From: Lydia Wright <lydia.wright@equifax.com>
Sent: Thursday, October 24, 2019 7:38 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Nick Oldham <nicholas.oldham@equifax.com>; Kyle Brown <kyle.brown2@equifax.com>
Subject: Equifax Comments to Draft Framework

Please see attached.

Thanks!

Many thanks,

Lydia Wright

EA to Nick Oldham, Chief Privacy and Data Governance Officer

o 470.373.2068 • m 404.291.8084

lydia.wright@equifax.com

EQUIFAX

October 24, 2019

Katie MacFarland
National Institute of Standards and Technology,
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
Submitted electronically to privacyframework@nist.gov

NIST Privacy Framework: Preliminary Draft Comments

Equifax would first like to take the opportunity to thank NIST, specifically those who have devoted substantial time and effort to developing the Privacy Framework. We recognize that this has been an intensive process with the goal of developing a methodology for all industries to improve the way that we talk about privacy, measure privacy risks, and address those risks through a defined, flexible, organization-specific methodology. We appreciate the opportunity to provide feedback to NIST on the preliminary draft and continue the robust discussion NIST has been engaged in with stakeholders. To that end, we have identified four areas of the NIST Privacy Framework Preliminary Draft (the "Framework") which we believe should be expanded upon, clarified, or modified. These areas are:

EQUIFAX

Mapping the Privacy Framework Core to Corresponding Cybersecurity Framework Core Elements

The preliminary draft note to reviewers invites commentators to discuss whether the privacy framework "enables[s] organizations to use the Privacy Framework in conjunction with the Framework for Improving Critical Infrastructure Cybersecurity to collaboratively address privacy and cybersecurity risks." While the Framework core uses shaded boxes to indicate where core functions, categories, and sub-categories are either identical to or similar to functions, categories, and sub-categories, the exact mapping is left to the implementer to ascertain. While many of the identifiers of similar core components are equivalent (merely with a '-P' added for the privacy framework core components), some of the similar core components identifiers are not.

Based on our review, we believe the following chart represents the mapping between equivalent and similar components of the privacy framework core and the cybersecurity framework core. NIST is, of course, invited to check that the mappings match what was intended.

PF Subcategory	CSF[1]
ID.BE-P1: The organization's role in the data processing ecosystem is identified and communicated.	**ID.BE-1**
ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	**ID.BE-3**
ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	**ID.RA-4** **ID.RA-5**
ID.RA-P5: Risk responses are identified, prioritized, and implemented.	**ID.RA-6**
ID.DE-P1: Data processing ecosystem risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	**ID.RM-1** **ID.SC-1**
ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.	**ID.SC-2**
ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	**ID.SC-3**
ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual or framework obligations.	**ID.SC-4**
GV.PP-P1: Organizational privacy values and policies (e.g., conditions on data processing, individuals' prerogatives with respect to data processing) are established and communicated.	**ID.GV-1**
GV.PP-P3: Roles and responsibilities for the workforce are established with respect to privacy.	**ID.AM-6**
GV.PP-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	**ID.AM-6**

[1] Throughout this document we will refer to the NIST Framework for Improving Critical Infrastructure Cybersecurity as the "CSF".

GV.PP-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	**ID.GV-3**
GV.PP-P6: Governance and risk management policies, processes and procedures address privacy risks.	**ID.GV-4**
GV.RM-P1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	**ID.RM-1**
GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.	**ID.RM-2**
GV.RM-P3: The organization's determination of risk tolerance is informed by its role in the data processing ecosystem.	**ID.RM-3**
GV.AT-P1: The workforce is informed and trained on its roles and responsibilities.	**PR.AT-1**
GV.AT-P2: Senior executives understand their roles and responsibilities.	**PR.AT-4**
GV.AT-P3: Privacy personnel understand their roles and responsibilities.	**PR.AT-5**
GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	**PR.AT-3**
CT.PO-P4: An information life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.	**PR.IP-2**
CT.DM-P5: Data are destroyed according to policy.	**PR.IP-6**
CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	**PR.PT-1**
PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	**PR.AC-1**
PR.AC-P2: Physical access to data and devices is managed.	**PR.AC-2**
PR.AC-P3: Remote access is managed.	**PR.AC-3**
PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**PR.AC-4**
PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	**PR.AC-5**
PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	**PR.AC-6**
PR.DS-P1: Data-at-rest are protected.	**PR.DS-1**
PR.DS-P2: Data-in-transit are protected.	**PR.DS-2**
PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	**PR.DS-3**
PR.DS-P4: Adequate capacity to ensure availability is maintained.	**PR.DS-4**
PR.DS-P5: Protections against data leaks are implemented.	**PR.DS-5**
PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**PR.DS-6**
PR.DS-P7: The development and testing environment(s) are separate from the production environment.	**PR.DS-7**
PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	**PR.DS-8**
PR.DP-P1: A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	**PR.IP-1**

PR.DP-P2: Configuration change control processes are established and in place.	**PR.IP-3**
PR.DP-P3: Backups of information are conducted, maintained, and tested.	**PR.IP-4**
PR.DP-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	**PR.IP-5**
PR.DP-P5: Protection processes are improved.	**PR.IP-7**
PR.DP-P6: Effectiveness of protection technologies is shared.	**PR.IP-8**
PR.DP-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	**PR.IP-9**
PR.DP-P8: Response and recovery plans are tested.	**PR.IP-10**
PR.DP-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	**PR.IP-11**
PR.DP-P10: A vulnerability management plan is developed and implemented.	**PR.IP-12**
PR.MA-P1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	**PR.MA-1**
PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	**PR.MA-2**
PR.PT-P1: Removable media is protected and its use restricted according to policy.	**PR.RT-2**
PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	**PR.PT-3**
PR.PT-P3: Communications and control networks are protected.	**PR.PT-3**
PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	**PR.PT-5**

Privacy Breaches

The Framework uses the term "privacy breach" to describe situations where there is a loss of confidentiality, integrity, or availability of data due to unauthorized access or unauthorized use.[2] The Framework distinguishes a privacy breach from a problematic data action by noting that problematic data actions are those that are authorized, but result in unintended consequences from data processing while privacy breaches are the result of some unauthorized access or use of information. As indicated by Figure 8, a privacy breach is a situation that can be addressed by controls in both the Framework and the CSF, and at least appears to be akin to what the CSF calls a "cybersecurity incident." We believe it is telling that the word "breach" is absent from the CSF. The term "breach" invokes the concept of data breach and the corresponding state data breach notification laws, which may not be applicable to these situations.

Recommendation: Replace the term "privacy breach" with "privacy incident."

[2] NIST Privacy Framework Preliminary Draft, September 6th, 2019 ("Framework"), at lines 233-35. See also Appendix B at page 30, defining "Privacy Breach."

Methodology for Target Profile Determination

NIST clearly recognizes the danger that organizations will merely implement the Core as a checklist of activities rather than developing target profiles aligned to identified business and privacy risks.[3] NIST asked whether the Framework can be "be inclusive of, and not disruptive to, effective privacy practices in use today." Equifax believes it can be inclusive of existing practices. Many of the Framework's components are already part of common privacy program activities. The benefit of the Framework is that it can act as a guide for privacy program development in a risk informed way by setting guideposts for privacy professionals to consider and understand privacy risks and, more importantly, how to design a program to mitigate those risks.

NIST invites organizations to consider their "business requirements, risk tolerance, privacy values, and resources" when developing target profiles. Equifax believes that further guidance in these areas would be helpful to guard against the checklist approach to core implementation.

Recommendation: Provide additional guidance on how to derive relevant privacy outcomes from business objectives (see Business Requirements below), risk tolerance, privacy values, and resources—more specific recommendations for each are provided below. We recommend NIST also add an additional factor, namely compliance obligations. Many of the privacy outcomes may be required by law or regulation to have some form of implementation and, thus, organizations will need to consider their compliance obligations in articulating privacy outcomes for their target profile.

Business Requirements

Properly ascertaining the business requirements that may implicate privacy interests of individuals is fraught with risks. Chief among them is that businesses may state a requirement that entails certain privacy risks, rather than a business objective that allows for methods of achieving the objective without incurring the privacy risks. For example, one might suggest that a business requirement is "to collect prospect information for marketing purposes." This requirement creates privacy risks. A better approach is to begin with the end in mind; in other words, focus on the objective. The business objective is "to improve sales," or more narrowly "to connect with prospects." Whereas the former (requirements) creates privacy risks that must be managed, the latter (objectives) allows for a more flexible, risk-based implementation to achieve business objectives. Further, when selecting and particularizing privacy outcomes, the question can be posed, does this privacy outcome support business objectives or impede those objectives.

Recommendation: replace "business requirements" with "business objectives" throughout.

Risk Tolerance

Risk tolerance is something that the transportation industry has dealt with since its inception. Zero tolerance for risk would kill the automobile, airline, and railroad industries. Why do we accept risk

[3] Framework at lines 622-24 ("The Subcategories should not be read as a checklist in isolation from their Categories, which often provide a risk-based modifier on Subcategory selection.").

in these areas? We realize the social benefits of efficient travel may outweigh the risks. Unfortunately, measuring and communicating risk tolerance for privacy risks is not a well-developed field. We believe that by including guidance on how to articulate risk tolerance in the creation of target profiles, NIST can help advance and improve the industry's ability to make risk-based privacy decisions.

While some privacy risk tolerance will be subsumed in an organization's decision to exclude certain privacy values from their privacy program, others will need to be explicitly identified when business objectives, resources, and privacy values exhibit tension. Consider software designed to monitor chat room activity to promote civility amongst participants. Because of the sensitive nature of the chat room's subject (such as discussing a medical condition), a privacy value the software developer wants to support is anonymity. The need to identify participants to prevent trolling might have a chilling effect, altering behavior and resulting in participant abandonment. Having 10% of potential participants either abandon or fail to use the service might be an acceptable risk to identify and remove trolls. Having 90% of potential participants abandon the service, however, would be an unacceptable risk. This might impact a decision on the target profile as such.

Factors used to create target profile	Sub-category	Target Profile
Business Objective: prevent trolling **Privacy Value:** anonymity **Risk Tolerance:** 10% abandonment	**CT.DP-P2:** Data are processed to limit the identification of individuals (e.g., differential privacy techniques, tokenization).	Systems use randomly assigned pseudonyms to identify accounts

Contrast this to another organization that has a much higher risk tolerance for abandonment by customers which thus allows a much weaker form of identification protection.

Factors used to create target profile	Sub-category	Target Profile
Business Objective: prevent trolling **Privacy Value:** anonymity **Risk Tolerance:** 40% abandonment	**CT.DP-P2:** Data are processed to limit the identification of individuals (e.g., differential privacy techniques, tokenization).	Systems use first names only to identify accounts

By articulating risk tolerance, organizations can have discussions internally, or with leadership, regulators or other stakeholders about the appropriate levels of risk tolerance.

Recommendation: NIST should expand on its guidance explaining the role of risk tolerance in the development of target profiles.

Privacy Values

While NIST touches on privacy values in the introductory section, we recommend more be done to suggest how organizations should think about privacy values or how those values relate to privacy outcomes. While organizations may be encouraged to develop their own set of privacy values, the concept of a privacy value is often confused with privacy outcomes or privacy principles; therefore, guidance

from NIST around the contours of privacy values may be helpful. There are many normative models for privacy which organizations can consider and customize to articulate their privacy values; we've illustrated a few of those in the chart below.[4] Of course, like the core itself, we would not expect these models to act as checklists for organizations in developing their privacy values; instead, we believe it is important for NIST to provide guidance on how to think about privacy values and how to distinguish them from privacy principles and privacy outcomes in the context of an organization's unique business, regulatory, and consumer environment.

Recommendation: Provide more robust description of privacy values and how those privacy values might be used to identify target profile Core activities and/or be mapped to categories or sub-categories.

<table>
<tr><th colspan="2">Privacy Values</th><th colspan="3">Privacy Harms</th></tr>
<tr><th>Hartzog</th><th>Westin</th><th>Prosser</th><th>Calo</th><th>Solove</th></tr>
<tr><td>Obscurity, Trust, Autonomy</td><td>Solitude, Intimacy, Anonymity, Reserve</td><td>Intrusion upon Seclusion, Public Disclosure, False Light, Appropriation</td><td>Subjective and Objective Harms</td><td>Information Dissemination, Information Processing, Collection, Invasion</td></tr>
<tr><td rowspan="6">Obscurity - when information and people are hard or unlikely to be found or understand, people are relatively safe and rely on that risk calculus</td><td rowspan="4">Reserve is the "creation of a psychological barrier against unwanted intrusion"; this creation of a psychological barrier requires others to respect an individual's need or desire to restrict communication of information concerning him or herself.</td><td>Public disclosure of embarrassing private facts;</td><td rowspan="3">Objective Unanticipated or coerced use of information</td><td>INFORMATION DISSEMINATION – Disclosure involves the revelation of truthful information about a person that impacts their security or the ways others judge their character</td></tr>
<tr><td></td><td>INFORMATION DISSEMINATION – Exposure revealing another's nudity, grief, or bodily functions</td></tr>
<tr><td>Appropriation of name or likeness.</td><td>INFORMATION DISSEMINATION – Appropriation using a data subject's identity to serve the aims and interests of another</td></tr>
<tr><td rowspan="3">Intrusion upon seclusion or solitude, or into private affairs</td><td rowspan="4">Subjective Perception of unwanted observation (using a liberal definition of observation)</td><td>COLLECTION – Surveillance watching, listening to, or recording of an individual's activities</td></tr>
<tr><td>COLLECTION - Interrogation questioning or probing for information</td></tr>
<tr><td>Solitude is a physical separation from others</td><td>INVASION – Intrusion invasive acts that disturb one's tranquility or solitude</td></tr>
<tr><td>Anonymity is the "desire of individuals for times of 'public privacy.'"</td><td></td><td>INFORMATION PROCESSING – Identification the linking of information to a particular individual</td></tr>
<tr><td></td><td></td><td>INFORMATION PROCESSING – Aggregation the combination of various pieces of information (over sources or time)</td></tr>
</table>

[4] Hartzog's three pillars (Autonomy, Trust and Obscurity) and Westin's four states of privacy (Reserve, Anonymity, Solitude and Intimacy) represent positive aspirational values to extol. Prosser, Calo and Solove's models each provide harms to be avoided.

				INFORMATION DISSEMINATION - Increased Accessibility amplifying the accessibility of information
Trust - willingness to become vulnerable to the actions of another	**Intimacy** is a "close, relaxed, and frank relationship between two or more individuals" that results from the seclusion of a pair or small group of individuals.			**INFORMATION DISSEMINATION - Breach of Confidentiality** breaking a promise to keep a person's information confidential
				INFORMATION PROCESSING - Secondary Use information collected for one purpose is used for another purpose
				INFORMATION PROCESSING – Insecurity carelessness in protecting information from leaks or improper access
Autonomy - freedom to develop reliable and sustainable relationships of trust and create and maintain zones of obscurity (freedom from external interference)				**INVASION - Decisional Interference** incursion into the individuals decision regarding their private affairs
			Objective Unanticipated or coerced use of information	**INFORMATION PROCESSING – Exclusion** failure to let a data subject know about the data that others have about her and participate in its handling or use
				INFORMATION DISSEMINATION – Blackmail threat to disclose personal information
		Publicity which places a person in a **false light** in the public eye		**INFORMATION DISSEMINATION – Distortion** dissemination of false or misleading information about individuals

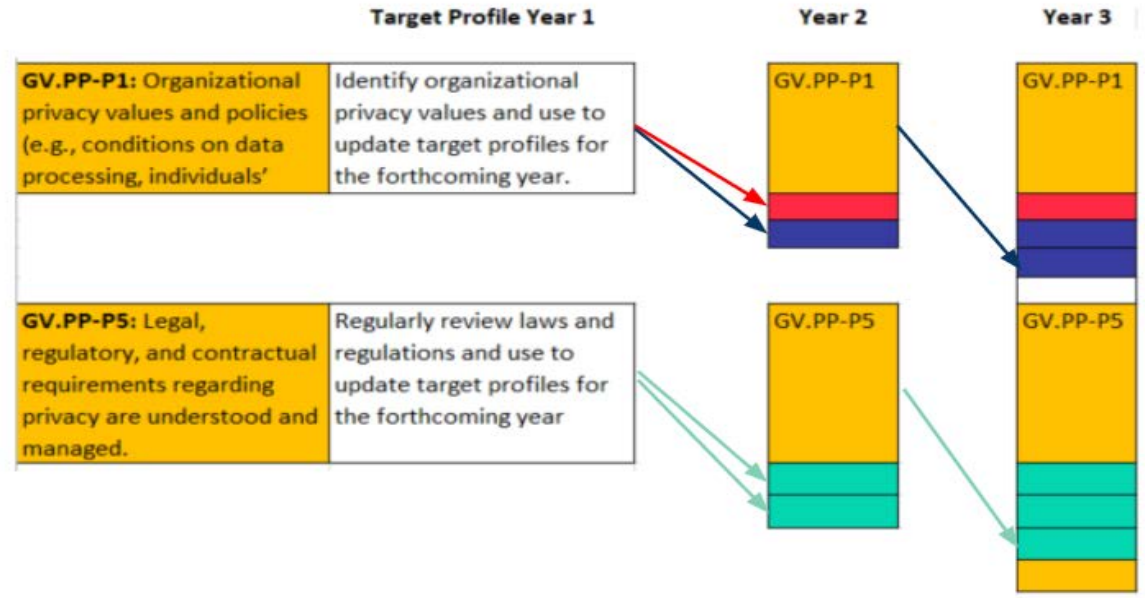
Resources

Availability of resources necessarily has an influence on the ability of an organization to achieve certain privacy outcomes. Keeping all removable media in an evidence locker style system requiring approval of an oversight board for removal and use might satisfy **PR.PT-P1** (Removable media is protected and its use restricted according to policy) but it is extremely resource intensive and may not be necessary. Determining a target profile is partially about identifying what the organization can reasonably achieve given available resources. But target profiles could also be used to demonstrate where the organization would like to be in the future or where it could be given additional resources. Target profiles could also act as a vehicle to demonstrate how different resource allocations may result in different privacy outcomes across the organization's privacy program. In that respect, the target profile can play multiple roles.

Recommendation: Provide additional guidance on the roles that target profiles play vis-à-vis resources. Whether it is a roadmap from which the privacy program requests funding, an end-goal given realistic availability of funding, or a way to demonstrate how resources can be allocated to achieve different goals, NIST should provide some examples of how the profiles can be used in advancing privacy controls at an organization. This would help provide additional context to business stakeholders on why target profiles are an important tool in the privacy practitioner's arsenal.

Compliance Obligations

It is difficult in today's regulatory environment to develop a robust privacy program that does not consider an organization's compliance obligations. Because target profiles can be used as a road-map for how an organization wants to improve its privacy program over time, there is an opportunity for organizations to use target profiles to help manage compliance efforts. While compliance obligations are also part of the Core activities (GV.PP-P5), they necessarily play a part in identifying and prioritizing core outcomes as well. This is similarly true for privacy values. GV.PP-P1 requires that organizational privacy values be established and communicated. As previously discussed, privacy values constitutes a primary source of determining an organization's target profile. This suggests that target profiles could represent a continuous evolution of the organization.



Equifax realizes that the Framework is not meant to be a compliance tool; however, given that compliance risks represent secondary consequences of any privacy risk analysis, compliance activities are a necessary element of reducing overall privacy risks.

Recommendation: NIST should add compliance obligations as a factor relevant to determining target profiles.

Profile Scoping

NIST target users of the Privacy Framework include both small organizations and large enterprises with multiple divisions, product lines and subsidiary organizations. Little guidance is currently provided on the appropriate scope of current profiles and target profiles. One would assume that a large organization may have more than one profile, but a smaller organization may have only a single profile for the entire enterprise. However, the current draft of the framework doesn't provide guidance on how to scope profiles across an organization. For instance, where the entire business may have a singular view of

privacy values, different divisions may have different business objectives. Similarly, different geographical parts of a single division may have different resources, risk tolerances, or compliance obligations. This might suggest a profile for each division and geographical operation. Of course, a company could decide to share resources and have a company-wide risk tolerance, which would suggest fewer profiles.

Recommendation: Given the five factors influencing profile development (business objectives, privacy values, resources, risk tolerance, and compliance obligations), NIST should provide guidance on how organizations should develop their profiles based on distinctions within these five factors.

Nick Oldham
Chief Privacy & Data Governance Office
Equifax Inc.