From: Chahiti Asarpota <casarpota@forrester.com>
Sent: Thursday, October 24, 2019 5:00 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Heidi Shey <hlo@forrester.com>; Fatemeh Khatibloo <fkhatibloo@forrester.com>; Elsa Pikulik <epikulik@forrester.com>; Conor McCormick <cmccormick@forrester.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments

To Whom It May Concern,

Please find attached Forrester's comments on the NIST Privacy Framework as well as a cover letter and some relevant research. Please feel free to reach out if you have any questions.

Regards,

Chahiti Asarpota

FORRESTER
Challenge thinking. Lead change.

Chahiti Asarpota

Research Associate Serving B2C Marketers

Direct +1 (617)-613-6861 | casarpota@forrester.com

Forrester Research, Inc.
Forrester.com | Communities | Blogs | Twitter | LinkedIn | Facebook | Google+

60 Acorn Park Drive, Cambridge, MA 02140 United States

FORRESTER®

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

Forrester is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop consumer strategies that drive growth. Our unique insights are grounded in annual surveys of more than 675,000 consumers and business leaders worldwide, rigorous and objective research methodologies, and the shared wisdom of our most innovative clients. Through proprietary research, analytics, consulting, and advisory, we have a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations.

We appreciate the opportunity to provide comments on the September 2019 draft of NIST's Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management. This work comes at a critical moment:

- Consumer concerns about privacy are at an all time high. Our research shows that 73% of US online adults are concerned that their personal information is being permanently recorded and made accessible to businesses without their consent or knowledge. This figure is up 15 points from 2016.
- Privacy teams in organizations of all sizes are under-resourced for the challenges they face, as cited in our attached report, "Build Your Privacy Organization For Customer Data Management."
- The pace of regulatory change is unprecedented. For example, Europe's General Data Protection Regulation has effectively become a trade tariff: Japan's trade agreement with the EU required it to achieve adequacy with GDPR. In the US, the California Consumer Privacy Act will materially change organizations' ability to collect consumer data, forcing firms to up-level their privacy programs in order to maintain trust and access to critically important personal information

About Forrester's B2C Consumer Privacy Practice
The customer privacy practice at Forrester is led by Vice President & Principal Analyst Fatemeh Khatibloo, CIPM. This research encompasses major themes of customer trust, GDPR, CCPA, and other privacy regulations, preference management, identity management, and the global consumer data ecosystem. Forrester's privacy research answers vital questions about consumer data: what is can help businesses do, where and how it is best collected, and to use it ethically. This research helps CMOs empower customers with meaningful choices while simultaneously building trust.

About Forrester's Data Security And Privacy Practice
The data security and privacy practice at Forrester is led by Principal Analyst Heidi Shey and Senior Analyst Enza Iannopollo, CIPP/E. Data is the lifeblood of today's digital businesses. The goal of the research is to guide security and risk professionals through major changes to processes for data policy development, inventory, classification, and protection, and identifies the technologies and services that will help design and implement effective data security while enforcing privacy policy.

Attached, please find three relevant research reports, as well as our comments to the full draft dated September 6, 2019.

Sincerely,

Fatemeh Khatibloo, CIPM
VP, Principal Analyst

Heidi Shey
Principal Analyst

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section
1	Forrester Research	Heidi Shey hshey@forrester.com	3	82-83	Exec Sur
2	Forrester Research	Heidi Shey hshey@forrester.com	3	95	Exec Sur
3	Forrester Research	Heidi Shey hshey@forrester.com	4	122	1
4	Forrester Research	Heidi Shey hshey@forrester.com	4	149	1
5	Forrester Research	Heidi Shey hshey@forrester.com	6	Figure	1.2.1
6	Forrester Research	Heidi Shey hshey@forrester.com	6	Data A	1.2.1

Comment #	**Comment** (Include rationale for comment)
1	Current language is focused on consequences: "Individuals may not be able to understand the potential consequences for their privacy as they interact with systems, product, and services."
2	Regarding facilitating communication
3	Current language states that benefits are "fueled by data about individuals" is limiting, and readers may view this scope of personal data as data provided by an individual when we are fast entering a world where more and more machines/devices (internet of things) are also generating or collecting and storing data that can be associated with an individual.
4	In saying that the Framework is to encourage cross-organization collaboration, readers may interpret this type of collaboration as an optional practice.
5	In the venn diagram, privacy breach is at the intersection of cybersecurity risks and privacy risks to demonstrate the overlap.
6	Love how the definition of data action takes into account the data lifecycle, all the way to disposal.

Comment #	Suggested Change	Type of Comment (General/Editorial/Technical)
1	Not just understand potential consequences for privacy, but also understand the impact of their input in this ecosystem, such as what personal data is collected, how its used, for how long, and why (including whether third-parties have access).	General
2	Call out facilitating communication among employees in the organization too, rather than having it be implied in the prior two bullets.	General
3	Perhaps a sentence that acknowledges this changing environment, pointing to examples like robot vacuums, connected cars, etc. A researcher (Dennis Giese) at Defcon 2019 purchased several used and factory reset robot vacuums, and demonstrated how he was able to pull personal data like the name of a home wifi network and locate home address despite doing multiple factory resets.	General
4	Rather than encourage something that is required for success, call out cross-organization collaboration as a requirement, where the Framework provides a structure to enable cross-organization collaboration.	General
5	Given the focus on ethics as a part of privacy too, a "trust breach" would also be at this intersection alongside privacy breach. A trust breach is fundamentally different from a privacy breach or a data breach, and primarily driven by an unethical use of data.	General
6	No change here, but something that could be useful to note elsewhere (roadmap? Appendix?) would be what "disposal" means or entails, particularly secure disposal. In the wake of GDPR, I've found that technology vendors can have very loose interpretations regarding disposal to support the right to be forgotten; one vendor claimed that by masking the data from view from employees in a database, it was "deleted" since it was not visible/usable.	General

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section
7	Forrester Research	Heidi Shey hshey@forrester.com	11	405	2.3
8	Forrester Research	Heidi Shey hshey@forrester.com	11	406-40	2.3
9	Forrester Research	Heidi Shey hshey@forrester.com	18	644	Appendi
10	Forrester Research	Heidi Shey hshey@forrester.com	21	ID.IM-P	Table 2
11	Forrester Research	Heidi Shey hshey@forrester.com	21	ID.IM-P	Table 2

Comment #	Comment (Include rationale for comment)
7	Why do the tiers not represent maturity levels? The use of the term "tier", language of the tiers, and structure of tiering itself, shows a clear progression of maturity. The Profiles also contribute to the sense that is about maturity.
8	The statement about how some organizations may never need to achieve Tier 3 or 4 or may only focus on certain areas of these tiers can be misleading.
9	Mentions that the Core "encourages" cross-organization collaboration.
10	For inventory and mapping, as is, the subcategories appear to support a snapshot, point in time.
11	Seeking clarification. Would any of these subcategories account for data minimization? Or account for determining the useful lifecycle of data?

Comment #	Suggested Change	**Type of Comment** (General/Editorial/Technical)
7	Call it what it is: maturity. In the following paragraph describing how an organization can use the tiers, describes how a maturity model would be used (assess current state, prioritize next efforts, address gaps).	General
8	Suggest deletion to avoid confusion, as some may read this as an "out" without considering broader context. The prior paragraph already acknolwedges that an organiation should consider its risk management practices. And immediately after the statement in lines 407/408 also defines appropriateness.	General
9	Change "encourages" to "requires" and remove "Ideally," since cross-organization collaboration is built into the Core (Govern-P).	General
10	Add a subcategory that addresses change, to account for changes to the environent, introduction of new processes, etc that would require an update to inventory and mapping. If not a new subcategory, then language to indicate when rather than have readers assume this is a one time activity. As much as we'd like for people not to treat this as a checklist, it invariably will be used as one by some organizations.	General
11	When looking at the purpose of for data actions (ID.IM-P5), assessing data minimization and the useful lifecycle of data could be an adjacent activity to determine if too much data is being collected for that purpose, and determine when that data is no longer useful and should be disposed of. Or is data minimization and determination of useful lifecycle covered under ID.IM-P6? Please clarify.	General

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section
12	Forrester Research	Heidi Shey hshey@forrester.com	24	Contro	Table 2
13	Forrester Research	Heidi Shey hshey@forrester.com	25	CT.DP-I	Table 2
14	Forrester Research	Heidi Shey hshey@forrester.com	25	CM.PP-	Table 2
15	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	5		
16	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	7	248	1.2

Comment #	**Comment** (Include rationale for comment)
12	The naming of function Control-P seems misplaced.
13	Love how Disassociated Processing is included here!
14	As written, CM.PP-P1 is missing organizational alignment. I've run into organizations where one group (usually legal) has fulfilled the actions in this subcategory, but the rest of the organization does not know what has been established as policy, processes, procedures, and communicated to customers. This also illustrates the requirement for and importance of cross-organizational collaboration.
15	We applaud NISTs alignment of the Privacy Framework with the Cybersecurity Framework. Too often, we find that enterprises and consumers conflate security and privacy, without understanding how they are different but equally necessary.
16	As a follow on to the comment above, we recommend a section on the interplay of privacy risk against other business operational risks -- for example, business continuity risk, sectoral privacy risk, etc.

Comment #	Suggested Change	Type of Comment (General/Editorial/Technical)
12	Control-P, based on the description of categories and subcategories, seems like it would be better described as Manage-P. This function is more about data management. Control also has data security control connotations, and could be confused with Protect-P.	General
13	No change here, but a comment about guidance. Will there be additional guidance in an appendix? CT.DP-P1 through P3 are all areas where many organizations will likely struggle.	General
14	Include language that states that these actions are also aligned with or audited against actual procedures and controls. This is to help ensure that what is communicated is what is actually happening and supported behind the scenes.	General
15	n/a	General
16	Include a section 1.2.x explaining the "venn" of business and privacy risk	General

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section
17	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	6	203	Fig 2
18	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	7	256	1.2.2
19	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	7	239	1.2.1
20	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	8	261	1.2.2
21	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	29	687	Appendi
22	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	30	687	Appendi
23	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	35	Table 5	Appendi

Comment #	**Comment** (Include rationale for comment)
17	Privacy risk is currently defined as being "associated with unintended consequences of data processing." While "data processing" is later defined as the "collective set of data actions" we believe business users will better understand the definition of privacy risk if the word "use" is also included.
18	We find that many organizations' approach to privacy risk can also be the result of a lack of understanding of true risk.
19	The term "problematic data action" is important to define
20	Privacy professionals have broadly acknowledged that notice and consent are insufficient mechanisms for sharing risk with individuals due to the nature of how they are displayed and executed.
21	The term "category" may create confusion as it is used in several regulations (CCPA & GDPR) to describe the types of data collected about individuals
22	The term "individual" does not sufficiently capture the entirety of data types that are of concern in a privacy framework or risk assessment
23	The defintion of "Disassociability" may be insuffcient as an objective due to the proliferation of mechanisms for reidentification of data and events to an individual or device

Comment #	Suggested Change	Type of Comment (General/Editorial/Technical)
17	Change the right hand circle of Fig 2 to read "Privacy Risks associated with unintended consequences of data processing and data use"	Editorial
18	Organizations may choose to respond to privacy risk in different ways, depending on the potential impact to individuals and resulting impacts to organizations. In some cases, organizations' response may be affected by a lack of understanding of their true privacy risk.	General
19	Add "problematic data action" to the Glossary, or provide some examples or general explanation in the body of the text	Editorial
20	Suggest either calling out these historically used mechanisms as being insufficient to transfer risk in the current digital ecosystem; alternatively, remove this clause from the risk transfer bullet entirely and call out "human readable privacy notices and meaningful choice" as an action in Profiles	Technical
21	It may be worth adding a footnote or explanation that the word "category" here is used differently than in the aforementioned regs	Technical
22	Add a definition for "personal information" to the glossary. The definition should include "data that can reasonably be connected to an individual, including digital signals, device identifiers, observed behaviors, biometrics, etc"	Technical
23	"Enabling and enforcing the processing of data without association to individuals or devices when appropriate, and ensuring that these individuals or devices cannot be reidentified or reverse engineered using mathematical or machine learning mechanisms."	Technical

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section
24	Forrester Research	Fatemeh Khatibloo fkhatibloo@forrester.c	37	855	Appendi

Comment #	**Comment** (Include rationale for comment)
24	Business environment is only one element of change that organizations must monitor

Comment #	Suggested Change	**Type of Comment** (General/Editorial/Technical)
24	"An organization monitiors how changes in its business environment, cultural norms, individuals' expectations, and technological advances may be affecting its privacy risk across its systems, products, and services, and iteratively use the practicies in this appendix to adjust accordingly."	