From: Kahn, Geoffrey <geoffrey.kahn@accenture.com>
Sent: Wednesday, October 23, 2019 4:41 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Hoffman, Robert <robert.hoffman@accenture.com>; Houston-Carter, R. C. <r.c.houston-carter@accenture.com>; Cooke, Adelina M. <adelina.m.cooke@accenture.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments from Accenture

NIST Team,

Accenture's comments on the Preliminary Draft Privacy Framework are attached. As you will see in the letter and your comment matrix, we are making several significant substantive suggestions and would welcome the opportunity to discuss in person.

Thank you,

Geof

Geof Kahn

Senior Manager for Government Relations (Cyber/Tech)

800 Connecticut Ave, NW Suite 600

Geoffrey.kahn@accenture.com

703-947-1602

This message is for the designated recipient only and may contain privileged, proprietary, or otherwise confidential information. If you have received it in error, please notify the sender immediately and delete the original. Any other use of the e-mail by you is prohibited. Where allowed by local law, electronic communications with Accenture and its affiliates, including e-mail and instant messaging (including content), may be scanned by our systems for the purposes of information security and assessment of internal compliance with Accenture policy. Your privacy is important to us. Accenture uses your personal data only in compliance with data protection laws. For further information on how Accenture processes your personal data, please see our privacy statement at https://www.accenture.com/us-en/privacy-policy.

_____

www.accenture.com

October 24, 2019

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

RE: NIST Privacy Framework: Preliminary Draft Comments

As a leading global professional services company, Accenture provides a broad range of services and solutions in strategy, consulting, digital, technology, security, and operations that span multiple industries. The vast majority of our clients collect, use, share, or otherwise handle personal data. Today, there is a big opportunity for companies to take a more mindful approach to consumer privacy and to design a holistic customer experience while doing so. Consumers do want a better, more customer-focused experience, with 65% willing to share more personal data in return.[1] However, the emergence of legal and regulatory regimes in the European Union (EU) and in a number of U.S. states (e.g. California) and in other countries (e.g. Canada, Brazil, India, and China) complicate company efforts to develop a holistic approach and a balanced strategy to secure and sustain customer trust. That's why handling data responsibly is a fast-emerging component of corporate accountability.

Accenture is grateful for the opportunity to provide input to the Preliminary Draft of the NIST Privacy Framework and we applaud NIST for its longstanding and ongoing contributions to public private partnerships, including the current process on consumer privacy. We have one overarching recommendation – to make the framework more relevant in aiding companies manage their privacy programs and their overall data strategies – and a few operational recommendations that are supplemented by our attached comment matrix.

From the outset, it's clear that the Preliminary Framework was drafted to intentionally mirror the structure of the successful NIST Framework for Improving Critical Infrastructure Cybersecurity. We believe this structural approach in the Preliminary Framework is insufficient to aid American businesses who are seeking tools to help them make informed judgments about what information to collect and how to use it.

There are two primary differences between the Cybersecurity Framework and the Preliminary Privacy Framework. First, the Cybersecurity Framework was developed and exists in a largely unregulated environment for cybersecurity purposes. In contrast, many American businesses large and small are already subject to laws that impact consumer and employee privacy: Consumer data is regulated by a range of laws, such as the EU's General Data Protection Regulation, and soon by the California Consumer Privacy Act. Those, along with a number of sector-specific laws and others designed to protect children, compel many American companies across industries to design and manage their privacy programs around compliance in a complex legal and regulatory environment.

Second, the cybersecurity framework was released with the understanding that cybersecurity tools and capabilities would continue to evolve both in terms of technology and governance, with the latter

[1] https://www.accenture.com/_acnmedia/pdf-110/accenture-see-people-not-patterns.pdf#zoom=50

influenced by changes in the former. As a result, the cybersecurity framework was a valuable tool in getting people to learn foundational terminologies and thus improve the effectiveness of risk management discussions. In our experience, companies have been dealing with a common set of principles on data privacy governance for decades. While the digital economy has increased the volume and velocity of companies' dealings with personal data, the underlying privacy principles and terminology have been broadly understood and have remained largely unchanged.

Together, these negate the potential value of the "tier" component of the Preliminary Privacy Framework as a risk management approach. We believe the "core" and "profile" components remain of high value.

As an alternative to the "tier" component, we recommend the Preliminary Framework be organized around common privacy principles upon which existing laws and regulations and companies' privacy programs are generally based. We recommend categorizing those as: (1) strategy and governance; (2) accountability/stewardship; (3) data use and retention; (4) data lifecycle management; (5) transparency and privacy notices; (6) individual rights; (7) privacy risk management; (8) third-party risk management; (9) data breach management; and (10) other broadly accepted privacy principles.[2]

In line with the above, we believe that the Framework and its users would benefit from the inclusion of language around how to build accountability and stewardship around personal data. The foundations of that domain should include core functions that include: (1) policies and procedures that operationalize the entities' obligations across first and second lines of defense; (2) training and communications to encourage staff and contractors' awareness and adherence to the privacy program; and (3) response and enforcement procedures to address inquiries, complaints, and, where appropriate, breaches of the privacy management program.

At a more operational level, the draft framework includes a thoughtful approach to privacy engineering, but in our engagements across industries we rarely see "privacy engineers." Instead, we most often work with cybersecurity professionals who are asked to implement privacy principles or requirements. We also encounter privacy professionals who work to implement privacy by design, conduct privacy assessments and mitigate against privacy risk by leveraging privacy principles and objectives to implement realistic practical solutions in given business scenarios. There is a need for privacy engineers to advise on the granular administration of data, but we recommend revising privacy engineering to align with privacy objectives and principles in addition to relevant security objectives. Additionally, we believe that the Framework could benefit from further explanations as to how to implement privacy principles by including operational examples and uses cases along with third-party guidelines (e.g. IEEE, Universities, MITRE).

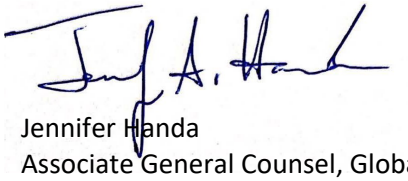
Finally, the Framework would benefit from language around managing privacy in a world where artificial intelligence and machine learning become more ubiquitous and how businesses can leverage those tools to achieve the privacy principles (e.g. identifying uses of data for things other than the originally intended purpose).

Accenture continues to be encouraged by NIST's collaborative approach to developing this framework. We recognize that our recommendations would require a reframing of the document and further

[2] An example of additional privacy principles: *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

engagement with relevant stakeholders. We would welcome the opportunity to discuss our comments at your convenience. Please reach out to Robert Hoffman at robert.hoffman@accenture.com or (703) 947-1019 if you have any questions or would like to discuss our comments and recommendations.

Sincerely,



Jennifer Handa
Associate General Counsel, Global Compliance and Ethics
Accenture

Comment #	Organization Name	Page #	Line #	Section	**Comment** (Include rationale for comment)	Suggested Change	**Type of Comment** (General/Editorial /Technical)
1	Accenture	N/A	N/A	N/A	There are two primary differences between the Cybersecurity Framework and the Preliminary Privacy Framework. First, the Cybersecurity Framework was developed and exists in a largely unregulated environment for cybersecurity purposes. In contrast, many American businesses large and small are already subject to laws that impact consumer and employee privacy: Consumer data is regulated by a range of laws, such as the EU's General Data Protection Regulation, and soon by the California Consumer Privacy Act. Those, along with a number of sector-specific laws and others designed to protect children, compel many American companies across industries to design and manage their privacy programs around compliance in a complex legal and regulatory environment. Second, the cybersecurity framework was released with the understanding that cybersecurity tools and capabilities would continue to evolve both in terms of technology and governance, with the latter influenced by changes in the former. As a result, the cybersecurity framework was a valuable tool in getting people to learn foundational terminologies and thus improve the effectiveness of risk management discussions. In our experience, companies have been dealing with a common set of principles on data privacy governance for decades. While the digital economy has increased the volume and velocity of	As an alternative to the "tier" component, we recommend the Preliminary Framework be organized around common privacy principles upon which existing laws and regulations and companies privacy programs are generally based. We recommend categorizing those as: (1) strategy and governance; (2) accountability/stewardship; (3) data use and retention; (4) data lifecycle management; (5) transparency and privacy notices; (6) individual rights; (7) privacy risk management; (8) third-party risk management; (9) data breach management; and (10) other broadly accepted privacy principles. (e.g. the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)	General
2	Accenture	N/A	N/A	N/A	Overall, the framework lacks a forward-thinking component that deals with managing privacy in a world with ubiquitous use of artificial intelligence/machine learning (AI/ML) and other emerging technologies.	We recommend thinking about how to include emerging technologies like AI/ML into the framework.	General

3	Accenture	N/A	N/A	ID.DE-P	The framework has a section on Data Processing Ecosystem Risk Management but only two references to the cloud. In a environment where we are increasingly relying on cloud and third parties—clients have to be very attentive about how they manage their processes and information in the cloud .	We recommend ID.DE-P or the explanatory language add more context and tools for implementing privacy within a cloud environment. Some suggested additions are (1) Due diligence questionnaires beforehand; (2) Contractual responsibilities for managing the data; (3) Monitoring and auditing the privacy practices of the cloud and 3rd party providers;	Editorial
4	Accenture	N/A	N/A	CT.DM-P	The framework would benefit from a section on deidentification, minimization, and aggregation.	Recommend section CT.DM-P include references to deidentification, minimization, aggregation--describing them, their purposes, and examples of how they could be used as part of a privacy program.	Technical
5	Accenture	N/A	N/A	3.2	The document generally discusses accountability as a risk management exercise in the context of the framework but does not reflect the broader and more fundamental role of accountability as defined in GDPR, and organizations would benefit from consistence between the Framework and GDPR in how these terms are being used.	We recommend reworking the accountability section to more clearly reflect the elements of accountability as defined in GDPR, and include policies and procedures that operationalize the entities' obligations.	General
6	Accenture	15	526	3.4	The System Development Life Cycle (SDLC) reference for systems feels out of touch with the process of change in sophisticated organizations.	The Financial Servicse industry and a growing number of firms in other sectors have shifted away from SDLC to "agile", which is effectively where business and IT collaborate on development far earlier in the process to test, learn and refine their procesess. We recommend focusing on "agile" since leading companies are moving beyond SDLC.	Technical

7	Accenture	8	261	1.2.2	We have two comments about section 1.2.2. which talks about sharing and transfering privacy risk: (1) Consent is not necessarily an effective mechanism to transfer privacy risk. Rather, it has often been used in a mechanical way to shift the burden to individuals without offering consumers real choice, and to avoid investments and accountable practices of the organization. (2) Companies are not effectively sharing privacy risk when they contract with service providers. This is true legally under GDPR but also the case as a general pinciple. For example, when companies hire a vendor or sub processor, they are responsible for the actions of those providers, so risks are in fact accumulated.	Recommend characteriznig these issues as actions companies can take as part of the nexus between privacy risk management and risk assessment but removing the concepts of transfering or sharing privacy risk with these actions.	Technical
8	Accenture	6	208	1.2.1	The venn diagram does not account for things like cyber attacks and other extended privacy risks	We recommend rethinking the venn diagram on page six to consider the malicious and/or irregular activities associated with privacy risks.	Technical
9	Accenture	5	173	1.1	The examples under the Control Function are at a policy level and should be part of the Governance function. We expect granular key control activities as part of the Control function.	We recommend moving the examples list to the Governance Function.	Technical
10	Accenture	20	683	Appendix A	The categories under the Control Function are limited. There are various key privacy controls across the privacy compliance domains which should be included as categories under the Control function.	We recommend adding the following: (1) Strategy and Governance; (2) Individual Rights; (3) Privacy Notice; (4) Data Use and Retention; (5 Privacy Risk Management; (6) Data Lifecycle Management; (7) Data Breach Management; (8) Third Party Risk Management..	Technical