James Crandall
Policy Analyst, Tax and Accounting Policy

AMERICAN PETROLEUM INSTITUTE

Submitted via privacyframework@nist.gov

Monday, January 14, 2019

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

Subject: Comments of API on Development of Privacy Framework

Dear Katie,

The American Petroleum Institute (API) welcomes the opportunity to comment upon NIST's Request for Information (RFI) regarding the development of a privacy framework. The oil and natural gas industry commends NIST and its leadership and approach to privacy, which has been non-regulatory, industry-driven, flexible, and consensus based. America's oil and natural gas industry agrees that many organizations need to manage and communicate privacy risks better and develop innovative approaches to protect individuals' privacy in an increasingly connected and complex technological environment.

API is the only national trade association representing all facets of the natural gas and oil industry, which supports 10.3 million U.S. jobs and nearly 8 percent of the U.S. economy. For nearly a hundred years, API which started as a standards-setting organization has developed almost 700 standards to enhance the safety of our workers and protect the community and environment – standards the world looks to as a guide. API's more than 600 members include large integrated companies, as well as exploration and production, refining, marketing, pipeline, marine businesses, and service and supply firms. They provide most of the nation's energy and are backed by a growing grassroots movement of more than 47 million Americans.

Many companies, including those within oil and gas, have tended to base their privacy programs on regulation and guidance around such regulation. While companies are not likely to move off regulation based programs, a U.S. national privacy framework does have benefits. For example, it may provide a goal for countries with weak or unclear privacy law, helping them to coalesce to a common implementation which would facilitate corporate compliance. It might provide the basis for a European Union declaration of "adequacy" for U.S. corporations/entities which implement the framework.

We address 19 of the 26 organizational consideration topics in the RFI below.

Organizational Consideration Number One: The greatest challenges in improving organizations' privacy protections for individuals

The human element is the most important and greatest challenge of privacy protections. There are several aspects to this challenge:

1. Privacy regulations are not always intuitive. Many workers might consider the ability to access data as akin to allowing one to do what one wishes with it, but this is not the case with personal data which focuses on the purpose of the data collection and how the data is to be used.
2. The definition of personal information is likewise not always consistent or intuitive. Most U.S. based personnel would not consider "business card data" (name, address, and contact information) to be sensitive but this data is subject to privacy regulation in Europe and other jurisdictions. Different generations have different concepts of privacy and different views on privacy laws or regulations.
3. Competing priorities may cause individuals to work around privacy controls. Project deadlines and other such aspects may result in workers cutting corners to advance projects. These shortcuts might inadvertently violate privacy controls.
4. Awareness training is a principal control for addressing human error, negligence, and oversight; training must not only cover privacy requirements but also how to report and contain incidents.

There are several additional challenges in additional to address humans.

- A risk-based approach to privacy can be difficult because of the nuances of combining data. Some information by itself is not particularly sensitive nor constitutes personal information but might be considered personal information combined with other similar information. A classic example is a building address and a room or office number. The former is "public" information and the latter is simply a number or combination of numbers and letters that absent a context mean nothing. An office number in combination with a building address, though, is likely personal information because the two combined identify the occupant of the room.
- This combination issue is compounded using analytics and associated big data/data lake repositories which combine more and more data (and hence run the risk of creating more privacy records) and have cybersecurity data protection issues.
- Most corporations take a corporate-wide approach to privacy, implementing binding corporate rules or corporate policies that apply a standard approach, usually attempting to meet the strongest regulation, across the entire company. As there is great variation among the laws of different countries/states, there is a need in many cases to handle one-off and/or contradictory aspects of the laws. This generally must be done at the local level as there are no compendiums of privacy law across all the jurisdictions where the Oil and Natural Gas industry does business.
- Increased use of the cloud results in personal data passing through Platform-as-a-Service (PaaS) or smaller vendors. Contracts with these suppliers must include proper clauses to provide legal privacy protection.
- Much privacy regulation assumes a free association of the data processor and the data subject such that the data subject volunteers information in return for a service and can freely object or not provide the data. This is not the case with existing employees (data subjects) and their employer (data processor) which restricts use of many of the available techniques for authorizing data use. Monitoring of internal employees is also a challenge; some solutions suggested by privacy professionals, like not reviewing content marked as "personal", run contrary to security needs (as someone trying to exfiltrate sensitive data could simply mark it as "personal" and therefore skirt monitoring defenses.
- Automation, via Robotic Process Automation (RPA) and machine learning, bring additional issues. RPA is effectively "middleware" and as such, is not tracked as intently as real

applications. As RPA bots tend to execute redundant tasks previously done by humans, a standard way to manage them is to treat them as "personnel" (as this avoids the need to create new security profiles, etc.) RPA bots, though, are not really "persons" so processes need to be altered to ensure privacy protections are provided to real people and not to the processes. Machine learning algorithms require data for training which can get into the big data / data lake issues where other solutions, like neural networks, are currently unexplainable which would violate some privacy regulations which require one to explain to a data subject how decisions (like those around credit) are reached.

Organizational Consideration Number Two: The greatest challenges in developing a cross-sector standards-based framework for privacy

Maintaining a business focus is a major challenge, particularly when the framework must abridge across consumer-facing industries and those that are not. The oil and gas industry contain a mix of companies, only some of which are consumer facing. Privacy considerations for employee data may be very different than for consumer or customer data.

A standards framework that focuses only on consumers therefore will be less useful for the oil and natural gas industry.

Existing privacy programs across oil and gas companies varies according to the variety of business models. The presence of different programs internationally, such as the GDPR in Europe and other programs in Canada, Australia, etc. should not come to define a U.S. program, even if flexibility is needed in the framework to consider the existence of other programs.

Organizational Consideration Number Three: How organizations define and assess risk generally, and privacy risk specifically

Virtually all oil and natural gas companies define risk as a function of likelihood and impact. Some oil and natural gas companies utilize the Factor Analysis of Information Risk (FAIR) which defines "risk" as "probable frequency and probable magnitude of future loss". Most companies have specific (separate) frameworks for addressing health, environment, and safety (HES) risks.

Privacy tends to fit within information risk which is defined as the risk of misusing personal information. "Misuse" is itself generally defined by some set of privacy principles. Example principles include:

- Collect personal data in a legal manner and for specified legitimate business purposes only
- Process personal data only as necessary for the specified purposes
- Keep personal data as accurate and complete as possible for their intended purpose.
- Permit individuals to review their personal data and to request correction of factual inaccuracies in accordance
- Secure personal data by reasonable and appropriate information protection safeguards
- Retain personal data in accordance with corporate information retention policies and when no longer required for the stated purpose or by law, destroy personal data in a manner which protects the confidentiality of the data

Any privacy issues identified within a privacy impact assessment will likely be mitigated as opposed to taking other risk-based approaches like accepting the risk or using compensating controls.

Organizational Consideration Number Four: The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management

Most companies within oil and natural gas have a data privacy corporate policy and include privacy within the corporate Business Conduct and Ethics Code. Inclusion in these documents generally require business units to report compliance status, including any deficiencies, yearly to the board of directors (normally through the board audit committee.)

Organizational Consideration Number Five: Current policies and procedures for managing privacy risk

The corporate policy referenced in question 4 will normally cover which entities within the corporation are responsible for managing privacy risk. Business unit managers are responsible for privacy policy compliance within their business units. Tasks include ensuring awareness training is completed, performing risk assessments, and allocating enough resources. Employees must understand and comply with applicable policies with responsibilities including protecting personal data under their care from improper use and disclosure.

The corporate-wide privacy manager serves as subject matter expert and contact person for issues relating to data privacy. Regulation requires this person and his/her contact information to be available to the public. Some companies will ensure that such an officer is in-country in restrictive jurisdictions whereas for other locations, inquiries may be routed to a central officer. The privacy officer will dispense guidance and advice to business units to assist with privacy compliance.

Corporate audit departments will conduct periodic data privacy audits and recommend corrective action. Corporate counsel will provide legal advice on privacy. Different companies organize these services differently. Oil and natural gas companies with a strong presence in Europe will base their privacy officer on that continent and will have dedicated lawyers reporting to him/her. Other companies may have a central but separate legal and privacy officers.

Organizational Consideration Number Six: How senior management communicates and oversees policies and procedures for managing privacy risk

Privacy is included as a separate component within the risk framework of many oil and natural gas companies. A primary reason for this separation is the gargantuan fines possible from privacy violations. The benefits of the separation are that privacy risk must be reported separately (rather than folded into other information risks) and, consequently, the processes, procedures, and controls specific to privacy alone are developed.

Organizational Consideration Number Seven: Formal processes within organizations to address privacy risks that suddenly increase in severity

We are not exactly sure as to what this question is referring to as we are not sure as to the meaning (or even of an example) of “privacy risks that suddenly increase in severity.”

If this is referring to incident response, then companies will have branches built-in to properly (and legally) handle breach notification requirements if personal data were involved in an incident.

Organizational Consideration Number Eight: The minimum set of attributes desired for the Privacy Framework, as described in the Privacy Framework Development and Attributes section of this RFI, and whether any attributes should be added, removed or clarified

The listed attributes are fine although other than the sixth one, all are general and do not apply specifically to privacy.

Organizational Consideration Number Nine: What an outcome-based approach to privacy would look like

Privacy-by-design is one outcome-based approach -- information architecture should ensure that privacy is built into solutions offered by the company. Another aspect of an approach may be to successfully manage suppliers and other third parties with contracts and the appropriate privacy clauses included. Avoiding breaches should be a target outcome of any approach.

Organizational Consideration Number Ten: What standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles organizations are aware of or using to identify, assess, manage, and communicate privacy risk at the management, operational, and technical levels, and whether any of them currently meet the minimum attributes described above

Most companies can tie their privacy risk profiles back to standards and frameworks used for other information risk. As an example, access controls which would be part of a privacy program can be linked back to international standards like ISO 27000 which, in turn, have been linked back to NIST Cybersecurity Framework. The CSF is the basis for many oil and natural gas cybersecurity programs.

Organizational Consideration Number Eleven: How current regulatory or regulatory reporting requirements (e.g., local, state, national, international) relate to the use of standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles

There tends to be little formal relation of regulation to standards, frameworks, models, etc. State breach notification laws tend to include their own unique definitions of personal information and/or notification requirements (including content of the letters). International privacy law tends to be principles based but there is no universal principal list. (OECD created an initial list of principles in 1980 and while European and other country law borrows from these principles, none quote directly.) One exception might be the Payment Card Industry (PCI) standards which are referenced in some legislation.

Organizational Consideration Number Twelve: Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices

Payment Card Industry (PCI) standards are “mandated” for those in the industry who have retail facilities and accept credit cards. Outside of that, there are really no standards, frameworks, models, etc. mandated for the industry.

Organizational Consideration Number Thirteen: The role(s) national/international standards and organizations that develop national/international standards play or should play in providing

confidence mechanisms for privacy standards, frameworks, models, methodologies, tools, guidelines, and principles

Most oil and natural gas companies tend to base their privacy programs on regulation and guidance around the regulation rather than using international standards. Roughly fifteen years ago, one oil and gas company adopted the Organization for Economic Co-operation and Development (OECD) principles for privacy but converted to using the European Union principles by 2010 because these facilitated compliance with the key privacy law for that entity at the time. Companies will continue to build their programs off the regulations.

Organizational Consideration Number Fourteen: The international implications of a Privacy Framework on global business or in policymaking in other countries

Some countries have weak or unclear privacy laws, and some have regulation that changes depending on the person or party in power. A privacy framework might provide a goal for these countries and, if adopted, would facilitate corporate compliance.

A privacy framework might serve as the basis for the European Union to declare U.S. privacy implementation "adequate" and, therefore, facilitate cross-border transfer of personal information. A framework also has the potential to facilitate further international harmonization.

Organizational Consideration Number Fifteen: How the Privacy Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform privacy functions within organizations.

The oil and natural gas industry does not see much, if any, impact of a privacy framework on a knowledgeable and skilled workforce.

Organizational Consideration Number Sixteen: Please describe how your organization currently manages privacy risk. For example, do you structure your program around the information life cycle (i.e., the different stages—from collection to disposal—through which PII is processed), around principles such as the fair information practice principles (FIPPs), or by some other construct?

Most oil and natural gas companies structure their privacy programs around principles in "key" privacy regulations. Companies that had used OECD and other principles have generally moved away from these toward other legal mandates.

Organizational Consideration Number Seventeen: Whether any aspects of the Cybersecurity Framework could be a model for this Privacy Framework, and what is the relationship between the two frameworks.

The Cybersecurity Framework (CSF) certainly applies directly to the security principle for privacy. Access management and the risk assessment aspects of the Identify function directly apply.
The CSF, though, lacks categories around unauthorized use of information which is a key aspect of privacy compliance. The monitoring categories/subcategories, within the detect function, talk about the need the monitor but do not include guidance as to how to properly manage collected information which likely includes personal data.

Organizational Consideration Number Eighteen: Please describe your preferred organizational construct for the Privacy Framework. For example, would you like to see a Privacy Framework that is structured around:

a) **The information life cycle;**
b) **Principles such as FIPPs;**
c) **The NIST privacy engineering objectives of predictability, manageability, and disassociability or other objectives;**
d) **Use cases or design patterns;**
e) **A construct similar to the Cybersecurity Framework functions, categories, and subcategories; or**
f) **Other organizing constructs?**

As most oil and natural gas companies base their programs on regulatory principles, the Privacy Framework, to ease mapping, should be organized around a principles approach.

Other aspects listed above, like information life cycle, engineering objectives, use cases and design patterns, etc. should be covered in guidance associated with the framework.

The CSF function concept may not make sense as the basis for the entire document but certainly has applicability with a "security" principle.

Specific Privacy Practices

In addition to the approaches above, NIST is interested in identifying core privacy practices that are broadly applicable across sectors and organizations. NIST is interested in information on the degree of adoption of the following practices regarding products and services:

- De-identification;
- Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared;
- Enabling user preferences;
- Setting default privacy configurations;
- Use of cryptographic technology to achieve privacy outcomes—for example, the disassociability privacy engineering objective;
- Data management, including:
- Tracking permissions or other types of data tracking tools,
- Metadata,
- Machine readability,
- Data correction and deletion; and
- Usable design or requirements.

Organizational Consideration Number Nineteen: Whether the practices listed above are widely used by organizations

Few oil and natural gas companies are consumer facing and, consequently, have not implemented many if any of the listed privacy practices. Those companies who do work directly with customers do so through vendors/suppliers and expect those entities to supply the proper technology.

Conclusion

The American Petroleum Institute appreciates the opportunity to provide comments on a proposed privacy framework. We recommend that NIST considers a risk-based approach that aligns with existing standards to help provide a scalable, easily adoptable system to manage privacy risk. America's oil and natural gas industry is ready to work with the NIST to help develop a privacy framework that benefits all Americans.

Respectfully submitted,

James Crandall
API