From: Katie McInnis <katie.mcinnis@consumer.org>
Sent: Thursday, October 24, 2019 3:02 PM
To: privacyframework <privacyframework@nist.gov>
Subject: Consumer Reports's Comments

Dear Sir or Madam,

Our comments on the preliminary draft of the Privacy Framework are attached to this email.

Thanks,
Katie McInnis

--

Katie McInnis

Policy Counsel 202.238.9250 | pronouns: she/her

Image removed by sender.@katielmcinnis

CR.org CR.org/advocacy

October 24, 2019

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

Re: NIST Privacy Framework: Preliminary Draft Comments

Dear Ms. Katie MacFarland:

Consumer Reports,[1] writes to respond to the request for comments on the preliminary draft of the Privacy Framework from the National Institute of Standards and Technology (NIST). We appreciate this chance for comment and hope that our comments prove useful to NIST.

Although we appreciate the creation of a preliminary Privacy Framework, the Framework is limited in its usefulness since it lacks any substantive guidance for companies about what constitutes positive or harmful data processing. In order to properly incentivize or guide businesses to process data with the consumer's interest in mind, the Framework should seek to limit data processing to context and reasonable consumer expectations. Without a limit on out-of-context data processing, the Framework serves to only classify the kind of data processing companies are already engaging in. For example, the Weather Channel app "told users that sharing their locations would let them get personalized local weather reports" but in fact the company used individual's location information "for unrelated commercial purposes, like targeted marketing and analysis for hedge funds."[2] A reasonable user would expect that sensitive location information was not being shared for unrelated purposes, but rather only used to give them location-based weather information. In addition, we have also seen companies like Facebook[3] and Twitter[4] collect

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its advocacy work in the areas of privacy, telecommunications, financial services, food and product safety, health care, among other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

[2] Jennifer Valentino-DeVries & Natasha Singer, *Los Angeles Accuses Weather Channel App of Covertly Mining User Data*, N.Y. TIMES (Jan. 3, 2019), https://www.nytimes.com/2019/01/03/technology/weather-channel-app-lawsuit.html.

[3] Natasha Lomas, *Yes Facebook is Using Your 2FA Phone Number to Target You with Ads*, TECHCRUNCH (Sept. 27, 2018), https://techcrunch.com/2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/.

[4] Jon Fingas, *Twitter Admits Your Phone Number May Have Been Used for Targeting Ads*, ENGADGET (Oct. 8, 2019), https://www.engadget.com/2019/10/08/twitter-phone-numbers-possibly-used-for-ad-targeting/.

consumers' phone number for the purposes of multi-factor authentication and then use those phone numbers to target advertisements. Examples like these demonstrate that companies need to look first to consumer expectations and whether the company's actions contravened such expectations (and privacy controls) in order to assess privacy outcomes. Two categories of data out-of-context data processing that consumers might object to are (1) expansive, intransparent data sharing and selling arrangements,[5] and (2) excessive first-party data collection, use, and retention. Unfortunately, the opaque risk assessment matrix presented in the Framework is not designed to address either of concerns.

Furthermore, we urge NIST to (1) address our concerns about the preliminary draft of the Privacy Framework; (2) not tether consumer privacy concerns to subjective assessments of privacy risk or harm; (3) call for comprehensive privacy legislation in order to sufficiently protect consumers; and (4) reconsider the concerns raised in our response to NIST's Request for Information (RFI) in January 2019 since these concerns were not met by the preliminary Privacy Framework.

The Preliminary Draft of the Privacy Framework Does Not Achieve Its Stated Goals

In NIST's request for comment, the organization asks for feedback on whether "this preliminary draft adequately define outcomes that: "…strengthen individuals' privacy protection; enable effective organizational use…" As stated earlier in our comments, the Framework does not attain these goals.

This document does not define outcomes that strengthen individuals' privacy protections—indeed it provides no normative guidance around outcomes at all. Without such guidance, the Framework will be highly limited in its usefulness. Rather, by focusing only on privacy *process*, the Framework works to codify existing data processing practices without (1) sufficiently indicating the danger posed to consumers and society from some of these processes or (2) incentivizing companies to limit the amount of data they process in the first instance. While organizational structures are important, they cannot be effective in delivering privacy without clear outcomes, rules, or principles. The individual consumer who will be affected by a company's data processing needs to be better oriented within the Framework as a whole. Already companies are not sufficiently incentivized to protect or respect consumer privacy—a Framework that does not focus on how data processing will affect the consumer will fail to encourage companies to better prioritize consumer privacy. Indeed, on page 12, lines 417-19 of the Framework, NIST states that

[5] For example, Privacy International found that 61 percent of the apps they tested were automatically sending data to Facebook about the user and their use of the app. This sharing happened without disclosure to the end user and occurred whether or not the user had a Facebook account. (*Investigating Apps Interactions with Facebook on Android*, PRIVACY INT'L (Dec. 2018), https://privacyinternational.org/appdata.) Privacy International also found that many reproductive health/menstruation-tracking apps were also sharing highly personal information with Facebook, without any transparency to the user or ability to stop this sharing. (*No Body's Business But Mine: Menstruation Apps Are Sharing Your Data*, PRIVACY INT'L (Sept. 9, 2019), https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data.)

the Privacy Framework can "help organizations answer the fundamental question, 'How are we considering the impacts to individuals as we develop our systems, products, and services?'" If that is the goal of this Framework, then there needs to be more here about how consumers are affected in order to better communicate to businesses how their data processing and collection affects consumers in myriad ways. In order for the Framework to be effective for organizations it must include substantive guidance on what kinds of data processing are acceptable and which are harmful/unacceptable.

Consumer Privacy Concerns Cannot be Tethered to Subjective Assessments of Risk or Harm Since Data Collection in the First Instance Presents a Privacy Risk to the Consumer

As an initial matter, we encourage NIST and public and private organizations to not tether most consumer protections to subjective assessments of privacy risk and harm. Rather, any privacy framework should recognize that consumers will always have a privacy *interest* in data collection, use, retention, or sharing because once private information is in the hands of another there is *always* a chance of some misuse. For example, data collected in the past could be publicly breached, accessed through mandatory legal process, or used for price discrimination to decrease a consumer's share of consumer surplus from any transaction.[6] From the perspective of the consumer, there is *necessarily* privacy risk when someone else has their data. With limited exceptions, a privacy law's protections should not be contingent upon a company's own (and necessarily biased toward its own interests) evaluation of how significant those risks are.

And for this very reason, while the United States has fewer privacy protections than other countries, the laws we have passed have not been artificially constrained by *ad hoc* determinations of privacy risks or harms. The Wiretap Act,[7] for example, does not ask potential eavesdroppers to weigh the relative harms and benefits to determine the legality of intercepting a potential communication. Nor does the Video Privacy Protection Act[8] allow someone to make subjective judgments about how "harmful" the release of someone's viewing habits might be. Rather, the laws' protections apply *per se*, obviating any risk analysis, leading to clearly stronger protections and more clear and predictable rules for everyone.

Because the proliferation of data is, to the consumer, unpredictable and hard to control, the law's protections should apply *per se* protections for privacy intrusions. Potential harms to the consumer may not be obvious when the data is first collected because data collected in the past could be used in new and unexpected ways. In addition, risk assessment introduces unnecessary uncertainty into the law, both for companies and consumers (who might not necessarily agree on what constitutes an acceptable privacy risk).

---

[6] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY FORUM BIG DATA & PRIVACY WORKSHOP PAPER COLLECTION (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[7] 18 U.S.C. § 2511.

[8] 18 U.S.C. § 2710.

Furthermore, in practice these risk assessments will be made (often opaquely) by companies with skewed incentives to allow data processing and disregard consumer interests. Even then, such assessments will not always be rational: businesses are run by humans, and humans exhibit a natural human tendency to overestimate a small chance of something good happening and to underestimate the chances of something bad happening.[9] This is a core tenet of behavioral economics, and explains why people play the lottery despite the odds and decreasing marginal value of money, or do not buckle their seat belts despite the low cost and tremendous risk. Translated to data privacy, companies will tend to undervalue data security, and undervalue data minimization as well, discounting the likelihood of a security event, but overly optimistic about the potential for found wealth in data troves. Therefore, a consumer privacy protections framework should reflect the reality of human nature, and eliminate opportunities for skewed incentives and irrational tendencies to weaken privacy protections.

Security, on the other hand, is one area where a risk-based framework is reasonable. Security necessarily involves a balancing of costs and the potential harms from inadvertently exposed data. Companies should consider possible ill effects when they are deciding how much to spend on a potential loss. Privacy risk may also be appropriately considered when assessing penalties for violations, as penalties are typically determined by considering a host of factors, including the likelihood of adverse consequences for consumers as a result of prohibited behavior.

Since a Voluntary Framework Will Not Sufficiently Protect Consumers, NIST Should Call for Privacy Legislation

While NIST does not have the authority to mandate compliance with its framework, any "non-voluntary" framework is unlikely to materially advance privacy protections for consumers; NIST should acknowledge these limitations and call for the enactment of affirmative privacy legislation. Additionally, as stated above, privacy protections should not be tethered to subjective evaluations of risk.

Reconsider Our Response to NIST's RFI in January 2019

Our comments provided to NIST on January 14, 2019 have been attached to the end of these comments as an addendum.

[9] Klaus Mathis & Ariel David Steffen, *From Rational Choice to Behavioural Economics*, UNIV. OF LUCERNE (2015) https://www.unilu.ch/fileadmin/fakultaeten/rf/mathis/Dok/1_Mathis_Steffen_From_Rational_Choice_to_Behavioural_Economics.pdf.

Thank you for the opportunity to respond to your preliminary draft of the Privacy Framework.

Sincerely,

Katie McInnis
Policy Counsel

Consumer Reports
Suite 500
1101 17th Street, NW
Washington, DC 20036

Addendum

January 14, 2019

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

Re: Developing a Privacy Framework, Docket Number 181101997-8997-01

Dear Ms. Katie MacFarland,

Consumer Reports[10] writes to respond to the request for information on Developing a Privacy Framework from the National Institute of Standards and Technology. Below we have responded to each relevant query posed in the Request for Information. We appreciate this chance for comment and hope that our comments prove useful to NIST.

Organizational Considerations

1. **The greatest challenges in improving organizations' privacy protections for individuals;**
2. **The greatest challenges in developing a cross-sector standards-based framework for privacy;**
3. **How organizations define and assess risk generally, and privacy risk specifically;**

As an initial matter, we encourage NIST and public and private organizations to not tether most consumer protections to subjective assessments or privacy risk and harm. Rather, any privacy framework should recognize that consumers will always have a privacy *interest* in data collection, use, retention, or sharing because once private information is in the hands of another there is *always*

[10] Consumer Reports is an expert, independent, nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. As the world's largest independent product-testing organization, it conducts its policy and mobilization work in the areas of privacy, telecommunications, financial services, food and product safety, and other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

a chance of some misuse. For example, data collected in the past could be publicly breached, accessed through mandatory legal process, or used for price discrimination to decrease a consumer's share of consumer surplus from any transaction.[11] From the perspective of the consumer, there is *necessarily* privacy risk when someone else has their data. With limited exceptions, a privacy law's protections should not be contingent upon a company's own (and necessarily biased toward its own interests) evaluation of how significant those risks are.

And for this very reason, while the United States has fewer privacy protections than other countries, the laws we have passed have not been artificially constrained by *ad hoc* determinations of privacy risks or harms. The Wiretap Act,[12] for example, does not ask potential eavesdroppers to weigh the relative harms and benefits to determine the legality of intercepting a potential communication. Nor does the Video Privacy Protection Act[13] allow someone to make subjective judgments about how "harmful" the release of someone's viewing habits might be. Rather, the laws' protections apply *per se*, obviating any risk analysis, leading to clearly stronger protections and more clear and predictable rules for everyone.

Because the proliferation of data is, to the consumer, unpredictable and hard to control, the law's protections should apply *per se* protections for privacy intrusions. Potential harms to the consumer may not be obvious when the data is first collected because data collected in the past could be used in new and unexpected ways. In addition, risk assessment introduces unnecessary uncertainty into the law, both for companies and consumers (who might not necessarily agree on what constitutes an acceptable privacy risk).

Furthermore, in practice these risk assessments will be made (often opaquely) by companies with skewed incentives to allow data processing and disregard consumer interests. Even then, such assessments will not always be rational: businesses are run by humans, and humans exhibit a natural human tendency to overestimate a small chance of something good happening and to underestimate the chances of something bad happening.[14] This is a core tenet of behavioral economics, and explains why people play the lottery despite the odds and decreasing marginal value of money, or do not buckle their seat belts despite the low cost and tremendous risk. Translated to data privacy, companies will tend to undervalue data security, and undervalue data minimization as well, discounting the likelihood of a security event, but overly optimistic about the potential for found wealth in data troves. Therefore, a consumer privacy protections framework

---

[11] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY FORUM BIG DATA & PRIVACY WORKSHOP PAPER COLLECTION (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[12] 18 U.S. § 2511.

[13] 18 U.S.C. § 2710.

[14] Klaus Mathis & Ariel David Steffen, *From Rational Choice to Behavioural Economics*, UNIV. OF LUCERNE (2015) https://www.unilu.ch/fileadmin/fakultaeten/rf/mathis/Dok/1_Mathis_Steffen_From_Rational_Choice_to_Behavioural_Economics.pdf.

should reflect the reality of human nature, and eliminate opportunities for skewed incentives and irrational tendencies to weaken privacy protections.

Security, on the other hand, is one area where a risk-based framework is reasonable. Security necessarily involves a balancing of costs and the potential harms from inadvertently exposed data. Companies should consider possible ill effects when they are deciding how much to spend on a potential loss. Privacy risk may also be appropriately considered when assessing penalties for violations, as penalties are typically determined by considering a host of factors, including the likelihood of adverse consequences for consumers as a result of prohibited behavior.

4. **The extent to which privacy risk is incorporated into different organizations' overarching enterprise risk management;**
5. **Current policies and procedures for managing privacy risk;**
6. **How senior management communicates and oversees policies and procedures for managing privacy risk;**
7. **Formal processes within organizations to address privacy risks that suddenly increase in severity;**
8. **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;**

Attributes 1-3 are reasonable attributes to include in a privacy framework. While NIST does not have the authority to mandate compliance with its framework, any "non-voluntary" framework is unlikely to materially advance privacy protections for consumers; NIST should acknowledge these limitations and call for the enactment of affirmative privacy legislation. Additionally, as stated above, privacy protections should not be tethered to subjective evaluations of risk.

To the extent that "outcome-based" means that companies should not put the onus on users to manage privacy concerns, this attribute is sensible, and the framework should get companies to accord their default practices to align with consumers' reasonable expectations and preferences.

9. **What an outcome-based approach to privacy would look like;**

An outcome-based approach to privacy would, ideally, be based in assessments as to whether or not the organization respected consumers' privacy preferences and choices along with an assessment of how secure the data is. In addition, outcomes-based should mean that data practices are consistent with consumers' reasonable expectations. For example, the Weather Channel app "told users that sharing their locations would let them get personalized local weather reports"[15] but

[15] Jennifer Valentino-DeVries & Natasha Singer, *Los Angeles Accuses Weather Channel App of Covertly Mining User Data*, N.Y. TIMES (Jan. 3, 2019), https://www.nytimes.com/2019/01/03/technology/weather-channel-app-

in fact the company used individual's location information "for unrelated commercial purposes, like targeted marketing and analysis for hedge funds."[16] A reasonable user would expect that sensitive location information was not being shared for unrelated purposes, but rather only used to give them location-based weather information. Examples like this one demonstrate that companies need to look first to consumer expectations and whether the company's actions contravened such expectations (and privacy controls) in order to assess privacy outcomes.

10. **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;**
11. **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;**
12. **Any mandates to use specific standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles or conflicts between requirements and desired practices;**
13. **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;**
14. **The international implications of a Privacy Framework on global business or in policymaking in other countries; and**
15. **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.**

<u>Structuring the Privacy Framework</u>

16. **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?**
17. **Whether any aspects of the Cybersecurity Framework could be a model for this Privacy Framework, and what is the relationship between the two frameworks.**

---

lawsuit.html.

[16] Jennifer Valentino-DeVries, et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

18. **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 [6] 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?**

Consumer Reports supports some combination of (a) the information life cycle, (b), principles such as the Fair Information Privacy Practices (FIPPs), and (d) uses cases or design patterns. Information life cycle focuses on moments of collection, retention, sharing, and deletion. Principles like the FIPPs are essential to frame privacy practices as they go beyond risk. And use cases/patterns are useful to show good and bad practices (e.g., the Federal Trade Commission's Dot Com Disclosures[17]).

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.**

[17] *.Com Disclosures*, FED. TRADE COMM'N (Mar. 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf

Deidentification;

Consumer Reports supports the inclusion of deidentification in this list of specific privacy practices. However, NIST should expand on what deidentification means in order to require higher levels of transparency as to deidentification practices and better protections for making de-identified data public. In order for a company to assert that any such data is deidentified they should be required to document the deidentification methods used to provide for meaningful external accountability. Companies should be required to do this in order to gain the benefits of extra data retention, sharing, or use of purportedly deidentified data.

In addition, while deidentification of consumer data is a valuable goal since it allows companies to extract value from consumer data while minimizing privacy and security impacts, there should be a higher standard of deidentification when such data is made public. This is an issue that is not unique to NIST. For instance, the Federal Trade Commission's three-part test[18] does not control for situations in which the data is made public. The three-part test should include rules for situations in which the deidentified data is later made public and these rules should be strong enough to prevent re-identification in the future. For instance, the test could be expanded to require that there is no "reasonable foreseeability" that the data could be reidentified.

Enabling users to have a reliable understanding about how information is being collected, stored, used, and shared;

The best way for companies to provide choices and a reliable understanding of what is being collected without overwhelming the consumer is to accord data collection, in the first instance, with consumer expectations. If a company wants to engage in additional, non-contextual data collection or sharing, it should obtain the consumer's permission to do so. This request should be relatively rare, as most consumers are unlikely to want unrelated data collection absent a compelling value proposition.

Furthermore, in order to strike the balance of effective consumer information without overwhelming the user, companies should avoid the use of user interfaces that deceive or manipulate users into acting in a way that benefits the company and not the individual. These dark patterns of design[19] can nudge users away from choosing the privacy-protective choices made

---

[18] "...data is not 'reasonably linkable' to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits to not try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data." *Protecting Consumer Privacy in an Era of Rapid Change*, FED. TRADE COMM'N (Mar. 2012), iv, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[19] "To put it plainly, dark pattern design is deception and dishonesty by design…The technique, as it's deployed online today, often feeds off and exploits the fact that content-overloaded consumers skim-read stuff they're presented with, especially if it looks dull and they're in the midst of trying to do something else — like sign up to a service, complete a purchase, get to something they actually want to look at, or find out what their friends have sent them.
Manipulative timing is a key element of dark pattern design. In other words *when* you see a notification can determine how you respond to it. Or if you even notice it. Interruptions generally pile on the cognitive overload — and deceptive

available to them. The Norwegian Consumer Council (NCC) published an in-depth report on the use of these dark patterns in June 2018, noting that big tech companies like Facebook and Google utilize tools like "privacy intrusive default settings, misleading wording, giving users an illusion of control, hiding away privacy-friendly choices, take-it-or-leave-it choices, and choice architectures where choosing the privacy friendly option requires more effort for the users" in order to nudge or compel certain actions by the user.[20] This is not the first time Facebook was the focus of criticism due to their use of dark patterns in design: in 2016 Facebook used a consent flow that made it appear that WhatsApp users' did not have the opportunity to opt-out by using a hard-to-spot alternative button (and a buried opt-out) in order to mask the privacy implications of linking a WhatsApp account with a Facebook account, which included sharing user data with Facebook for the purposes of ad targeting.[21] Dark patterns like the ones detailed in the NCC's report are also used by smaller and medium-sized online service providers or manufacturers in order to steer users through a consent flow in a way that is beneficial to the company.[22]

In addition, although lengthy disclosures at the initial point of interaction have not fostered sufficient consumer understanding, companies should still be required to provide these disclosures and be more transparent and explicit about their data collection and practices. While few consumers read privacy policies, detailed disclosures should be written for the groups that already read them: regulators, reporters, and consumer-protection organizations like Consumer Reports. All of these entities are engaged in monitoring privacy policies for policy, consumer protection, and investment purposes and should continue to do so, but with more explicit information at hand. Today's policies are often vaguely expansive, providing little reliable concrete information about companies' actual practices. A transparency mandate to provide more precise information could remedy that.

Since consumers currently lack transparency for how their data is collected, used, shared, stored, and deleted, individual Americans need more transparency around those practices in addition to what specific information is being collected about them. While the California Consumer Privacy Act (CCPA) provides California residents with the ability to find out the categories and specific pieces of personal information that has been collected about them, any federal privacy framework should require more transparency from companies. In addition, the privacy policies that companies provide should specify what data they are collecting and when.

---

design deploys them to make it harder for a web user to be fully in control of their faculties during a key moment of decision." Natasha Lomas, *WTF is Dark Pattern Design?*, TECHCRUNCH (July 1, 2018), https://techcrunch.com/2018/07/01/wtf-is-dark-pattern-design/.

[20] *Deceived by Design*: *How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy*, NORWEGIAN CONSUMERS COUNCIL (June 27, 2018), *available at* https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/.

[21] Natasha Lomas, *WhatsApp to Share User Data with Facebook for Ad Targeting—Here's How to Opt Out*, TECHCRUNCH (Aug. 25, 2018), https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/.

[22] *See*, *e.g.*, *Hall of Shame*, DARK PATTERNS, https://darkpatterns.org/hall-of-shame (last visited Dec. 18, 2018).

Detailed disclosures will allow for experts to assess and provide consumers with better information and tools to evaluate and compare their privacy choices. For instance, in order to provide consumers with more information about their options, Consumer Reports and its partners developed The Digital Standard,[23] an open standard for testing products for privacy and security in order to help consumers make informed decisions in the marketplace. The testing includes assessments of a company's stated privacy practices in both the user interfaces and in their privacy policies. This effort depends on the transparency that privacy policies and user interfaces provide consumers. In addition, one of the important criteria under our Digital Standard is that the user can see and control everything the company knows about the individual. In order for a company's data practices to be responsible under the Standard, the company must enable the consumer to be able to know what user information the company is collecting, must only request and collect information that is needed to make the product or service work correctly, and must explicitly disclose every way in which it uses the individual's data.[24]

Enabling user preferences;

Please see our response to query 20 on *Control* below.

Setting default privacy configurations;

Privacy settings should be set to minimize the amount of data collected about the user by default. Data minimization, done correctly, would redistribute the onus of good data practices onto the company and off of the consumer. Consumers are already overwhelmed with the number of decisions they are asked to make. Consumers should be empowered to use products without fear that the service or product will mine and collect more data than the consumer would reasonably expect. Ever-present pop-up dialogs and byzantine user controls do not serve users well; instead, consumers should be entitled to expect that data collection and sharing will be limited to the context of their interactions with any given company.

Specifically, a business that collects a consumer's personal information should limit its collection and sharing of personal information with third parties to *what is reasonably necessary to provide a service or conduct an activity that a consumer has requested*. Additional data collection or sharing should only happen with a user's clear and informed permission. Such a principle could have narrow exceptions—such as allowing collection or sharing as is reasonably necessary for security or fraud prevention. Additionally, some related, operational processing of already-collected data should be allowed without bothering the user for permission—such as first-party analytics, research, and marketing.[25]

---

[23] *The Standard*, THE DIGITAL STANDARD, https://www.thedigitalstandard.org/the-standard (last visited Jan. 14, 2019).
[24] *Id*.
[25] However, due to the breadth of the security/fraud exception and the potential for this exception swallowing the rule, data collected or retained solely for security or fraud prevention should not be used for related operational purposes.

Use of cryptographic technology to achieve privacy outcomes—for example, the disassociability privacy engineering objective;

Just as deidentification methods need to be documented, so too does the use of cryptographic technology. In order to make use of these technologies, companies should publicly document the methods used in order to claim that the information has been sufficiently protected through such techniques.

19. Whether the practices listed above are widely used by organizations;

20. Whether, in addition to the practices noted above, there are other practices that should be considered for inclusion in the Privacy Framework;

In order to address the full range of consumer privacy interests and values, NIST should add a number of new principles to its Privacy Framework, including: data minimization, user control, data access and correction, data portability, and no discrimination or penalization for users who exercise privacy rights.

Data Minimization

NIST should data minimization the leading principle of its privacy framework to reflect the amount of work this one principle should shoulder. Please see our response to S*etting default privacy configurations* above for more on data minimization.

Control

Although data minimization should be doing most of the work in any privacy framework, if a company wants to engage in additional, non-contextual data collection or sharing, it should obtain the consumer's permission to do so. This request should be relatively rare, as most consumers are unlikely to want unrelated data collection absent a compelling value proposition. We urge industry and the NTIA to avoid a model that follows the cookie consent banners in Europe, which often confusingly conflate both contextual, first-party collection and usage with non-essential third-party sharing for advertising.

Since consumers do not expect their data to be shared by a company with a third party, such sharing should not occur without the consumer's prior affirmative consent. Therefore, under this principle the user's ability to control their personal information should extend to personal information that is obtained from third parties as well as first-party interactions. In addition, any data control requirement should include third parties. Without the inclusion of third-party data on individuals, this requirement is undermined by that loophole. Finally, consumers need the ability to request

---

This approach to consumer data dovetails with Professor Jack M. Balkin's concept of "information fiduciaries" in which the company must be loyal to the consumer's interests and show a duty of care to the data collected. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, FACULTY SCHOLARSHIP SERIES 5154 (2016), https://digitalcommons.law.yale.edu/fss_papers/5154.

deletion of their account information as one aspect of their ability to control their data.

Consumers should be entitled to the reasonable expectation that companies do not collect more or different types of data than what is reasonably necessary for a requested service. Therefore, companies should have to get the consumer's opt-in consent for additional data collection or sharing, in response to a dedicated prompt that is not tied to other boilerplate disclosures or other permissions, in order to conduct this excess data collection. A consumer's consent should be freely given. Further, as we discuss *infra* at the end of this question, we oppose pay-for-privacy schemes and urge NIST to include a prohibition against discriminatory treatment of a consumer on the basis of their exercise of these controls.

If a company wants to engage in out-of-context data collection or sharing, it should make a clear and compelling case to the consumer and only proceed with permission. An opt-out approach is inconsistent with consumer demands and expectations. If NIST insists on advocating for an opt-out regime, the control needs to be scalable in order for the consumers' choices to be uniformly implemented across the digital spectrum. Opt-outs should be powerful and universal. In the past, we have seen opt-outs that lack the ability to scale or the requirement that all entities respect the opt-out which fails to protect consumers. Unfortunately, as tracking technology has gotten more invasive, we have also seen the collapse of industry efforts to self-regulate. The same weaknesses that existed years ago in the online marketplace largely persist to this day: the rules only apply to coalition members; industry opt-outs are fragile and easily overridden; industry opt-outs only address usage and do not impose meaningful collection or retention limitations; and notice and privacy interfaces were seriously flawed.[26] One strong example of a powerful and universal opt-out for consumers is encapsulated in Senator Ron Wyden's discussion draft of the *Consumer Data Protection Act*,[27] which establishes a national Do Not Track system that would permit consumers to stop third-party companies from tracking them on the web by sharing data, selling data, or targeting advertisements based on their personal information. Furthermore, the bill requires the use of device-level signifiers such as "Do Not Track" instructions for unauthenticated consumer data divorced from real world identifiers.

Consumers should have policy controls that prevents companies from evading their tracking preferences.

Data Access and Correction

Consumers should have the ability to access the actual data that companies have on the individual

[26] *Statement of Justin Brookman Before the U.S. Senate Comm. On Commerce, Sci., and Transp.*, CTR. FOR DEMOCRACY & TECH. (Apr. 24, 2013), https://cdt.org/files/pdfs/Brookman-DNT-Testimony.pdf.

[27] *Consumer Data Protection Act, Discussion Draft*, SENATOR RON WYDEN (Nov. 1, 2018), https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf.

and not just categories of data. The California Consumer Privacy Act (CCPA), which goes into effect in 2020, provides Californians with important new consumer protections, including the right to request that companies provide consumers the categories and specific pieces of personal information collected about them.[28] A federal law or framework should expand those protections to all Americans.

Data Portability

In addition, data portability is not addressed in this Privacy Framework. Consumers need the ability to not only see what data companies have about them but also the right to take their consumer data elsewhere. Without this element, consumers will be locked into one service or product and will be unable to exercise their preferences. This is especially important with regards to consumers' ability to trust the companies they currently interact with. For example, a consumer could desire to move their data to another company due to a recent breach or misuse of their data by the current company they use or interact with. Without data portability, consumers will be blocked or highly disincentivized from exercising this option. In addition, data portability allows for greater competition in the marketplace. If consumers are not able to take their data to a new company, the market will strongly preference entrenched legacy organizations and not foster an innovative business landscape.

Finally, a comprehensive tenet on data access and correction should include some level of authentication for the end-user who is requesting access. While authentication is undesirable for other elements in these principles, the ability to assess the identity of the requestee is necessary to ensure the security of the data that the company controls about an individual. Without such a measure, malicious actors could gain access to the personal data companies have about an individual.

No Discrimination or Penalization

NIST's Privacy Framework should be revised to include a call for no discrimination or denial of service on the basis of a consumer exercising their privacy preferences and controls.

Privacy should not be a luxury good. Any enunciation of a privacy framework should include a prohibition against any discrimination with regards to the consumer or a denial of service for implementing their privacy choices. Pay-for-privacy schemes could also further exacerbate the untenable and unbalanced relationship between consumers and the companies that continually track them across on- and offline in order to create an intricate dossier of information about them. Any service plan that charges users more for making privacy-conscious choices will disproportionately affect lower-income households. Furthermore, pay-for-privacy plans will also

[28] *SB-1121, California Consumer Privacy Act of 2018*, CALIF. STATE LEGISLATURE (2018), http://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180SB1121.

serve to make monthly service plan or product costs less transparent and frustrate consumer efforts to comparison shop. Finally, although some online products and services will inherently lack some functionality if a consumer fully exercises all privacy protections provided, consumers should not be denied service or access on the basis of their personal data and privacy concerns.

21. **How the practices listed above or other proposed practices relate to existing international standards and best practices;**
22. **Which of these practices you see as being the most critical for protecting individuals' privacy;**

As stated above, NIST should make data minimization the leading principle of its privacy framework to reflect the amount of work this one principle should shoulder.

23. **Whether some of these practices are inapplicable for particular sectors or environments;**
24. **Which of these practices pose the most significant implementation challenge, and whether the challenges vary by technology or other factors such as size or workforce capability of the organization;**

In general, the most effective way to improve accountability within organizations is to provide for substantial external consequences for bad privacy practices. The costs for a business to comply with any privacy framework should not be overly expensive—rather the rules for any framework should be straightforward and easily understood. The threat of enforcement should incentivize companies to develop practices and procedures to best avoid legal liability. That said, a privacy law or framework may reasonably mandate some degree of internal assessment in order to push companies to meaningfully assess their data practices. Importantly, however, these process requirements cannot substitute for strong substantive protections.

25. **Whether these practices are relevant for new technologies like the Internet of Things and artificial intelligence; and**

All of the aforementioned practices are relevant for new technologies like connected devices and automated decision-making systems. The efficacy of any privacy framework would be immensely undermined if the principles of the framework only applied to some parts of the internet and digital products and not others.

Connected Devices

The presence and proliferation of connected devices for consumers, industrial operations, and public infrastructure implicates a range of privacy, security, safety, and legal accountability issues. Forefront among the issues IoT devices pose is safety. In addition, privacy and data security

practices that benefit and protect the consumer must be a priority for manufacturers, policy makers, and enforcement authorities.

Although consumers desire connected devices that can make their lives easier, more efficient, and more productive, consumers are unaware or unable to protect against the security concerns posed by vulnerable or outdated IoT devices and accompanying software. Currently, the safety of connected devices is often obscured or unknown to the common consumer. Consumers should be provided with effective and accurate information in order to select products based on security, safety, and privacy, in addition to the price, form, and function of a product. Because the safety of these products is hard for a consumer to measure but pose risks not only to their home networks but also their personal data, companies should be held accountable and compete against other similar companies on the basis of their data privacy and security standards.

Additionally, consumers should be able to buy connected products with confidence due to the possibly sensitive nature of the data trafficked through the device or due to the possibly vulnerable users of the connected product. For instance, a connected home device like a Google Home or an Amazon Echo has the potential to convey a lot of personal and sensitive information about an individual's buying, listening, and searching habits, in addition to audio information about activities within the home. Consumers often buy connected devices that are used by many members of the family, including vulnerable users like children. Although there are protections for devices marketed and designed for children, consumers need to be empowered to choose products that are safe for all members of their family or household. Internet connected devices should meet standard safety and security measures in order to allow the consumer to choose products based on price, features, and other attributes without any additional knowledge regarding device cybersecurity.

Automated Decisionmaking

Algorithmic decision tools and predictive analytics are being used to make decisions about consumers without sufficient transparency, testing, or accountability. While there is great potential in these emerging technologies, consumers need greater protections for the use of these tools. Therefore, we urge a federal entity like the Federal Trade Commission or NIST to give guidance directing companies and organizations that use algorithms to do regular assessments of the accuracy of the algorithmic decisions, and to inspect the source code in order to root out any inherent or sample-bias that has been embedded in the algorithm.

In order for consumers to be sufficiently protected, a federal authority, like the Federal Trade Commission, should have the ability and capacity to assess algorithms that process personal information. The agency should have the authority to create rules requiring audits of algorithms and mandating in some cases some right of redress and human intervention. In the meantime, NIST should craft guidelines for the use of algorithms to help determine whether a particular algorithm

produces decisions that are fair, accurate and representative. To that end, any guidance, at a minimum, should include the following principles:

- **The use of algorithms should be transparent to the end users.** When algorithms make decisions about consumers the individual should have notice that an algorithm was used. In many cases, such as in the sorting of posts in a social media feed or in the prioritization of search results, this will be obvious and no dedicated notice will be necessary; but in some non-intuitive settings, companies should let consumers know when some decision-making relies on algorithmic evaluation.
- **Algorithmic decision-making should be testable for errors and bias, while still preserving intellectual property rights.** Algorithms should be able to be tested by outside researchers and investigators.[29] Opaque algorithms that have the ability to affect a large number of people in life-changing ways should be subject to higher scrutiny.[30] Using this assessment, algorithms used in life-altering situations, such as the employment process and in the creation of FICO and similar scores,[31] warrant greater scrutiny.

Currently, the U.S. lags behind on algorithmic transparency compared to our European counterparts:[32] The European Union incorporated algorithmic transparency and accountability into their new data privacy law: any decision based "solely on automated processing" which includes "legal effects" or "similarly significantly affects" an individual, be subject to "suitable safeguards," including an opportunity to obtain an explanation of an algorithmic decision, and to challenge such decisions."[33] France's president, Emmanuel Macron, pledged that the country will make all algorithms used by its governments open to the public.[34] And in June, the United Kingdom called for public sector entities to be transparent and accountable about their data practices and to "carefully

---

[29] *See*, *e.g.*, Lauren Kirchner, *Federal Judge Unseals New York Crime Lab's Software for Analyzing DNA Evidence*, PROPUBLICA (Oct. 20, 2017), https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence.

[30] CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016).

[31] Algorithms are used in state and local agencies across the country, including Arkansas: "Algorithmic tools like the one Arkansas instituted in 2016 are everywhere from health care to law enforcement, altering the ways people affected can usually only glimpse, if they know they're being used at all. Even if the details of the algorithms are accessible, which isn't always the case, they're often beyond the understanding of the people using them, raising questions about what transparency means in an automated age, and concerns about people's ability to contest decisions made by machines." Colin Lecher, *What Happens When an Algorithm Cuts Your Health Care*, THE VERGE (Mar. 21, 2018), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy. The article describes similar algorithmic tools used in other states, including California, Colorado, and Idaho.

[32] Julia Angwin, *Making Algorithms Accountable*, PROPUBLICA (Aug. 1, 2016), https://www.propublica.org/article/making-algorithms-accountable.

[33] Art. 22, GENERAL DATA PRIVACY REGULATION, https://gdpr-info.eu/art-22-gdpr/.

[34] Nicholas Thompson, *Emmanuel Macron Talks to Wired about France's AI Strategy*, WIRED (Mar. 31, 2018), https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/.

consider the social implications of the data and algorithms used."[35]

- **Algorithms should be designed with fairness and accuracy in mind.** Companies should not simply rely on outsiders to detect problems with their algorithms; instead, companies should be required to plan for and design to avoid adverse consequences at all stages of the development of algorithms. Algorithms based on current data sets should be examined closely at the design stage in order to weed out historic discriminatory attitudes.[36] Algorithms can "inherit the prejudices of prior decision makers…in other cases, data may simply reflect the biases that persist in society at large."[37] To correct for sample size disparity that would disproportionately favor the creators or the majority of the data-set population, the data sets used in the algorithmic tool should be thoroughly assessed to root out any unintended bias towards any group.[38] Since algorithms and all data-driven products "will always reflect the design choices of the humans who built them,"[39] companies should commit to the further diversification of their employees.[40]
- **The data set used for algorithmic decision-making should avoid the use of proxies.** Algorithms can only serve to address the question posed to it. When possible, algorithms should avoid the use of unnecessary proxies like zip codes or credit scores that may be used to make discriminatory decisions against individuals. This problem persists even when the creators are trying to correct for unexpectedly biased results: "Even in situations where data miners are extremely careful, they can still [e]ffect discriminatory results with models

---

[35] *Data Ethics Framework*, UK DEP'T FOR DIGITAL, CULTURE, MEDIA & SPORT (June 13, 2018), https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework.

[36] The use of algorithms in the criminal justice sector sufficiently demonstrates the perils of using existing data sets to evaluate problems in a new way. "Our analysis of Northpointe's tool, called COMPAS [...] found that black defendants were far more likely than white defendants to be incorrectly judged to be at a higher rate of recidivism, while white defendants were more likely than black defendants to be incorrectly flagged as low risk[…]even when controlling for prior crimes." Jeff Larson, *et al.*, *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. The risk assessment used by Northpointe was based on data that included items that can be correlated with race, such as poverty, joblessness, and social marginalization. Judges have used these scores in their sentencing decisions, despite the exacerbation of bias that the algorithm created. This algorithm, that was used to decide many individuals' fates, was not rigorously tested before use: "As often happens with risk assessment tools, many jurisdictions have adopted Northpointe's software before rigorously testing whether it works." Julia Angwin & Jeff Larson, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[37] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact,* 104 CALIF. LAW REV. 671 (2016), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899

[38] Organizations can available tools to test whether algorithms already in use and algorithms in the design stage have a discriminatory effect. Researchers are actively developing tools they hope companies and government agencies could use to test whether their algorithms yield discriminatory results and to fix them when necessary. *See*, *e.g.*, *Utah Computer Scientists Discover How to Find Bias in Algorithms*, UNIV. OF UTAH (Aug. 14, 2015), https://unews.utah.edu/programming-and-prejudice/. Cathy O'Neil also created a company that audits algorithms to see how biased they are. *See* O'NEIL RISK CONSULTING & ALGORITHMIC AUDITING, http://www.oneilrisk.com/ (last visited Aug. 17, 2018).

[39] Nanette Byrnes, *Why We Should Expect Algorithms to be Biased*, MIT TECH. REV. (June 24, 2016), https://www.technologyreview.com/s/601775/why-we-should-expect-algorithms-to-be-biased/.

[40] *See*, *e.g.*, Nitasha Tiku, *Google's Diversity Stats are Still Very Dismal*, WIRED (June 14, 2018), https://www.wired.com/story/googles-employee-diversity-numbers-havent-really-improved/.

that, quite unintentionally, pick out proxy variables for protected classes."[41] For instance, a joint collaboration between Consumer Reports and ProPublica demonstrated that car insurance companies were using an individual's zip code as a proxy for race and class in order to discriminatorily charge customers in minority-majority neighborhoods a higher price for car insurance.[42]

- **Algorithmic decision-making processes that could have significant consumer consequences should be explainable.** In some cases, algorithms are programmed to learn or evolve over time, such that a developer might not know why certain inputs lead to certain results. This could lead to unfair results if there is no meaningful accountability for how decisions are made. If an algorithm is (1) used for a significant purpose, like the determination of a credit score[43] and (2) cannot be sufficiently explained, then the process should not be used.

Thank you for the opportunity to comment on the NIST's developing privacy framework. If you have any questions, please feel free to contact us at 202.462.6262.

Katie McInnis
Policy Counsel
Consumer Reports
1101 17th Street NW, Suite 500
Washington, DC 20036

[41] *Big Data's Disparate Impact*, *supra* note 37; Karen Levy & danah boyd, *Networked Rights and Networked Harms*, paper presented at the INT'L COMMC'N ASSOC.'S DATA & DISCRIMINATION PRECONFERENCE (May 14, 2014), http://www.datasociety.net/initiatives/privacyand-harm-in-a-networked-society/.

[42] *Auto Insurers Charging Higher Rates in Some Minority Neighborhoods*, CONSUMER REPORTS (Apr. 4, 2017), https://www.consumerreports.org/media-room/pressreleases/2017/04/propublica_and_consumer_reports_auto_insurers_charging_higher_rates_in_some_minority_neighborhoods11/.

[43] BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION?, FED. TRADE COMM'N (Jan. 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf. For this reason, the Fair Credit Reporting Act requires explainability today for credit determinations. However, other important determinations not covered by FCRA may be completely unregulated.