Federal Trade Commission Staff Comment on the Preliminary Draft for the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management

I. Introduction

Thank you for the opportunity to comment on the Preliminary Draft for the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management ("Draft Privacy Framework" or "Framework").[1] These comments represent the views of the staff of the Bureau of Consumer Protection. The Commission has voted to authorize BCP staff to submit these comments.

In today's digital age, the collection, sharing, and use of consumer data has advanced innovation that many consumers find beneficial, such as improving consumer safety while driving through connected cars that offer real-time notifications of dangerous conditions;[2] facilitating financial transactions through mobile payment systems;[3] improving health and wellness through information provided by diagnostics, screening apps, and wearables;[4] and improving the safety and comfort of homes through IoT devices.[5]

The widespread collection, sharing, and use of consumer data, however, can also raise significant risks. The news frequently reports on problematic privacy practices that can result in

[1] NIST, PRELIMINARY DRAFT, NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT (2019) ("DRAFT PRIVACY FRAMEWORK"), *available at* https://www.nist.gov/sites/default/files/documents/2019/09/09/nist_privacy_framework_preliminary_draft.pdf.
[2] *See, e.g., What Are the Benefits of Connected Vehicles?*, DEPT. OF TRANS. OST-R RESOURCE (last visited Oct. 21, 2019), https://www.its.dot.gov/cv_basics/cv_basics_benefits.htm.
[3] *See, e.g.*, Brenda Porter-Rockwell, *5 Benefits of Using a Mobile Payment App*, LG-FCU (Aug. 23, 2017), https://www.lgfcu.org/personal-finance/5-benefits-of-using-a-mobile-payment-app.
[4] *See, e.g.*, C. Lu *et al.*, *The Use of Mobile Health Applications to Improve Patient Experience: Cross-Sectional Study in Chinese Public Hospitals*, 6(5) JMIR MHEALTH UHEALTH 126 (2018), *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5990855/; *Digital Health*, FOOD & DRUG ADMIN. (last visited Oct. 21, 2019), https://www.fda.gov/medical-devices/digital-health.
[5] *See, e.g.*, Nell Lewis, *The 'Living Laboratory': Inside a Neighborhood of Smart Homes*, CNN (Aug. 8, 2019), *available at* https://www.cnn.com/2019/08/07/business/alabama-power-smart-neighborhood/index.html.

adverse outcomes for consumers.[6] Organizations must therefore take steps to safeguard the privacy of the consumer data that they collect, store, use, transfer, or share with others.

We commend NIST for addressing this timely issue by proposing a tool designed to help management start a dialogue about how to manage privacy risks within their organizations. We also commend NIST's inclusive, multi-stakeholder process in which it has solicited comments and feedback from industry, government, and consumer representatives.

This comment first describes the Commission's deep experience in protecting consumer privacy through enforcement, education, and policy work. Then, highlighting certain lessons that can be drawn from past privacy cases, this comment recommends that NIST consider certain clarifications to its Draft Privacy Framework. We provide these comments in an effort to ensure that the Framework and accompanying documents provide useful information and guidance to organizations without overly burdening them. These comments are not intended to provide a template for FTC law enforcement.

II. Background on the Federal Trade Commission

The Federal Trade Commission ("FTC" or "Commission") is an independent administrative agency responsible for protecting consumers and promoting competition. For decades, the Commission has been a leader in protecting consumer privacy through its enforcement actions, consumer and business education, and policy initiatives.

The FTC protects consumer privacy through enforcement actions under the FTC Act, which prohibits unfair and deceptive acts or practices—including unfair and deceptive privacy

[6] *See, e.g.*, Brakkton Booker, *Housing Department Slaps Facebook With Discrimination Charge*, NPR (Mar. 28, 2019), *available at* https://www.npr.org/2019/03/28/707614254/hud-slaps-facebook-with-housing-discrimination-charge; Alex Hern, *Vibrator Maker Ordered to Pay Out C$4m for Tracking Users' Sexual Activity*, THE GUARDIAN (Mar. 14, 2017), *available at* https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits.

practices—in or affecting commerce.[7] The FTC also enforces a number of other statutes that protect consumer privacy, including the Fair Credit Reporting Act ("FCRA")[8] and the Gramm-Leach-Bliley Act ("GLB"),[9] which protect certain consumer financial information; the Children's Online Privacy Protection Act ("COPPA"),[10] which protects certain children's information; and the Telemarketing Sales Rule ("TSR"),[11] the CAN-SPAM Rule,[12] and the Fair Debt Collection Practices Act ("FDCPA"),[13] all of which protect consumers from certain unwanted intrusions.

The FTC has brought hundreds of cases protecting the privacy of consumer information. For example, the FTC has brought enforcement actions against organizations that, among other things, collected information from children online without parental consent;[14] developed "stalking apps" to surreptitiously monitor other adults;[15] deceived consumers about the collection, use, or disclosure of their financial, health, or other personal information;[16] made

---

[7] 15 U.S.C. § 45(a). The FTC's unfairness cases have challenged privacy and security practices that cause or are likely to cause substantial harm to consumers. *See, e.g., In re Lenovo, Inc.*, Case No. C-4636 (F.T.C. January 2, 2018) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/1523134_c4636_lenovo_united_states_complaint.pdf (alleging laptop manufacturer Lenovo unfairly preinstalled man-in-the-middle software that collected consumer internet browsing information without adequate consumer notice or consent).

[8] 15 U.S.C. § 1681 *et seq.*

[9] 15 U.S.C. § 6801 *et seq.*; Privacy of Consumer Financial Information, 16 C.F.R. Pt. 313 ("GLB Privacy Rule"); Standards for Safeguarding Customer Information, 16 C.F.R. Pt. 314 ("GLB Safeguards Rule"); Regulation P, 12 C.F.R. Pt. 1016.

[10] 15 U.S.C. § 6501 *et seq.*; Children's Online Privacy Protection Rule, 16 C.F.R. Pt. 312 ("COPPA Rule").

[11] Telemarketing Sales Rule, 16 C.F.R. Pt. 310 (implementing Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. § 6101 *et seq.*).

[12] CAN-SPAM Rule, 16 C.F.R. Pt. 316, implementing Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM") of 2003, 15 U.S.C. § 7701 *et seq*.

[13] 15 U.S.C. § 1692 *et seq*.

[14] *E.g., FTC v. Google LLC & YouTube LLC*, No. 1:19-cv-02642 (D.D.C. Sept. 10, 2019) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_revised_complaint.pdf; *United States v. Musical.ly*, No. 2:19-cv-1439 (C.D. Cal. Feb. 27, 2019) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/musical.ly_complaint_ecf_2-27-19.pdf.

[15] *In re Retina-X Studios*, LLC, FTC No. 172 3118 (Oct. 22, 2019) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/172_3118_-_retina-x_studios_complaint_updated.pdf.

[16] *E.g., In re Unrollme, Inc.*, FTC No. 172 3139 (Aug. 8, 2019) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/172_3139_unrollme_complaint_8-8-19.pdf; *In re PayPal, Inc.*, Case No. C-4651 (F.T.C. May 24, 2018) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/1623102_c-4651_paypal_venmo_complaint_final.pdf; *FTC et al. v. Vizio, Inc.*, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) (Complaint), *available at*

false promises about their compliance with the EU-U.S. Privacy Shield Framework;[17] deceptively tracked consumers online;[18] publicly posted private data online without consumers' knowledge or consent;[19] or disclosed sensitive consumer information to unauthorized third parties.[20] In short, when organizations engage in illegal privacy practices, the FTC holds those organizations accountable.

These enforcement actions, including the complaints, consent agreements, and corresponding analyses to aid public comment, provide guidance on the Commission's views as to which privacy practices violate the law as well as the necessary elements of a reasonable privacy program. For example, the Commission routinely requires companies under order for privacy violations to, among other things, designate an employee or employees to coordinate and be responsible for a privacy program; perform a risk assessment to identify material privacy risks; design and implement safeguards to control the identified risks; monitor the effectiveness

---

https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf; *In re Practice Fusion, Inc.*, No. C-4591 (F.T.C. Aug. 16, 2016) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/160816practicefusioncmpt.pdf.

[17] *E.g.*, *In re SecurTest, Inc.*, No. C-4685 (F.T.C. Aug. 21, 2019) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/182_3152_c4685_securtest_complaint.pdf; *see also* Press Release, Fed. Trade Comm'n, Five Companies Settle FTC Allegations That They Falsely Claimed Participation in EU-U.S. Privacy Shield (Sept. 3, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/five-companies-settle-ftc-allegations-they-falsely-claimed.

[18] *E.g.*, *In re Turn, Inc.*, Case No. C-4612 (F.T.C. Apr. 21, 2017) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/152_3099_c4612_turn_complaint.pdf; *In re Compete, Inc.*, FTC No. 102 3155 (Feb. 25, 2013) (Complaint), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130222competecmpt.pdf; *In re Sears Holding Mgmt. Corp.*, Case No. C-4264 (F.T.C. June 4, 2009) (Decision and Order), *available at* https://www.ftc.gov/enforcement/cases-proceedings/082-3099-c-4264/sears-holdings-management-corporation-corporation, *later modified at In re Sears Holding Mgmt Corp.*, Case No. C-4264 (F.T.C. Feb. 28, 2018) (Order Approving the Petition to Reopen and Modify Final Order), *available at* https://www.ftc.gov/system/files/documents/cases/c4264searsordergrantingpetition.pdf.

[19] *E.g.*, *FTC v. EmpMedia (MyEx)*, No. 2:18-cv-00035 (D. Nev. June 15, 2018) (Order Granting Motion for Default Judgment and Final Order for Permanent Injunction and Other Relief), *available at* https://www.ftc.gov/system/files/documents/cases/emp_order_granting_default_judgment_6-22-18.pdf; *In re Jerk LLC d/b/a Jerk.com*, Case No. 9361 (F.T.C. March 25, 2015) (Commission Opinion), *available at* https://www.ftc.gov/system/files/documents/cases/150325jerkopinion_0.pdf.

[20] *E.g.*, *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009).

of those controls; and regularly evaluate and update the privacy program in light of any changes to its business practices or business environment.[21]

The Commission also promotes consumer privacy by engaging in consumer and business education, including through blog posts, educational materials, and social media activity. Recent topics have included children's privacy,[22] "stalkerware,"[23] revenge porn,[24] information security,[25] online safety,[26] credit monitoring,[27] and the privacy of genetic information.[28]

Finally, the Commission promotes consumer privacy by undertaking a number of policy initiatives. For example, the Commission has hosted workshops related to children's privacy,[29] connected cars,[30] education technology,[31] drones,[32] and smart TVs.[33] Since 2016, the

---

[21] *E.g.*, *United States v. Facebook, Inc.*, No. 19-cv-2184, (D.D.C. Jul. 24, 2019) (Stipulated Order), *available at* https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf; *In re Uber Technologies, Inc.*, Case No. C-4662 (F.T.C. Oct. 26, 2018) (Revised Final Decision and Order), *available at* https://www.ftc.gov/system/files/documents/cases/152_3054_c4662_uber_technologies_revised_decision_and_order.pdf; *FTC et al. v. Vizio, Inc.*, Case No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) (Stipulated Order), *available at* https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.

[22] Peder Magee, *Happy 20th Birthday, COPPA*, FTC (Oct. 22, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/10/happy-20th-birthday-coppa; Lesley Fair, *$170 million FTC-NY YouTube Settlement Offers COPPA Compliance Tips for Platforms and Providers*, FTC (Sept. 4, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/09/170-million-ftc-ny-youtube-settlement-offers-coppa.

[23] Lesley Fair, *FTC Takes Action Against Stalking Apps*, FTC (Oct. 22, 2019), https://www.consumer.ftc.gov/blog/2019/10/stalking-apps-retina-x-settles-charges.

[24] Jennifer Leach, *What to Do If You're the Target of Revenge Porn*, FTC (Jan. 11, 2018), https://www.consumer.ftc.gov/blog/2018/01/what-do-if-youre-target-revenge-porn.

[25] *E.g.*, Lesley Fair, *Safeguard Your Network and Customer Credentials*, FTC (Apr. 23, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/04/safeguard-your-network-customer-credentials-tips-latest-ftc; Lesley Fair, *$575 Million Equifax Settlement Illustrates Security Basics for Your Business*, FTC (Jul. 22, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/575-million-equifax-settlement-illustrates-security-basics.

[26] Lisa Lake, *Where is Your Online Search Leading You?*, FTC (Aug. 27, 2019), https://www.consumer.ftc.gov/blog/2019/08/where-your-online-search-leading-you; Ari Lazarus, *Back to School: Online Safety*, FTC (Aug. 22, 2019), https://www.consumer.ftc.gov/blog/2019/08/back-school-online-safety.

[27] Amanda Koulousias, *Servicemembers and Guardsmen: Free Electronic Credit Monitoring Coming Soon*, Military Consumer (June 24, 2019), https://www.militaryconsumer.gov/blog/servicemembers-and-guardsmen-free-electronic-credit-monitoring-coming-soon-0.

[28] *E.g.*, Elisa Jillson, *Selling Genetic Testing Kits? Read On.*, FTC (Mar. 21, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/03/selling-genetic-testing-kits-read.

[29] FTC WORKSHOP, *The Future of the COPPA Rule: An FTC Workshop* (Oct. 7, 2019), https://www.ftc.gov/news-events/events-calendar/future-coppa-rule-ftc-workshop.

[30] FTC WORKSHOP, *Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles* (June 28, 2017), https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.

Commission has also hosted *PrivacyCon*, an annual conference that brings together academics, consumer advocates, researchers and others to discuss and present the latest research and trends related to consumer privacy and data security.[34] The Commission has also issued or authorized staff to issue a number of relevant reports, including:

- *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*;[35]
- *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*;[36]
- *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*;[37]
- *Cross-Device Tracking: A Federal Trade Commission Staff Report*;[38] and
- *Internet of Things: Privacy and Security in a Connected World*.[39]

The Commission recently explored consumer privacy issues through a series of hearings on *Competition and Consumer Protection in the 21st Century*,[40] and it is currently examining

---

[31] FTC WORKSHOP, *Student Privacy and Ed Tech* (Dec. 1, 2017), https://www.ftc.gov/news-events/press-releases/2017/10/ftc-department-education-announce-workshop-explore-privacy-issues.
[32] FTC WORKSHOP, *Fall Technology Series: Drones* (Oct. 13, 2017), https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones.
[33] FTC WORKSHOP, *Fall Technology Series: Smart TV* (Dec. 7, 2016), https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv.
[34] *E.g.*, FTC CONFERENCE, *PrivacyCon 2019* (June 27, 2019), https://www.ftc.gov/news-events/events-calendar/privacycon-2019.
[35] FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[36] FTC, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.
[37] FTC, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.
[38] FTC, CROSS-DEVICE TRACKING: A FEDERAL TRADE COMMISSION STAFF REPORT (2017), *available at* https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.
[39] FTC, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (2017), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[40] FTC HEARING, *Hearing #12: The FTC's Approach to Consumer Privacy* (Apr. 9-10, 2019), https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-

whether it should update the COPPA Rule in light of emerging technologies and changing business practices in the online children's marketplace.[41]

III. Recommendations

NIST has proposed the Draft Privacy Framework as a voluntary tool intended to help organizations start a dialogue about managing privacy risks.[42] We recognize that the Draft Privacy Framework is the first step of many, and that NIST plans to continue its work in a number of areas, as reflected in its Proposed NIST Privacy Framework Roadmap Topic Areas.[43] With that in mind, we offer the following comments and recommendations on the Draft Privacy Framework.

As a preliminary matter, we agree with NIST's approach of creating a flexible framework that allows organizations to tailor their privacy program to the individual needs of their business, their data processing practices, and their business environment. Privacy programs are not one-size-fits-all, but rather must be tailored to the size and complexity of the organization, the scope and nature of its data processing activities, and the volume and sensitivity of the consumer data at stake.[44]

---

february-2019; *see also* Press Release, Fed. Trade Comm'n, FTC Announces Hearings on Competition and Consumer Protection in the 21st Century (June 20, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st.

[41] FTC WORKSHOP, *The Future of the COPPA Rule: An FTC Workshop* (Oct. 7, 2019), https://www.ftc.gov/news-events/events-calendar/future-coppa-rule-ftc-workshop.

[42] *E.g.*, DRAFT PRIVACY FRAMEWORK, at 3 (the Core functions "enables a dialogue… about important privacy protection activities and desired outcomes.").

[43] NIST, PROPOSED NIST PRIVACY FRAMEWORK ROADMAP TOPIC AREAS (2019), *available at* https://www.nist.gov/sites/default/files/documents/2019/06/26/pf-roadmap-areas-06.26.2019.pdf.

[44] *See e.g.*, *In re Uber Technologies, Inc.*, Case No. C-4662 (F.T.C. Oct. 26, 2018) (Decision and Order), *available at* https://www.ftc.gov/system/files/documents/cases/152_3054_c4662_uber_technologies_revised_decision_and_order.pdf (requiring implementation of privacy program that "contain controls and procedures appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Personal Information"); *FTC et al. v. Vizio, Inc.*, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) (Decision and Order), *available at* https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf (same).

We also agree with the Draft Privacy Framework's recognition that privacy programs need to evolve with an organization's changing practices and business environment.[45] The Commission's recent settlement with Musical.ly, now known as TikTok, is illustrative. In that case, the company launched a lip-synching app that was not necessarily targeted to kids when it was launched. At some point, however, it became readily apparent that a large percentage of the app's audience consisted of children under 13. Many companies developing apps with broad appeal may find themselves in this position. A risk assessment up front may justify a decision that the company does not need to obtain parental consent under COPPA, but an ongoing assessment may catch changes in user bases, technologies, or content that would suggest the need for additional compliance measures.[46]

While we commend NIST's overall approach and believe that the Framework will provide important guidance to business, we have five suggestions for clarifying the Draft Privacy Framework that NIST may want to consider.

First, we recommend that NIST consider clarifying that "privacy breaches," generally defined as "unauthorized access to information," should be considered at each step of the Framework. Currently, the Draft Privacy Framework addresses privacy risks, defined as "the likelihood that individuals will experience problems resulting from data processing, and the impact should they occur," only generally.[47] Although privacy breaches are a subset of privacy

---

[45] *See, e.g., In re Uber Technologies, Inc.*, Case No. C-4662 (F.T.C. Oct. 26, 2018) (Decision and Order), *available at* https://www.ftc.gov/system/files/documents/cases/152_3054_c4662_uber_technologies_revised_decision_and_order.pdf (requiring company to regularly monitor effectiveness of privacy program, and make adjustments as necessary in light of that monitoring, changes to the company's business operations or arrangements, or "any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the privacy program"); *FTC et al. v. Vizio, Inc.*, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) (Stipulated Order), *available at* https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf (same).

[46] *See United States v. Musical.ly*, No. 2:19-cv-01439 (C.D. Cal. Feb. 27, 2019) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/musical.ly_complaint_ecf_2-27-19.pdf.

[47] DRAFT PRIVACY FRAMEWORK, at 30 (Appendix B: Glossary).

risks,[48] the Draft Privacy Framework suggests that privacy breaches may need to be addressed only in the Protect – P Core Function, which more directly describes controls relating to data security.

For example, the Draft Privacy Framework currently states: "There are five Functions: Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P. The first four can be used to manage privacy risks arising from *data processing*, while Protect-P can help organizations manage privacy risks associated with *privacy breaches*."[49] The risk of unauthorized access to information, however, is one of the most significant privacy risks against which organizations need to safeguard, and should be addressed at each step of the Draft Privacy Framework. For example, failing to address the risk of unauthorized access at the assessment or governing stage of the Framework is likely to result in an organization's failure to properly control for that risk. While we understand that NIST wants to explain how organizations can use the Draft Privacy Framework alongside NIST's Cybersecurity Framework,[50] we believe that clarifying the discussion of privacy risks and privacy breaches would be useful, particularly for organizations that may not also use NIST's Cybersecurity Framework.

Second, we recommend that NIST consider clarifying that an organization's risk assessment, safeguards, and other related procedures for managing privacy risks should account for the sensitivity of the consumer data that it is processing. Generally, collecting, using, or sharing sensitive information, such as precise geolocation data, biometric data, or health information, poses greater privacy risks to individuals and requires greater measures to safeguard it. Currently, the Draft Privacy Framework describes an approach where organizations address

[48] *E.g.*, *id.* at 6 (Figure 2).
[49] *See id.* at 5 (emphasis in original); *see also id.* at 10 (Identify-P Function relates to developing "the organizational understanding to manage privacy risk for individuals arising from *data processing*") (emphasis added).
[50] NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY VERSION 1.1 (2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

privacy risks by considering potential problems individuals could experience from data processing.[51] This outcome-based approach is useful, particularly in situations where even non-sensitive data can become sensitive based on how it is collected, used or shared. However, we recommend expanding this approach to include an explicit consideration of the sensitivity of data, which can help predict risky outcomes

For example, in the FTC enforcement action against Lenovo, the laptop manufacturer preinstalled "man-in-the-middle" software that injected ads on certain shopping websites. While the data used for this limited purpose was generally non-sensitive, the software accessed all of the laptop users' internet browsing activity, including login credentials, financial account information, health information, and the content of communications. The Commission alleged, among other things, that Lenovo's privacy practices were unfair because the company did not provide consumers with sufficient notice and consent mechanisms appropriate to processing such sensitive information.[52]

In deciding whether to install "man in the middle" software in the future, a company using an "outcomes-based approach" without specifically considering the sensitivity of the data may not accurately predict the privacy risks of collecting sensitive data if the software would only be used to serve ads. But, if the company were to focus on the objective sensitivity of the data collected by the software as part of its assessment of potential problems for consumers and the impact should those problems occur, the company may be more likely to accurately consider the privacy risks associated with that collection. While we note that the Draft Privacy Framework does mention considering data sensitivity as part of an organization's risk

[51] *E.g.*, DRAFT PRIVACY FRAMEWORK, at 6.
[52] *See In re Lenovo, Inc.*, Case No. C-4636 (F.T.C. Sept. 13, 2017) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/1523134_c4636_lenovo_united_states_complaint.pdf.

assessment,[53] we believe a more robust discussion of this concept would be useful. For example, discussing data sensitivity could be helpful, among other places, where the Framework discusses the approach of responding to privacy risks by "avoiding the risk."[54] NIST may want to consider providing an example of avoiding the risk by companies deciding to limit the collection of sensitive data.

Third, we recommend NIST consider offering a more detailed discussion of the analysis an organization should undertake as part of the Draft Privacy Framework's Communicate-P Core Function, which is intended to enable organizations and individuals to have a "reliable understanding" of how data are processed.[55] In our experience, ensuring that organizations and individuals have an understanding of a company's actual data processing practices is critical to a successful privacy framework. NIST may therefore want to consider posing a series of questions to help shape its Communicate-P Core Function, such as,

- Given the context of the organization's interaction with consumers, what would be their reasonable expectations regarding the organization's data processing practices (including collection, use, sharing, and storage)?
- What are the organization's public-facing representations regarding its data processing practices and are those representations prominent and understandable? and
- Are the organization's actual data processing practices in alignment with individual expectations and public-facing representations?

[53] *See* DRAFT PRIVACY FRAMEWORK, at 22 (Identify-P Core, Subcategory ID.RA-P1), and 36 (Appendix D - Conducting Privacy Risk Assessments).
[54] *See id.*, at 6-7 ("Avoiding the risk (e.g., organizations may determine that the risks outweigh the benefits, and forego or terminate the data processing")).
[55] *See id.* at 10; *see also id.* at 26 (Communicate-P Core, Subcategory CM.AW-P1 states, "Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.").

We believe that a more robust discussion of this key function is important because, in our experience, one of the most common privacy violations committed by organizations occurs when they fail to accurately describe how they collect, use, or share consumer data.

For example, in the FTC's recent enforcement action against Facebook, Inc., the FTC alleged that the company violated the FTC Act and a prior FTC order when it collected, used, or shared consumer data in a manner contrary to its promises to users.[56] The Commission alleged that the company had promised to share certain consumer data only with a user's "Friends," but in fact, also shared that data with app developers used by those Friends. Similarly, when the company collected certain telephone numbers for the stated purpose of improving account security, such as for two-factor authentication, it also used those telephone numbers for the undisclosed purpose of advertising. The Commission assessed a $5 billion civil penalty for Facebook's alleged violations of the Commission's prior order.[57] In addition to undermining consumer trust, organizations can incur significant legal risk if they do not live up to their privacy promises and do not accurately communicate how consumer data is collected, used, or shared.[58]

Fourth, we recommend that NIST consider clarifying that the Govern – P Core Function of the Framework includes considering the designation of specific individual(s) to be in charge

[56] *United States v. Facebook, Inc.*, No. 1:19-cv-02184, (D.D.C. Jul. 24, 2019) (Stipulated Order), *available at* https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

[57] The Commission could assess civil penalties against Facebook because its privacy practices violated a prior Commission order. 15 U.S.C. § 45(l). Privacy violations may also be subject to civil penalties under COPPA, 15 U.S.C. § 6502(c), and the FCRA, 15 U.S.C. § 1681(s)(a)(2)(A).

[58] *See, e.g., United States v. Facebook, Inc.*, No. 1:19-cv-02184, (D.D.C. Jul. 24, 2019) (Stipulated Order), *available at* https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf; *see also In re Unrollme, Inc.*, FTC No. 172 3139 (Aug. 8, 2019) (Complaint), *available at* https://www.ftc.gov/system/files/documents/cases/172_3139_unrollme_complaint_8-8-19.pdf (alleging company failed to inform consumers that it would collect, maintain, and sell information from users' email receipts while providing unrelated email subscription management services).

of creating, implementing, and maintaining the privacy program.[59] Currently, the Draft Privacy Framework describes assigning responsibilities to a cross-functional team to implement an organization's privacy policies, which is generally an effective approach. However, it is important for the Draft Privacy Framework to explicitly state that specific individual(s) should be designated as responsible for overseeing the creation, implementation, and maintenance of the privacy program across the entire company.

For example, the first case example in the Hypothetical NIST Privacy Framework Use Case Profiles[60] ("Hypothetical Case Profiles") shows a hypothetical cross-functional team, including legal team members, product engineers and management, working seamlessly together to discuss and implement privacy policies for a new dashboard application. There does not appear to be anybody driving implementation of the privacy program, but various team members nevertheless notice gaps in the data map that need addressing even when those gaps fall out of their assigned area of responsibility. In our enforcement experience, this is the exception and not the norm. We believe that without someone in charge of creating, implementing and maintaining an organization's privacy program, it is more likely that such gaps would fall through the cracks. Even adequately assigned responsibilities may go unfinished as client-driven or other work takes priority or staff turnover results in new employees being unaware of their privacy-related responsibilities. Without someone in charge of the privacy program, an organization also is less likely to update its privacy-related policies or practices in response to changes in its products,

---

[59] *See, e.g.*, *In re Uber Technologies, Inc.*, Case No. C-4662 (F.T.C. Oct. 26, 2018) (Decision and Order), *available at* https://www.ftc.gov/system/files/documents/cases/152_3054_c4662_uber_technologies_revised_decision_and_order.pdf (requiring designation of employee or employees to "coordinate and be responsible" for the privacy program); *FTC et al. v. Vizio, Inc.*, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), *available at* https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf (same). *Cf.* 16 C.F.R. § 314.4(a) (requiring certain financial institutions under the FTC's jurisdiction to "[d]esignate an employee or employees to coordinate" information security program).

[60] NIST, HYPOTHETICAL NIST PRIVACY FRAMEWORK USE CASE PROFILES (2019) ("HYPOTHETICAL CASE PROFILES"), *available at* https://www.nist.gov/sites/default/files/documents/2019/06/26/pf-hypothetical-use-cases-06.26.2019.pdf.

practices or business environment. As a result, the Commission regularly requires organizations that are under order for privacy violations to designate a person or persons to be in charge of creating, implementing, and maintaining the privacy program.[61]

Finally, we recommend NIST consider clarifying the Draft Privacy Framework's discussion regarding 'current' and 'target' privacy profiles to reflect that performing a comprehensive risk assessment is a necessary first step before making decisions about which privacy controls should be implemented and the timetable for such implementation. Currently, the Draft Privacy Framework suggests that it may be acceptable for an organization to not have a fully-implemented privacy program on Day 1.[62] We agree that not all aspects of the Draft Privacy Framework may apply to an individual organization, and that it may not be feasible for an organization to implement all privacy-related controls and safeguards at once. However, reviewing all aspects of the company's operations that process consumer data, including inventorying all consumer data that is collected, stored or shared, and then assessing the privacy risks of that data processing, is an important first step before an organization can decide which privacy controls need to be implemented, and in which order of priority.

For example, in the second case example in NIST's Hypothetical Case Profiles, Company B allows its most pressing business or customer needs to drive its decisions about which specific privacy controls to implement, and decides not to do a full risk assessment of its data processing activities until a later time. In our enforcement experience, this can allow significant vulnerabilities and privacy risks affecting large numbers of consumers to be left unaddressed

---

[61] *E.g.*, *United States v. Facebook, Inc.*, No. 1:19-cv-02184, (D.D.C. Jul. 24, 2019) (Stipulated Order), *available at* https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf; *In re Uber Technologies, Inc.*, Case No. C-4662 (F.T.C. Oct. 26, 2018) (Decision and Order), *available at* https://www.ftc.gov/system/files/documents/cases/152_3054_c4662_uber_technologies_revised_decision_and_order.pdf; *FTC et al. v. Vizio, Inc.*, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017) (Stipulated Order), *available at* https://www.ftc.gov/system/files/documents/cases/170206_vizio_stipulated_proposed_order.pdf.

[62] *See* DRAFT PRIVACY FRAMEWORK, at 10-11; *see also* HYPOTHETICAL CASE PROFILES, at 5-6.

while relatively small privacy risks are tackled. In this particular example, Company B developed apps used in Europe and Asia, thereby raising additional potential concerns about fully complying with the General Data Protection Rule and the EU-U.S. Privacy Shield Framework, and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules (APEC CBPR). A full risk assessment of Company B's data-processing activities would provide the necessary foundation for organizations to make informed decisions on managing their privacy risks.

Conclusion

Thank you again to NIST and to all of the stakeholders that contributed to this process. The FTC continues to devote substantial resources in this area and looks forward to working with NIST to promote privacy of consumer data.