From: Erica Silva
Sent: Thu 24 October 2019 20:21
To: privacyframework@nist.gov
Cc: Sharad Patel <Sharad.Patel@PACONSULTING.COM>; Harry Bowen <Harry.Bowen@PACONSULTING.COM>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Hi,

Please find attached comments from PA Consulting.

With best regards,

Erica

Erica Silva

PA Consulting Group | 10 Bressenden Place, London SW1E 5DN, United Kingdom

M: +44 7971829664 | paconsulting.com
Follow us | Twitter | LinkedIn

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)
1	PA Consulting	Erica Silva				This framework allows for a common approach that helps communicate and formalise Privacy Risk Management. At the same time, it is flexible enough to be used in all sectors, in a variety of business and regulatory contexts, and by small to large organisations. It is a much needed start to a common approach that for sure will evolve as organisations start testing and mapping to technical standards.		General
2	PA Consulting	Erica Silva				Not all data/information will have Privacy risk associated to them. Throughout the framework there is no reference of the fact that Privacy is the management and protection of personal data/personal information. This is a key pre-requisite for generating privacy risk, and it is surprising that the framework does not mention and/or define personal data/personal information.		General
3	PA Consulting	Harry Bowen	3	82		Data flows "through a complex ecosystem - so complex that individuals may not be able to understand the potential consequences for their privacy". I do not think this quite captures the issue. In actuality, the vast majority of individuals do not understand the impact to their privacy. Needs to be worded stronger to adequately frame the issue.		General
4	PA Consulting	Harry Bowen	6	206-214		These lines explain the difference between Privacy Risk and Cyber Security Risk. However, the most obvious difference is not highlighted; namely that privacy risk pertains to personal information that could never interact with anything Cyber i.e. technology, software, infrastructure or even technology hardware. This is the most distinguishing difference between the two and yet it is barely alluded to in this section.		
5	PA Consulting	Harry Bowen	11	381-396		There needs to be mention here, and explicit reference to, the proportionality of response to a privacy risk. When comparing profiles, particularly between as is and to be, it is critical to consider the proportionality of response to any given privacy risk. Using profiles would be a great way to articulate movement in privacy risk appetite, but this movement needs to be tempered by a proportionate response.		
6	PA Consulting	Harry Bowen	12	431-432		It's rightly pointed out that organisations should not look to 'comply' with the framework. But the point is left there and not elaborated further. I would expand this and explain that organisations "should like to flexibly apply the framework" in order to generate value through its use. In effect, summarise in one or two lines, sections 3.1-3.6.		

7	PA Consulting	Harry Bowen	14	446-449		This section describes how organisations "might collaborate with technology leaders and/or standards bodies to draft, develop, and coordinate standards guidelines and practices". This is a really key point and should be emphasised further by highlighting the shift in recent years to both principle based and standards based approaches to privacy. This will likely substantially increase in the near future and should be highlighted here.		
8	PA Consulting	Harry Bowen	16	545-595		A key way to use the Framework in this section is its ability to help define the 'data ecosystem'. However, there is no reference to international data transfers in this section. These transfers are often one of the highest risk areas of privacy compliance, particularly when combined with supplier outsourcing. Yet there is no mention of this in this section.		
9	PA Consulting	Harry Bowen	21		ID.IM-P	Contains no reference to classification/categorisation of inventoried and mapped personal data. Arguably any future activity cannot take place until the inventoried and mapped data is categoriesed/classified because without that occurring, there is incomplete information to prioritise based on risk.		
10	PA Consulting	Harry Bowen	22		ID.RA-P1	Key point missing from here is the importance of factoring in geographical location of processing into contextual factors. What countries and physical locations a business operates in will massively impact the context and correspond impact the risk assessment of privacy risk.		