To: National Institute of Standards and Technology
From: Threat Sketch, LLC
Re: Developing a Privacy Framework

Introduction

Threat Sketch, LLC is a North Carolina limited liability company and centrally located in in Winston-Salem. The company is focused on Cyber Risk Management and uses a SaaS model in conjunction with a number of proprietary databases and data analytics to accurately predict cyber risks in small and medium-sized businesses, nonprofit organizations, and local governments. Threat Sketch is both an advocate and service provider for these sectors and currently serves as one of the initial Executive Council members of the ICT Supply Chain Task Force that was established by the Department of Homeland Security to address holistic, cross-sector risks to the nation's critical infrastructure. Cybersecurity and Privacy go hand-in-hand for both Threat Sketch and the communities it serves, and the company believes that the development of a Privacy Framework can be an invaluable asset for American consumers and innovators. However, to successfully achieve its mission, the Privacy Framework will need a realistic look at all aspects of the risks associated with innovation in the 21st century, including market forces, legal structures, and consumer needs.

Objectives

Threat Sketch submits this public comment with the intent to help the National Institute of Standards and Technology ("NIST") formulate a Privacy Framework that proves to be as influential and helpful as the NIST Cybersecurity Framework. Threat Sketch also submits this comment to emphasize the multi-faceted nature of Privacy Risk and the need for the new framework to holistically identify the risks and provide guidelines for resolution.

Response to Request for Information

The National Institute of Standards and Technology has requested information and comments related to Risk Management, Organizational Considerations, Structuring the Privacy Framework, and Specific Privacy Practices for the purpose of developing a Privacy Framework. The first comment we make addresses an issue brought up in the webinar that NIST hosted on the subject: What constitutes "Privacy Risk"?

Privacy Risk Definition

The webinar that NIST hosted on November 29, 2018, brought up an interesting question: What constitutes "Privacy Risk"? Certainly the social risks of a breach of privacy[1]

and the economic risks of a breach of privacy[2] will be included in any definition. However, legal risks and institutional risks should also be of paramount importance for NIST as it considers the development of a Privacy Framework.

This Webinar made clear that NIST does not want the Privacy Framework to be a prescriptive Framework for regulatory compliance. Therefore, Threat Sketch understands the temptation to resist incorporating Legal Risk into its concept of "Privacy Risk." However, as we will discuss in greater detail in the next section, an objectives-based approach can provide important tools that can help organizations with their legal decisions while not prescribing particular solutions to compliance questions. Specifically, since most laws and regulations punish when harm is done, a results-focused Framework would be invaluable for small- and medium-sized businesses ("SMBs"), nonprofits, and local government actors.

Finally, it is no secret that confidence in institutions in the United States is not high.[3] Privacy violations by important American institutions could further erode confidence. As such, the risk to the system needs to be kept in mind and looked at it as a "public good" to all actors within the system. Consequently, this only heightens the need to gear tools to SMBs. Small business is one of the few institutions in America with an overwhelmingly positive confidence rating.[4] Yet, as is discussed in the Risk Management section, such businesses represent a critical threat to privacy wherever a supply chain is needed. This only reiterates the need to tailor solutions to SMBs in order to mitigate risk to the institutions of the American economy.

Risk Management

Under the NIST Cybersecurity Framework, as published in 2014 and revised in 2018, protective measures largely fell into three categories for three types of risks: Physical, Administrative, and Technological. As the Privacy Framework is realized, it is important that more types of risk are contemplated in order to not impinge innovation. Specifically, Institutional Risk, as described above, and Legal Risks—such as disclosure requirements and possible civil penalties—should be integral considerations for any organization utilizing a future Privacy Framework.

Traditional forms of risks and Institutional Risk largely speak for themselves, so this section will focus on the benefits of having the Framework guide organizations to manage Legal Risk in Privacy as well. In the webinar that NIST hosted regarding this Request for Information, it was reiterated that the Privacy Framework was not prescriptive and not meant as a compliance tool. Due to the fact that Legal Risk is such a substantial part of Privacy Risk, however, ignoring legal and compliance concerns in this Framework would be unwise.

Small- and medium-sized businesses[5] contribute just under half of America's private sector employment and over 40% of the private sector payroll, according to the Small Business Administration's August 2018 numbers.[6] SMBs, however, often have the hardest time complying with federal regulation and guidance.[7] And if the costs of compliance are too high,

one can only imagine the stress in the economy that is caused by the prospective costs of lawsuits or penalties under various theories that argue that the organization has not utilized "reasonable" measures to safeguard Americans' privacy. Because the need for workable and affordable guidance is so great for SMBs and their collective impact on the economy is so extensive, the Privacy Framework should make a dedicated effort to highlighting lower-cost, higher-impact tools these organizations can use. Nonprofits and local governments, both discussed in greater detail in the next section, would also benefit from such tools.

SMBs are critically important to supply chains, but often constitute the weakest links within them, as the organizations have few resources geared towards their needs. As noted by a recent Forbes article discussing the likely cybersecurity problems America will face in this New Year, SMBs in supply chain pose risks to the larger companies they serve and to the overall economy that could be "catastrophic."[8] This is a security problem for sure, but it is also a privacy problem if those weaknesses result in the disclosure of personally identifiable information. American consumers want their privacy secured, and filling in those holes in the supply chain should be a focus of the Privacy Framework.

NIST should also keep in mind the possibility for the Institute to provide structure for the legal side of Privacy Risk through this Framework. One need look no further than the NIST Cybersecurity Framework in order to see how this could be the case. In *Toward an International Standard of Care?*, published in 2015 by the Texas International Law Journal, the authors argue that, "U.S. cybersecurity law relies heavily on interpreting and implementing 'reasonable' and 'appropriate' cybersecurity measures . . . Given the fact that what constitutes 'reasonable' cybersecurity practices is not yet well defined, the NIST Cybersecurity Framework has the potential to be influential in shaping reasonable cybersecurity standards in the United States and further afield."[9] And indeed, the NIST Cybersecurity Framework was recently established as a safe harbor in an Ohio law requiring reasonable cybersecurity protections for consumers' data, meaning that compliance with the NIST Cybersecurity Framework (or other enumerated frameworks) equates to compliance with the requisite protections.[10] NIST should expect to wield similar influence in Privacy law as it has had in Data Security law, whether it courts that influence or not. And with that persuasive authority comes the responsibility to use it to at least point out that these legal and compliance risks are part of the overall "Privacy Risk" that SMBs need to manage.

Altogether, the combination of SMBs' and other resource constrained organizations' needs for Privacy tools, the American economy's and the American consumers' need to safeguard SMBs in the supply chain, and the influence NIST can wield in this space make getting a cost-conscious, workable Privacy Framework of paramount importance. NIST can do that by incorporating the traditional economic and social value of Privacy into its concept of risk—much as it did with the Cybersecurity Framework—but also by leaning heavily on liability in the legal system and American institutional credibility for a concept of the risks to the

American economy generally and to SMBs, non-profits, and local government actors in particular.

Organizational Considerations

The segments of the American economy that are affected by privacy concerns are diverse. They include any industry—regardless of subject matter—that relies on information about businesses, clients, consumers, or other stakeholders. They include manufacturers, retailers, and service providers. They include massive technology corporations, small mom-and-pop stores, hospitals, private medical practices, nonprofits, school districts, and much more. If a Privacy Framework is going to be truly influential for the entirety of the American economy, it must account for the different needs and abilities of all the economy's participants. Finally, the differing legal duties for different sectors must be taken into account.

As discussed in the Risk Management section, SMBs often get left behind in privacy discussions, because the cost of taking proactive steps is perceived as being simply too high to do properly. And of particular concern are federal and state legal systems that may punish an SMB for inadequate privacy protections. While this Framework may want to steer clear of prescribing a means of complying with any particular law—as the Webinar emphasized—NIST should not steer clear of guiding SMBs towards outcomes that expressly make violation of regulatory and legal regimes less likely. For example, reviewing vendor contracts for privacy and security warranties or covenants is an important part of insulating an organization from liability. Such a practice would also increase the overall level of privacy for American consumers. However, for that vendor, making privacy and security covenants or warranties just became a potential source of liability, and that vendor is often going to be an SMB[11]. Using this Framework to guide the SMB vendor towards objectives that make privacy breaches less likely will assist SMBs with avoiding liability while sticking to NIST's non-prescriptive model and increasing Americans' overall level of privacy.

While NIST, located within the Department of Commerce, may focus primarily on commercial entities, it is important to remember that other organizations rely upon guidance like that which the Framework hopes to provide. Specifically, non-profit and local government actors will need to be able to use privacy tools to keep Americans' data secure.

There are over 1,500,000 organizations in America that can be considered "nonprofits."[12] In 2014, they accounted for 5.3% of American GDP.[13] And over a 4-year period more than 25% of Americans over the age of 16 will volunteer for a non-profit organization.[14] This is all phenomenal news and reflects the nation's heart, but for the organizations themselves, that means they now have privacy obligations to donors, employees, and any of those 25% of Americans volunteering if the nonprofit collects information—like contact information—on those stakeholders. And for the best nonprofits—the ones that seek to move every dollar possible from donations to their mission—the prospect of investing in the

costly privacy tools that are made with large corporations in mind may be a non-starter. Worse still, many may not even be aware of their obligations to keep information private and secure or may think their nonprofit status makes them an unlikely target for a breach. Unfortunately, this is not the case.[15] Overall, however, the need to devote monies to their mission makes cost a significant—perhaps even determinative—factor in their analysis of Privacy Risk.

Local governments and the institutions that comprise them—such as public schools—also are in dire need of Privacy tools. These institutions are often even more financially constrained than their SMB and nonprofit colleagues, because when their revenue consists of an annual appropriation or perhaps tax revenue that they do not truly control, they can be faced with a very constrained set of resources and a statutorily-defined or publicly-expected mission. This can leave little room for investing in privacy protections. However, the result of not doing so could be severe.[16]

These three groups have two main things in common: they are incredibly important to American life and they currently have few tools geared towards their extraordinarily budget-conscious organizational structures. SMBs and non-profits[17] additionally face the prospect—whether real or perceived—of being wiped out by either compliance costs or non-compliance penalties. And that perception has real harms to American Privacy Risk in itself.

Structuring the Privacy Framework

The structures of the Privacy Framework and the Cybersecurity Framework should complement each other. As the Cybersecurity Framework provided steps for Identification, Detection, Protection, Response, and Recovery with regard to a data breach, so should the Privacy Framework map out an approximately linear path for safeguarding privacy. Two of the most important steps regarding privacy are "Risk Assessments," which should be incorporated early and often by those seeking to minimize Privacy Risk, and Mitigations of that Privacy Risk. Ideally this would be done in a vendor-neutral way to avoid SMBs, nonprofits, and local governments tuning the advice out because they feel someone is "selling" them, not truly assessing them. A process of Assessing vulnerabilities in order to Attribute a vulnerability to particular practices—or lack of practices—and then Mitigating that vulnerability reflects the risk-based approach that is best for most organizations. Response and Recovery sections could round out the parallel to the Cybersecurity Framework.

Assessing Privacy Risk must be the first step of this Framework so that organizations of whatever size may then identify risks and budget for Mitigation. Organizations need to look holistically at their possible vulnerabilities, prioritize which vulnerabilities are largest and which concern the most sensitive data, and use that information to Attribute the points of greatest concern to particular practices. The assessment should also consider an organization's jurisdiction so as to incorporate the Legal Risk element that is of such importance for SMBs,

nonprofits, and local governments who need tools to move them towards stable legal ground in this area.

The second step should be Attribution. Attributing risks would involve taking the results of the Risk Assessment and identifying particular actions/inactions to each risk. It is important to attribute each general vulnerability found in the Assessment phase to particular practices or inactions that allow for the vulnerability in order to avoid the illusion of greater privacy with no real changes. Having any organization that wants to adhere to the NIST Privacy Framework go through the effort of tying each vulnerability to specific examples will significantly help minimize their Privacy Risk if only because now the organizations are expressly aware of the linkage. It would likely also increase the "buy in" of SMBs, nonprofits, and local governments who want to avoid spending precious resources on cosmetic improvements to privacy.

After the tie has been made between practices and vulnerabilities, the Mitigation of risks should be the priority. It is rarely the case that a vulnerability can be eliminated entirely. This is why the "risk-based" approach has become so popular. Rather than trying to perfectly secure the privacy of every scrap of data held, an organization should mitigate the practices/inactions that create risks. By taking steps to make the vulnerabilities associated with the practices/inactions less harsh, Privacy Risk diminishes, even if it will never truly disappear.

The Response and Recovery functions would operate much as they presently do in the NIST Cybersecurity Framework, with an emphasis on stakeholder communication.

This section will conclude by way of a simplified example. If a small business keeps a database on the preferences of its clients, there is a Privacy Risk. The Risk Assessment function would identify the security protections on that database as a vulnerability. The Attribution function would tie the practice of using weaker passwords to the vulnerability of the database's security. The Mitigation function would recommend—among other things—the use of a Password Manager[18]. The Response function would require an organization that wants to adhere to the NIST Privacy Framework to plan ahead of time for the eventuality that a password could be guessed or stolen. And the Recovery function would require such an organization to plan for how they can get back up and running after such an eventuality.

This kind of a framework would give SMBs, nonprofits, and local governments the tools they need to comply with applicable law while not being a prescriptive formula for compliance. It also can be geared in a budget-friendly way by scaling monetary costs to sensitivity of data and providing mitigation tips for avoiding collection of data that would be the costliest to protect.

Specific Privacy Practices

The Specific Privacy Practices should be incorporated into the Mitigations function described above. To cite two specific examples, encryption and de-identification are prime mitigation candidates. If a Risk Assessment identifies personal information stored in a database as a target, the Assessment would tie the practice of collecting such data to the vulnerability of

the database. Encryption and de-identification are ways to mitigate those vulnerabilities and make the risk of disclosure less harmful. These processes also help comply with most state and federal regulations and statutes that apply to SMBs, nonprofits, and local governments, so the Framework would give the tools that such organizations need.

Conclusion

The NIST Privacy Framework is an exceptional opportunity to help small- and medium-sized businesses, nonprofits, and local governments gain the tools they need to safeguard their consumers', clients', donors', and other stakeholders' privacy. By incorporating Legal Risk and Institutional Risk—in addition to more traditional types of risk—into such a Framework, these tools can do immeasurable good for the American consumer and economy. The Framework should manage risk with an eye towards those that need the tools the most and in ways that they need. And it should be structured with a positive loop of Assessing risks, Attributing risks to practices/inactions, and Mitigating the effects of the vulnerability followed by a Response and Recovery.

---

[1] E.g. embarrassment, a populace that feels without control of their personal information, disclosure of contact information to those who might use it to harass.
[2] E.g. loss of customers, lack of faith in institutions, increased cost of vendor contracts.
[3] *See generally*, https://news.gallup.com/poll/1597/confidence-institutions.aspx.
[4] https://news.gallup.com/poll/1597/confidence-institutions.aspx
[5] Defined on a sector-by-sector basis by the Small Business Administration, but typically seen as businesses with fewer than between 500-800 employees or between $1 million-$20 million in annual receipts. *See* https://www.sba.gov/document/support--table-size-standards, which contains a spreadsheet that lists industries by the amount of annual receipts or employees needed to be considered a large enterprise. The Average number of employees needed for industries where that is a relevant marker is around 775; the average annual receipts for industries where that is a relevant marker is $18.1 million.
[6] https://www.sba.gov/sites/default/files/advocacy/Frequently-Asked-Questions-Small-Business-2018.pdf
[7] *See* Michael Hendrix, *The Regulatory Impact on Small Businesses: Complex. Cumbersome. Costly.*, U.S. Chamber of Commerce Foundation (March 14, 2017), https://www.uschamberfoundation.org/blog/post/regulations-impact-small-business-and-heart-americas-economy (finding upon a review of academic literature that, "The costs to smaller businesses with 50 employees or fewer are nearly 20% higher than the average for all firms").
[8] https://www.forbes.com/sites/forbestechcouncil/2018/12/28/cybersecurity-predictions-for-2019/#1fe59e734a27
[9] Scott Shackelford, et al. *Toward an International Standard of Care?* 50 TEX. INT'L L.J. 305, 340 (2015).
[10] Brandan Montminy, et al., *New Data Security Law Offers Safe Harbor; May Signal New Trend*, JD Supra, (November 27, 2018) https://www.jdsupra.com/legalnews/new-data-security-law-offers-safe-94751/.
[11] SMBs, having less negotiating power than larger businesses, may acquiesce to such covenants or warranties to keep their business afloat. However, when that happens, they currently are without tools to guide them to outcomes that can help avoid liability.
[12] https://nccs.urban.org/data-statistics/quick-facts-about-nonprofits
[13] *Id.*

[14] *Id.*
[15] *See*, *e.g.*, https://www.fema.gov/news-release/2018/09/21/beware-fraud-and-scams
[16] E.g. school counselor's notes released; public clinic health records disclosed; taxpayer records made public.
[17] Local government actors are admittedly more likely to be immune from liability—or at least limit liability—through sovereign immunity or a statute.
[18] https://threatsketch.com/password-managers-should-you-use-them/