing a Privacy Framework, 83 Fed. Reg. 56824 (Nov. 14, 2018).
[2] Google Inc., Comment on Developing the Administration's Approach to Consumer Privacy (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/google_comments_for_ntia_rfc_on_privacy.pdf.
[3] https://www.federalregister.gov/documents/2018/11/14/2018-24714/developing-a-privacy-framework#footnote-1-p56824

and Risk Management in Federal Systems."[4] In particular, we have addressed some of the foundational aspects of a successful, scalable, and dynamic privacy program based on our experience. There are many other areas where we have researched and published extensively, and we would welcome the opportunity to join other stakeholders in providing further feedback on any specific technologies or areas of privacy research.

Privacy Framework Development and Attributes

We agree with the minimum attributes identified in the notice, and are particularly supportive of NIST's emphasis on a transparent process, accessible language, and adaptable framework. In furtherance of those goals, we wanted to share some additional perspective on the value they add to the outcome.

Encouraging broad participation in this process is equally important to the success of the output as it is to the transparency of the process. Privacy practitioners, engineers, researchers (including user experience (UX) researchers), designers, and product experts are often under-represented in discussions about privacy management. We hope the workshop series will provide an opportunity to bring stakeholders with these backgrounds into the discussion so that their practical insight can be incorporated into this important document, as well as noted as part of the public process and documentation.

Additionally, NIST's commitment to common and accessible language will support the success of the Framework and, as an ancillary benefit, will also improve the public discourse on these important issues. Much of the ongoing conversation around privacy tends not to place sufficient emphasis on the systemic view of the topic, but rather addresses specific concerns or scenarios. The Framework can provide a common vocabulary and baseline understanding of the practical realities of privacy management, supporting a more nuanced and in-depth dialogue on privacy in addition to its practical guidance.

Finally, creating an adaptable Framework is uniquely challenging given the breadth of organizations and individuals in need of guidance on privacy. In addition to considering the variety of the intended audience for NIST's Framework itself, it is worth reflecting on the diversity of their users and customers. In a global marketplace, even small, US-based organizations may have customers or users from around the world. Each country has its own cultural identity, economy, laws, and political landscape that need to be considered when managing privacy obligations. Drawing attention to this fact in the Framework, and creating modules or prompts that could spur relevant research in these areas, is important to providing guidance appropriate to the variety of users that organizations serve.

---

[4] Brooks, et al., *An Introduction to Privacy Engineering and Risk Management in Federal Information Systems* (Jan. 5, 2017), https://www.nist.gov/publications/introduction-privacy-engineering-and-risk-management-federal-information-systems.

Google

Another core element of adaptability is scalability. Multinational companies with a history of managing complex privacy compliance will typically have the resources necessary to understand and respond to general technical advice in a manner that accords with the state of the art. However, smaller companies might struggle with insufficiently detailed or actionable guidance. Involving a diversity of stakeholders, including practitioners and researchers, will promote a rich discussion and ultimately a more durable Framework and roadmap.

Response to the Request for Information

Google recently celebrated our 20 year anniversary. For 20 years we have provided tools to people around the world in the service of our mission to organize the world's information and make it universally accessible and useful, and along the way we have worked to safeguard user data, to be transparent about how we use data, and to keep our users in control. As a multinational company, the cultural diversity of our users is reflected in the varied preferences and desires of our users around the globe. We have learned much about the practice of privacy as we've grown as a company, including learning from our mistakes. We have also learned much as a result of operating as a global company over a time when the Internet has seen dramatic growth and change.

We draw from that experience to make the following observations and recommendations about NIST's proposed Privacy Framework.

Risk Management

Developing a clear and operational definition of privacy risk is critical to the success of the Privacy Framework. Specifically, unlike the description in "An Introduction to Privacy Engineering and Risk Management in Federal Systems,"[5] the definition should be inclusive of the idea that privacy risk is not *solely* an unintended byproduct of the intended functioning of a system. This definition ignores the hazard of bad intentions. Indeed, significant privacy risk may be core to the intended functioning of the system in cases where organizations have ill-conceived plans. This is certainly more likely to happen without proper plans and guidance, but the Framework should not ignore this possibility and work to address this specific type of risk as well.

Guidance on improving organizations' management of privacy risk must be technology and industry agnostic in order to be effective. While context matters, individual privacy risk is not primarily based on the type of organization processing data. Rather it is factors like the type of processing, the stakes of the result, and the individual's specific circumstances or tolerance that motivate privacy concerns. This is acknowledged in the scope of existing privacy

[5] Brooks, et al., *An Introduction to Privacy Engineering and Risk Management in Federal Information Systems* (Jan. 5, 2017), https://www.nist.gov/publications/introduction-privacy-engineering-and-risk-management-federal-information-systems.

frameworks. For example, the GDPR governs the processing of personal data across sectors in the EU. Additionally, for the purpose of NIST's process, organizations outside of the technology industry might find the highest value in this guidance.

Organizational Considerations

Guidance on building and maintaining a privacy program should include: engaging a diverse team of experts early in the process, ensuring there are appropriate checkpoints for review, and planning for technical and human failures. Sustaining a privacy review program requires some flexibility to respond to changes to technical infrastructure, business practices, and data access and use. Additionally, the team's purview should be clear. Preferably, the experts will be empowered to review and investigate the purpose of a particular proposal, rather than focusing exclusively on questions related to implementation. Organizations can also give privacy teams the option to block product launches, which should be seen as a last resort but can empower the team to investigate difficult questions during the design process and encourages others to involve them throughout product development.

The best privacy practices are ineffective if people don't want to use a product or participate in the ecosystem of options. Design, user experience, and user research are primary, not secondary, considerations to building functional privacy systems. As a result, NIST should consider recommending that organizations build teams with a broad range of skills including these particular specialties.

As privacy expectations are fluid and influenced by a number of external forces (technological change, societal change, and regulatory change), the effective requirements can be a moving target. This Framework is an opportunity to prepare organizations for the ongoing work of privacy management by reinforcing that this work requires persistent attention and ongoing investment.

Structuring the Privacy Framework

The Framework should support managing privacy risk in a way that respects people and communities. This includes acknowledging that, in many cases, there is no single best answer to a privacy question. For example, some people prefer to see tailored ads and content while others prefer to minimize personalization of their experience. Neither of these views is inherently problematic for privacy. Organizations should plan to account for diversity in privacy preferences while building their systems, thus providing users with intuitive choices to control their data and experience. Establishing diverse perspectives on a team helps organizations plan for, and accommodate, this variety among individual views and needs.

As such, NIST should encourage organizations to foster diversity on the teams that work on privacy efforts. Successful privacy management requires the team to be able to understand and relate to and address situations that their users or customers are personally experiencing, which will likely represent a tremendously diverse set of problems and preferences. Building a

team that includes people of different genders, races, ethnicities, nationalities, ages, sexual orientations, physical abilities, socioeconomic backgrounds, etc will improve the quality of the system by improving the team's ability to collectively imagine, account for, and ultimately respond to the needs of their users.

In addition to demographic diversity, organizations should cultivate a variety of academic and career specialties on the team. While some privacy engineers are systems engineers,[6] organizations may also require experts on anonymization, user research and design, analysis and monitoring, incident response, and program management to effectively manage their privacy risk. Some of these experts take on tasks we traditionally describe as software engineering, while others promote consistency and solve judgement-call issues where human nature is part of the equation. On top of these roles, organizations will likely enlist support from legal professionals to appropriately manage legal risk and communications professionals to answer questions from the public about their privacy practices. Each of these contributions is part of a sustainable and successful privacy program.

To make this guidance actionable, it might be helpful to include categories of expertise or general job titles in the documentation of the Framework, in support of NIST's goal to produce accessible information. Technical titles and specialities can be confusing and intimidating for some individuals, which can impact whether the right variety of experts are working on a given issue. Additionally, some may overlook the importance of working with a range of non-technical experts as part of an organization's privacy management.

The Framework, and the documentation associated with it, should foster generalized support for increased development and use of these types of experts. As more and more organizations seek to tackle privacy challenges, the demand for these skills has already outstripped their supply. Scalable tools and processes may help, but the need for trained talent will not diminish and NIST can reinforce the need for additional professionals in these fields.

Specific Privacy Practices

In many contexts, the interface between individuals (customers, users, citizens) and an organization is the place where privacy is realized. Because of this, the statements and promises made at those moments are a pivotal part of any privacy process. In addition to making faithful representations to their users, organizations should work to define measurable and verifiable information about their privacy practices. When possible, organizations should share these as a contribution to the state of the art. Identifying these parameters enables an organization to monitor and address any issues that arise with their system. That said, many

[6] Brooks, et al., *An Introduction to Privacy Engineering and Risk Management in Federal Information Systems* (Jan. 5, 2017), https://www.nist.gov/publications/introduction-privacy-engineering-and-risk-management-federal-information-systems.

privacy assurances cannot be verified in this way because these statements are not just descriptions of technical safeguards, but often are pronouncements about an organization's values or business practices. The Framework can acknowledge that both types of statements serve a purpose, while explaining the value of measurable promises.

Organizations must prepare to detect, understand, and address problems. Creating technical safeguards, both through monitoring systems and by designing systems to default to certain behaviors (such as systems “failing closed” in security operations), is a worthwhile recommendation. Additionally, the guidance might reference assigning a team to actively look for problems (commonly called a “Red Team”), attacking your own system.

Finally, organizations must develop methodologies to learn from what went wrong, as well as near-misses, by interrogating and addressing the root cause of an issue. This process should apply whether it is an issue in a technical system, a process, or the standards or policies that guided execution. Due to the complexity of causes related to privacy risk, creating a channel of information from the privacy team to the leadership of the organization can help resolve issues where a balance of equities within the organization is in question.

Conclusion

Developing this Privacy Framework is important not only because of the direct output of guidance and associated documentation that NIST is assembling, but also for the opportunity to host a collaborative discussion among diverse stakeholders. We are eager to continue to participate, to share insight based on our experience, and to learn from and engage with other participants. Thank you again for your work and please reach out if you have any questions on the material shared in this comment.

Respectfully submitted,

Lea Kissner
Global Lead of Privacy Technology
Google