Comments from the Future of Privacy Forum to the Federal Trade Commission

Commercial Surveillance ANPR, R111004

November 2022

FUTURE OF PRIVACY FORUM

Table of Contents

EXECUTIVE SUMMARY

The Future of Privacy Forum welcomes this opportunity to comment on the Federal Trade Commission's Advance Notice of Proposed Rulemaking.

The Commission has spent decades enforcing prohibitions against unfair and deceptive data practices regarding a wide range of established and emerging technologies. Those privacy and security enforcement actions have been based on the FTC's statutory authority, which provides flexibility to address consumer harms arising from novel technologies and business practices, but which does not articulate granular rights for consumers or requirements for businesses. Clear, practical rules can more specifically define what data practices the Commission considers unfair or deceptive. This rulemaking process is an opportunity for the FTC to provide individuals with strong, enforceable rights and companies with greater clarity about their obligations under Section 5 of the FTC Act.

FPF urges the Commission to:

- Codify its "common law" privacy and security norms. FTC enforcement actions are often viewed by practitioners as precedent or guidance. But settlements and consent decrees do not provide explicit, comprehensive rules that companies must follow and upon which consumers can rely. The Commission should codify key aspects of its deception and unfairness settlements, while also incorporating lessons from FTC staff reports, workshops, privacy laws, self-regulatory regimes, and commercial best practices. Specifically, the FTC should:
    - require businesses to provide material, clear, and prominently accessible data use policies;
    - require businesses to implement reasonable security measures;
    - require businesses to comply with the representations they make about privacy and security, including self-regulatory commitments;
    - prohibit companies from circumventing individuals' clearly expressed privacy preferences without clear, explicit, superseding consent from the individual; and
    - articulate the circumstances in which the FTC considers discriminatory algorithmic decision-making to be an unfair trade practice, the factors the Commission considers when weighing that determination, and the degree to which the Commission's analysis relates to other anti-discrimination regimes.

EXECUTIVE SUMMARY (CON'T)

- Go beyond its common law privacy and security norms to mitigate important privacy risks and establish increased clarity regarding companies' responsibilities. When crafting these sorts of rules, the FTC should be guided by three principles:
    - data exists on a spectrum of identifiability, rather than in binary categories of "personal information" or "not personal information," and privacy enhancing technologies can reduce the identifiability of data and otherwise mitigate risks;
    - standards for evaluating the fairness of "secondary uses" of data are needed to define the boundaries of what secondary uses are compatible, based on a careful evaluation of context, expectations, harms, and benefits of processing, including competition;
    - It is especially important to consider the harms that sensitive data use can create, the manner in which those harms impact marginalized communities, and the heightened protections that may be appropriate to mitigate those harms. At the same time, sensitive data is essential to a wide range of activities, including detecting and addressing disparate outcomes.

As a practical matter, the FTC acts as the primary U.S. privacy enforcement agency. Although FPF views a new, pragmatic, comprehensive federal privacy law as the ideal mechanism for grappling with complex technologies and data flows, clear and practical FTC rules defining unfair and deceptive practices would benefit individuals and businesses.

II. The Commission's Authority

The Federal Trade Commission's efforts to address unlawful use of consumers' personal data arises from well-documented concerns regarding individuals', communities', and organizations' increased dependence on technology and data.[1] By focusing on practices that fall squarely within the scope of its Section 5 authority, Commission rules that address specific harmful data privacy and security practices would benefit consumers and provide companies with greater clarity about their obligations.[2] The Commission can address many data-driven harms through Magnuson-Moss rulemaking, though its authority is not unlimited.[3]

The Commission's Section 5 authority has proven to be a valuable tool to address certain harmful privacy and security practices. A trade regulation rule provides an opportunity for the Commission to clarify key aspects of its work to combat unfair and deceptive practices and focus on regulating the most harmful commercial practices.

A. Deception

The Commission's deception authority under Section 5 requires businesses to keep their promises to consumers and has been the core of the Commission's privacy enforcement. The FTC's 1983 Deception Policy Statement sets forth three key elements of a deception case: there must be (1) a representation, omission, or practice that is likely to mislead a consumer; (2) the interpretation of that act or practice is considered from the perspective of a reasonable consumer; and (3) the representation must be material.[4]

"A misrepresentation is an express or implied statement contrary to fact. A misleading omission occurs when qualifying information necessary to prevent a practice, claim representation, or

---

[1] *See generally*, "Big Data: A Tool for Inclusion or Exclusion?," FTC (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; Oscar Gandy Jr., "The Panoptic Sort: A Political Economy of Personal Information," (Westview Press 1993).

[2] An overly broad rulemaking could be comparable to the Commission's 1978 trade regulation rule banning all advertising directed at children, which spurred Congress to limit the Commission's powers under the 1980 Federal Trade Commission Improvements Act. Pub. L. 96-252, 94 Stat. 374 (1980).

[3] Rebecca Kelly Slaughter, "Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission," Yale Tech. L. J. (Aug. 2021) at 51-54, https://law.yale.edu/sites/default/files/area/center/isp/documents/algorithms_and_economic_justice_master_final.pdf (noting that, "rulemaking cannot target conduct that does not otherwise violate the law; in other words, the FTC cannot prescribe through rule conduct what it could not pursue through ex-post enforcement under the FTC Act." Failure to maintain affirmative consumer rights like data deletion have not been enforced by the Commission as unfair or deceptive trade practices.).

[4] Letter from James C. Miller III, Chairman to John D. Dingell, Chairman, House Comm. on Energy and Commerce, at 5-6 (Oct. 14, 1984). The Policy Statement is appended to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

reasonable expectation or belief from being misleading is not disclosed."[5] It is immaterial whether the author's intent is to deceive, but rather the likelihood of the content to mislead.[6] A vast majority of the Commission's data protection enforcement actions have dealt with broken promises of privacy and security, including promises regarding anonymous collection of data, the sale of data, and data security.[7]

As discussed below, FPF recommends that the FTC codify key aspects of its deception settlements, while also incorporating lessons from FTC staff reports, workshops, privacy laws, self-regulatory regimes, and commercial best practices. The FTC should:

- require businesses to provide material, clear, and prominently accessible data use policies;
- require businesses to comply with the representations they make about privacy and security in their privacy policies, including self-regulatory commitments; and
- prohibit companies from circumventing individuals' clearly expressed privacy preferences without clear, explicit, superseding consent from the individual.

B. Unfairness

When Congress enacted the FTC Act, it recognized the "impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[8] Although the "administrative and judicial evolution of the consumer unfairness concept has still left some necessary flexibility in the statute," it is possible to generate a reasonable working sense of the conduct that is covered relating to consumer privacy and data security.[9]

In *FTC v. Sperry & Hutchinson Trading Stamp Co*., the Supreme Court recognized the Commission's unfairness authority as an independent legal theory.[10] For an act or practice to be unfair, it must: (1) cause or be likely to cause substantial injury; (2) that injury cannot be outweighed by countervailing benefits to competition or consumers produced by the practice;

---

[5] *Id.*
[6] Chris Jay Hoofnagle, "Federal Trade Commission: Privacy Law and Policy," Cambridge University Press at 125, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2728003.
[7] *Id*. at 157; *See, e.g., FTC v. Chegg, Inc.,* No. 202-3151 (Oct. 31, 2022); *FTC v. Kochava, Inc,* No. 2:22-cv-377 (Aug. 29, 2022); *In the Matter of FTC v. CafePress*, No. C-4768 & C-4769 (June 24, 2022).
[8] "FTC Policy Statement on Unfairness," FTC (Dec. 17, 1980) https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness; *See also*, Hoofnagle, "Federal Trade Commission: Privacy Law and Policy," at 120 (noting that, "[s]ection 5 does not have a static meaning, and lawyers will always have to grapple with its application in new business contexts…it is a recognition of an ever-evolving commercial dexterity and the personal impact of economic power as important dimensions of trade"); *FTC v. Pfizer*, 81 F.T.C. 23, 61 (1972) (citation omitted) ("unfairness is potentially a dynamic analytical tool capable of a progressive, evolving application which can keep pace with a rapidly changing economy.").
[9] "FTC Policy Statement on Unfairness," FTC (Dec. 17, 1980).
[10] *FTC v. Sperry & Hutchinson Trading Stamp Co*., 405 US 233 (1972).

and (3) cannot be reasonably avoided.[11] The Commission may consider public policies in their analysis, including policies embodied in self-regulatory systems and other statutes, but it cannot use public policy as an independent basis for finding unfairness.[12] For example, the Commission has relied on the Telecommunications Act of 1996, which categorizes customers' phone records as confidential, to determine that collection and sale of customer phone records without consumer knowledge or consent constituted an unfair practice that was likely to cause substantial injuries to those consumers.[13]

To qualify as a "substantial injury," the practice may either cause substantial harm to a small number of people or relatively small harm to many people, and be unavoidable by the reasonable consumer.[14] "[H]istorically, the Commission has focused on practices that result in economic harms suffered by consumers, including harms that impede "a consumer's ability to make an economically rational product decision."[15] Though "emotional impact and other more subjective types of harm…will not ordinarily make a practice unfair,"[16] unwarranted health and safety risks and certain emotional effects that result in tangible injury may also support a finding of unfairness.[17] In reviewing informational injuries from harmful data privacy and security practices, the Commission has explored reputational harm that can arise, for example, from medical identity theft that exposes records of drug abuse.[18]

The independent nature of the consumer injury criterion does not mean that every substantial and unavoidable consumer injury is legally "unfair;" the injury also must not be outweighed by offsetting consumer or competitive benefits:[19]

---

[11] Hoofnagle, "Federal Trade Commission: Privacy Law and Policy," at 132.
[12] The Commission's original 1980 Unfairness Statement ("Unfairness Statement") was codified by Congress in 1994, but limited the public policy factor so that it could not independently support a claim of unfairness–meaning that the focal factor in unfairness was unjustified consumer injury. The Commission also "regularly borrows norms developed from the self-regulatory systems of industries and incorporates standards from statutory information privacy law to set standards under the FTC Act." Hoofnagle, "Federal Trade Commission: Privacy Law and Policy," at 146; *See also*, J. Howard Beales, "The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection," FTC (May 30, 2003), https://www.ftc.gov/news-events/news/speeches/ftcs-use-unfairness-authority-its-rise-fall-resurrection.
[13] *US v. Accusearch*, "Complaint for Injunctive and Other Equitable Relief," (2006), https://www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf.
[14] "FTC Policy Statement on Unfairness," FTC (Dec. 17, 1980) (noting that, "[t]he Commission is not concerned with trivial or merely speculative harms."); Cobun Keegan & Calli Schroeder, "Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms," Journal of Law, Economics and Policy, Vol. 15, No. 1, 2018 (Sept. 14, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4204208 (observing that, [h]istorically, the Commission has focused on practices that result in economic harms suffered by consumers, including harms that impede "a consumer's ability to make an economically rational product decision.") (citing to *Pfizer, Inc.*, 81 F.T.C. 23, 60-62 (1972)).
[15] *Id.*
[16] "FTC Policy Statement on Unfairness," FTC (Dec. 17, 1980).
[17] *Id.*; Keegan & Schroeder, "Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms."
[18] Informational Injury Workshop, FTC (Dec. 12, 2017), https://www.ftc.gov/news-events/events/2017/12/informational-injury-workshop.
[19] "FTC Policy Statement on Unfairness," FTC (Dec. 17, 1980).

> *A seller's failure to present complex technical data on his product may lessen a consumer's ability to choose, for example, but may also reduce the initial price he must pay for the article. The Commission is aware of these tradeoffs and will not find that a practice unfairly injures consumers unless it is injurious in its net effects. The Commission also takes account of the various costs that a remedy would entail. These include not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters.*[20]

It is imperative that consumer harms are balanced against the context of beneficial data processing and technology, such as offering valuable services and products, research in the public interest, fraud prevention, and data security.

Some experts argue that the Commission's unfairness authority has been used intermittently,[21] but can be better utilized to address the substantive merits of many harmful data privacy and security practices.[22] In 1975, then-Chairman Pitofky highlighted how "the misuse of certain types of private financial information can be 'legally unfair.'"[23] Since then, most privacy unfairness cases have involved consumer data that was sold for value or sensitive data that was transferred to third parties,[24] such as sensitive geolocation data[25] and confidential phone records.[26] In these cases, the Commission found that the activity led to economic harm, such as needing to change phone carriers,[27] or may have led to unwarranted health and safety risks, such as the risk of stalkers and abusers[28] or targeting those seeking reproductive health care.[29]

---

[20] *Id*.
[21] *See* J. Howard Beales, "The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection," FTC (May 30, 2003), https://www.ftc.gov/news-events/news/speeches/ftcs-use-unfairness-authority-its-rise-fall-resurrection#N_72 (providing a historical overview of the Commission's use of its unfairness authority).
[22] Some argue that the Commission's neglect of their unfairness enforcement authority for privacy harms reduces certainty and avoids the unique value in the cost-benefit analysis required for unfairness. *See, e.g.*, Keegan & Schroeder, "Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms," at 1.
[23] Statement of Chairman Pitofsky and Commissioners Anthony and Thompson, *In the Matter of Touch Tone Information, Inc.*, File No. 982-3619 (1999), https://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-majoritystatement.htm.
[24] *See ex., FTC v. Sequoia One LLC*, No. 2:15-cv-01512 (D.Nev.. Aug. 7, 2015), *Cornerstone and Co. v. FTC*, No. 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *FTC v. Bayview Solutions LLC*, No. 1:14-cv-01830 (D.D.C. Oct. 31, 2014) ;
See also Keegan & Schroeder, "Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms," at 14 ("Though the direct financial harm may not be calculable, the proxy of financial injury appears to be assumed based on (1) the sensitivity of the data; (2) the lack of direct relationship with consumers; and (3) consumers lack of knowledge of and agency over the sharing.").
[25] *FTC v. Kochava, Inc.*, No. 2:22-cv-377 (D. ID. Aug. 29, 2022).
[26] *U.S. v. Accusearch*, 570 F.3d 1187 (10 Cir. 2009).
[27] *Id.*
[28] *Id.*; *FTC v. Kochava, Inc.*, No. 2:22-cv-377 (D. ID. Aug. 29, 2022).
[29] *Id.*

As discussed below, FPF recommends that the FTC codify key aspects of its unfairness settlements, while also incorporating lessons from FTC staff reports, workshops, privacy laws, self-regulatory regimes, and commercial best practices. The FTC should:

- require businesses to provide material, clear, and prominently accessible data use policies;
- require businesses to implement reasonable security measures;
- articulate the circumstances in which the FTC considers algorithmic decision-making to be an unfair trade practice, the factors that the Commission considers when weighing that determination, and the degree to which the Commission's analysis relates to other anti-discrimination regimes.

III. Specific Recommendations

A. The FTC should codify long standing privacy and security norms derived from the Commission's enforcement actions and consent decrees

The FTC should codify its established privacy and security norms. FTC enforcement actions are often viewed by practitioners as precedent or guidance. But settlements and consent decrees do not provide explicit, comprehensive rules that companies must follow and upon which consumers can rely. The Commission should codify key, recurring aspects of its deception and unfairness settlements, while also incorporating lessons from FTC staff reports, workshops, privacy laws, self-regulatory regimes, and commercial best practices. Specifically, the FTC should:

- (1) require businesses to provide material, clear, and prominently accessible data use policies;[30]
- (2) require businesses to implement reasonable security measures;[31]

[30] *See, e.g., In re Lenovo, Inc.*, No. C-4636 (Sept. 13, 2017) (complaint) (charging laptop computer manufacturer with deceptive failure to disclose material facts related to pre-installed man-in-the-middle software which tracked users' web activities and created security vulnerabilities on users' laptops); *In re Practice Fusion, Inc.*, No. C-4591 (Aug. 16, 2016) (complaint) (charging Respondent with deceptive failure to disclose material fact that consumers' satisfaction survey responses would be published on its website); *See also* California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et. seq. (requiring certain businesses to maintain privacy policies); Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1301 et seq. (requiring covered entities to maintain privacy policies); Virginia Consumer Data Protection Act (VCDPA) Va. Code §59.1-571 (requiring certain businesses to maintain privacy policies).

[31] Data breaches can occur as a result of an organization's failure to implement low-cost and readily available security measures against well-known and reasonably foreseeable vulnerabilities. *See, e.g.*, *In re CafePress*, Nos. C-4768 & C-4769 (Jun. 24, 2022) (complaint) (charging an ecommerce website owner with unfair data security practices for failing to employ reasonable security measures to protect personal information from unauthorized access); *In re LightYear Dealer Tech., LLC*, No. C-4687 (Sept. 6, 2016) (complaint); *In re BJ's Wholesale Club, Inc.*, No. C-4148 (Sept. 23, 2005) (complaint).

- (3) require businesses to comply with the representations they make about privacy and security, including self-regulatory commitments;[32]
- (4) prohibit companies from circumventing individuals' clearly expressed privacy preferences without clear, explicit, superseding consent from the individual;

The Commission has spent decades enforcing the FTC Act's prohibition against unfair and deceptive data protection practices regarding a wide range of established and emerging technologies. As a practical matter, the FTC acts as the primary U.S. privacy enforcement agency.[33] Through enforcement efforts, including consent decrees, as well as staff reports[34] and public workshops,[35] the Commission has developed a thorough record of findings, recommendations, and guidance that shape modern best practices for privacy and data security.

Today, many businesses, consumers, advocates, and academics interpret the Commission's enforcement actions as a form of common law for U.S. data protection.[36] They monitor FTC actions, analyze consent decrees and settlements, and extrapolate from reasoning of settlements and Commissioners' statements, attempting to determine how the FTC would apply its authority to novel circumstances as a measure to proactively shape business policy and practice.[37] Despite this, many critique the Commission's reliance on enforcement actions as inherently retroactive and fact-specific, leaving consumers and companies without clear rules.[38]

Though many data protection best practices are implemented by businesses in the U.S. today, the adoption of these practices is not universal, and analysis of existing FTC settlements can yield

---

[32] *See In re Flo Health,* No. C-4747 (Jun. 21, 2021) (complaint); *In re Everalbum,* No. C-4743 (May 7, 2021) (complaint).
[33] *See generally* Daniel J. Solove & Woodrow Hartzog, "The FTC and the New Common Law of Privacy," 114 Colum. L. Rev. 583 (2014), https://columbialawreview.org/wp-content/uploads/2016/04/Solove-Hartzog.pdf. Technically, settlement agreements legally function as contracts.
[34] *See, e.g.*, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," FTC (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[35] *See, e.g.* "Informational Injury Workshop," FTC (Dec. 12, 2017), https://www.ftc.gov/news-events/events/2017/12/informational-injury-workshop.
[36] *See generally* Daniel J. Solove & Woodrow Hartzog, "The FTC and the New Common Law of Privacy," 114 Colum. L. Rev. 583 (2014), https://columbialawreview.org/wp-content/uploads/2016/04/Solove-Hartzog.pdf.
[37] *See, e.g.* Letter from Donald S. Clark, Sec'y FTC, to Alan Charles Raul, Sidley Austin, LLP (Aug. 31, 2009) ("They seem to analyze literally every word of the complaint and order in search of hidden messages; in particular many of the law firms with FTC practices put out client alerts whenever the FTC issues a settlements that includes highly detailed analyses of the pleadings and predictions on what they might portend for the future"); *See generally* Solove & Hartzog, "The FTC and the New Common Law of Privacy."
[38] *Id.*; Michael D. Scott, "The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?," 60 Admin. L. Rev. 127, 183 (2008) http://www.administrativelawreview.org/wp-content/uploads/2014/04/The-FTC-The-Unfairness-Doctrine-and-Data-Security-Breach-Litigation-Has-the-Commission-Gone-Too-Far_.pdf (noting that, "[t]he complaints and consent orders entered into in these cases provide limited guidance as to what a company should do or not do to avoid being the target of an unfairness action by the FTC").

numerous, sometimes conflicting interpretations. A lack of clear, universal rules can disadvantage businesses that protect privacy at the expense of growth or other commercial gains. Tracking, analyzing, and adapting to FTC enforcement actions is a resource-intensive process; many companies are unable or unwilling to fully invest, and even those who do are not guaranteed to have responded adequately to stave off future action.

Trade regulation rules by the Commission would create common requirements and demand attention from all organizations. Clear rules would also resolve inconsistent interpretations of Section 5's prohibitions against unfair and deceptive trade practices. Rulemaking can provide a solid basis for future workshops and guidance that articulate the FTC's views regarding the application of those rules to emerging technologies and business practices.[39] In addition, the Commission has an opportunity to do more than codify the status quo; the FTC should aim to ensure that organizational policies and practices–including those related to transparency, security, and compliance–are implemented strategically (rather than as "check-box" exercises) and provide common expectations for consumers.

1. Require businesses to provide material, clear, and prominently accessible data use policies.

The Future of Privacy Forum recommends that the Commission clarify and elaborate on its prior actions regarding data use policies by creating a rule that explicitly requires organizations to create and maintain a clear and prominently accessible data use policy, and specify what information should be contained therein.

Data use transparency has near-universal support among all stakeholder groups–including consumers, industry, advocates, and academics–as a baseline protection for consumers.[40] Such a requirement also aligns with the first 1973 Fair Information Practice: "there shall be no database

[39] "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," FTC, at v (March 2012) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. While the Commission has done much to address certain cases of misconduct, as noted by the Commission in their 2012 staff report on consumer privacy, the "industry as a whole must do better." *Id*.

[40] *See, e.g.,* Solove & Hartzog, "The FTC and the New Common Law of Privacy," at 672.

whose existence is a secret."[41] Though insufficient by itself to fully protect consumers, transparency into data collection, use, and transfer is a necessary starting point and a foundational principle of privacy regulation that supports all other rights and obligations, such as the ability of consumers to request certain data be deleted or opt to use more privacy-protective platforms,[42] and the obligation of the business to know the personal data they collect and why. Even when average consumers do not read data use policies, other important stakeholders will – including journalists, researchers, advocates, competing businesses, and regulators.[43] Further, as the privacy management industry continues to develop,[44] machine-readable data use policies will be necessary for the functioning of much emerging compliance technology.

To the extent that a data use policy implicates information that "is likely to affect the consumer's conduct or decision with regard to a product or service," the total absence of a data use policy is likely deceptive under the FTC Act.[45] Within a data use policy, the Commission has often found deception in the failure to include specific information clearly and comprehensively, including information related to the scope of data collection or dissemination, when such omissions were

---

[41] *See, e.g.,* Timothy Morey, Theodore Forbath, and Allison Schoop, "Customer Data: Designing for Transparency and Trust," Harvard Business Review (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (making the business case for why businesses should build and retain consumer trust and goodwill by being transparent about data collection and use practices); Gabrielle Rodgers, "Consumer Wants: Privacy Transparency, Online Security, Better Customer Experience," CMSWire (May 12, 2022), https://www.cmswire.com/customer-experience/consumer-wants-privacy-transparency-online-security-better-customer-experience/ (noting that most consumers want businesses to be transparent about how they collect and use personal data."); Richard Beaumont, "Transparency Should Be the New Privacy," International Association of Privacy Professionals (May 14, 2014) https://iapp.org/news/a/transparency-should-be-the-new-privacy/ (arguing that that, "[t]ransparency statements could be the vehicle to enable the majority of people to make better-informed choices than they currently do and use a truly market-driven approach to online privacy practice."); Nicolette Edwards, "Transparency Can Make Or Break 'big Data' Regulation," University of Colorado - Boulder (Aug. 12, 2021), https://www.colorado.edu/asmagazine/2021/08/12/transparency-can-make-or-break-big-data-regulation (offering an academic perspective on the importance of transparency around data collection and use).

[42] *See, e.g.*, Thomas C. Redman and Robert M. Waitman, "Do You Care About Privacy as Much as Your Customers Do?," Harvard Business Review (Jan. 28, 2020), https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do (discussing a 2019 survey finding that among over 2,500 respondents, 32% have switched companies or providers over data or data-sharing policies).

[43] Daniel Solove & Paul Schwartz, "Information Privacy Law," Wolters Kluwer (7th ed. 2021), at 875.

[44] *See, e.g.,* Andy Greenberg "An AI That Reads Privacy Policies So You Don't Have To," Wired (Feb. 9, 2018), https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/; Sebastian Zimmeck, "Data Rights Protocol and Global Privacy Control," Consumer Reports (Jan. 13, 2022), https://digital-lab.consumerreports.org/2022/01/13/data-rights-protocol-and-global-privacy-control/.

[45] "Concurring Statement of Commissioner J. Thomas Rosch Issuance of Preliminary FTC Staff Report Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers," FTC (Dec. 1, 2010), https://www.ftc.gov/sites/default/files/documents/public_statements/concurring-statement-commissioner-j.thomas-rosch-issuance-preliminary-ftc-staff-report/101201privacyreport.pdf.

material to consumers in deciding whether or how to use the product or respond to the survey.[46] The FTC has also issued findings of unfairness in regard to data use policies when such policies were overly vague, inaccurate, or had inadequate detail to provide notice of the organization's handling of user data.[47]

Potential Harms from a Lack of Transparency

Because statements regarding a business' personal data use are often material to consumers, the Commission needs to ensure that, at a minimum, all businesses are transparent with consumers about how their personal information (and any sensitive inferences) is collected, used, and shared through a data use policy. Despite their relative ubiquity, there is no comprehensive federal requirement that businesses disclose their data collection practices. Instead, data use policies, or privacy policies as they are often called,[48] have developed over time as a result of self-regulatory codes developed by industry and other stakeholders as well as a network of state-specific rules.[49] In some cases, not all data collecting entities and businesses disclose their data collection practices. For example, in 2019, researchers at Carnegie Mellon determined that

[46] In *in re Lenovo, Inc.*, the FTC charged device manufacturer Lenovo with deceptive failure to disclose to users the presence of pre-installed man-in-the-middle tracking software on laptops, which allowed the software provider to see all of users' sensitive personal information that was transmitted on the internet. *In re Lenovo, Inc.*, No. C-4636 (Sept. 3, 2017) (complaint). *See also In re Practice Fusion, Inc.*, the Commission charged a health technology company with deceptive failure to disclose that a healthcare provider survey given to patients would be publicly shared. *In re Practice Fusion, Inc.*, No. C-4591 (Aug. 6, 2016) (complaint).

[47] *See*, *Beneficial Corp.,* 86 F.T.C. 119 (1975), *aff'd in part, remanded on other grounds*, *Beneficial Corp. v. FTC*, 542 F.2d 611 (3d Cir. 1976) (finding that a company's failure to disclose that the company would use financial information it collected from customers for tax purposes to offer customer loans without consent constituted an unfair practice); *see also FTC v. Echometrix*, No. CV10-5516 (Nov. 30, 2010) (complaint) (determining that Echometrix's broad statement that the company used information for a wide-ranging list of general purposes was too vague to adequately disclose the material fact that information monitored and collected would be shared with third parties); *In re Sony*, No. C-4195 (Jun. 29, 2007) (complaint) (regarding a business' failure to disclose in their end user agreement or elsewhere that media software was tracking information from users' computers and transmitting to the business without consumers' notice or consent); *In the matter of Nomi Technologies, Inc.*, No. C-4538 (Sept. 3, 2015) (complaint) (regarding omitted material facts from a privacy policy that contravened consumer expectations by tracking shopping behavior without notice or consent); *FTC v. Rennert, Sandra L., et al.* No. CV-S-00-0861-JBR (Jul. 12, 2000) (complaint) (regarding inaccurate statements made about how data is shared and the security of such data).

[48] According to one survey, 75% of people surveyed falsely believed that when "a website has a privacy policy, it means the site will not share my information with other websites and companies." Joseph Turrow et al., "Open to Exploitation: American Shoppers Online and Offline," University of Pennsylvania Annenberg School of Communication (June 2015) at 3, https://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers; Joseph Turrow et al., "Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It," University of Pennsylvania Annenberg School of Communication (Sept. 29, 2009) at 21, https://repository.upenn.edu/cgi/viewcontent.cgi?article=1138&context=asc_papers.

[49] *See, e.g.*, Solove & Hartzog, "The FTC and the New Common Law of Privacy," at 592 (citing Michael D. Scott, "The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?," 60 Admin. L. Rev. 127, 130-31 (2008)); *See also* The California Online Privacy Protection Act of 2003 (CalOPPA), Cal. Civ. Code §§ 22575-22579.

nearly half (49 percent) of over one million Android applications did not idsplay privacy policy links in the app marketplace.[50]

A patchwork of legal obligations in terms of content and format–not only those found in U.S. state and sector-specific laws but also foreign law with extraterritorial applicability like the GDPR–has led to the development of long, inconsistent, and/or overly vague privacy policies that the average consumer typically does not read and often cannot understand.[51] Complicating matters, these policies are nearly always "all or nothing" for consumers, and may fail to provide ample information to serve as the basis for meaningful action or objection.[52]

This lack of understanding can impact consumer actions and choice. For instance, the Commission has found a failure to inform users about the impact of technical updates on data collection can undermine consumer expectations and increase security risks.[53] Moreover, a lack of transparency or personal autonomy over personal data most heavily affects marginalized and multi-marginalized communities, including economically disadvantaged people of all backgrounds who do not have the legal or technical expertise to understand data use policies, and are less likely to have knowledge of or access to privacy protective technologies.[54]

---

[50] Daniel Tkacik, "Apps Are Rife With Privacy Compliance Issues, And Here's Some Evidence," Carnegie Mellon University Security and Privacy Institute (Aug. 19, 2019), https://www.cylab.cmu.edu/news/2019/08/19-apps-privacy-compliance.html.

[51] *See, e.g.* Becky Chao, Eric Null, & Claire Park, "Enforcing a New Privacy Law: Who Should Hold Companies Accountable?," Open America - New Technology Institute at 3, https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/the-ftc-is-currently-the-primary-privacy-enforcer-but-its-authority-is-limited/ (last visited: Nov. 10, 2022).

[52] Daniel Solove, "Privacy Self-Management and the Consent Dilemma," 126 Harvard L. Rev. 1880 (2013), at 1883-88 (describing problems uninformed consumers have reading and comprehending privacy policies); "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," Federal Trade Commission at 2 (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[53] *In Re Zoom,* No. C-4731 (Nov. 9, 2020) (complaint) (alleging that Zoom failed to inform consumers that installing a standard Zoom software update would allow its software to circumvent a Safari browser security safeguard. This circumvention "harmed consumers by limiting the intended benefit of a privacy and security safeguard provided by their Safari browser...[without which] one wrong click could expose consumers to remote video surveillance by strangers through their computers' webcams." By not informing consumers that its software would circumvent a privacy-protective Safari browser update or to provide equivalent protections through an alternative mechanism, the Commission asserted that Zoom unlawfully deprived its users of these protections.).

[54] Spencer Overton, "For Communities of Color, Increased Smartphone Costs Mean Decreased Opportunity," Joint Center for Political and Economic Studies (July 20, 2018), https://jointcenter.org/for-communities-of-color-increased-smartphone-costs-mean-decreased-opportunity/ ("data show[s] that 66 percent of African Americans and 62 percent of Latinos use Android smartphones"); Sara Morrison, "'Privacy shouldn't be a luxury': Advocates want Google to do more to secure cheap Android phones," Vox (Jan. 17, 2020), https://www.vox.com/recode/2020/1/17/21069417/privacy-international-bloatware-android-google (observing that "manufacturers sometimes cut corners to produce a cheaper [Android] phone [...] that means lower-income people, in both the US and the rest of the world, are more exposed to privacy

Individuals that identify as LGBTQ+, in particular, have vested interests in understanding how their data is used and shared. FPF, in partnership with LGBT Tech, recently published a report on how Sexual Orientation and Gender Identity ("SOGI") information, given its revelatory nature, creates heightened risks of misuse or abuse for LGBTQI+ individuals.[55] While SOGI information can be processed to benefit the LGBTQI+ community, recent history and the current privacy law landscape show that the community can be disproportionately harmed by the misuse of this inherently sensitive data by societal institutions such as law enforcement, healthcare organizations, employers, or landlords, and not even be aware of it. Similarly, for individuals with disabilities, health and biometric data related to a disability, and other data that is used to make inferences about disability status,[56] can be shared and used for decisions in housing, employment, and education.[57]

Considerations for a Data Use Policy Rule

The Commission can promote meaningful and standardized transparency, prioritizing disclosure of data practices that could impede "a consumer's ability to make an economically rational product decision", while considering other countervailing values like safety and innovation. The FTC should also include some core requirements–including materiality, clarity, and prominent accessibility:

1. ***Materiality*:** The Commission should require businesses to disclose all material facts about their data use in their data use policies, which the Commission has defined as information that would impact consumer decision making about whether to use a

violations than wealthier people who can afford more expensive — and more secure — phones [...] When dealing with low-cost devices, we see quite a number of poor security practices.").

[55] *See,* Chris Wood, et al, "The Role of Data Protection in Safeguarding Sexual Orientation and Gender Identity Information*,"* FPF & LGBT Tech (June 2022), https://fpf.org/wp-content/uploads/2022/06/FPF-SOGI-Report-R2-singles-1.pdf.

[56] Lydia X.Z. Brown, et al., "Ableism And Disability Discrimination In New Surveillance Technologies: How New Surveillance Technologies In Education, Policing, Health Care, And The Workplace Disproportionately Harm Disabled People," Center for Democracy & Technology (2022), at 44-46 https://cdt.org/insights/ableism-and-disability-discrimination-in-new-surveillance-technologies-how-new-surveillance-technologies-in-education-policing-health-care-and-the-workplace-disproportionately-harm-disabled-people/.

[57] Lauren Smith, et al., "The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions," FPF (2019), at 13, https://fpf.org/wp-content/uploads/2019/01/2019_01_29-The_Internet_of_Things_and_Persons_with_Disabilities_For_Print_FINAL.pdf.

software or service.[58] According to Commission common law, material information about data practices may include:

a. The use of tracking technology that contravenes reasonable consumer expectations;[59]
b. Any collection of personal or sensitive personal information;[60]
c. All uses of personal and sensitive personal information;[61]
d. Whether and how personal information is shared with third parties;[62]
e. Any retroactive changes that govern personal information[63]

2. ***Clarity*:** The FTC should incentivize "privacy by design" principles of visibility and transparency.[64] For example, in 2010, the Future of Privacy Forum conducted an online behavioral advertising icon study, which sought to understand "the communication efficacy of [icon and short disclosure-based] behavioral advertising disclosures…as an alternative to providing transparency and choice via traditional online privacy notices."[65] The study found that respondents who were active online and engaged in more privacy-protective behavior were much more comfortable with online behavioral advertising when they were provided with transparency about how their internet browsing data was being used to conduct targeted advertising, as well the choice to receive general rather than targeted ads.[66]

---

[58] Letter from James C. Miller III to Hon. John D. Dingell, Federal Trade Commission at 176 (Oct. 14, 1983) https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf ("In the words of former FTC Chairman John C. Miller III, "[w]here the seller knows, or should have known, that an ordinary consumer would need omitted information to evaluate the product or service, or that the claim was false, materiality will be presumes because the manufacturer intended the information or omission to have an effect. Similarly, when evidence exists that a seller intended to make an implied claim, the Commission will infer materiality.").
[59] *In re Nomi Technologies, Inc.*, No. C-4538 (Sept. 3, 2015) (complaint).
[60] *In re Sears Holdings Management Corp*., No. C-4264 (Feb. 28, 2018) (complaint) at 6.
[61] *In re Nomi Technologies, Inc.*, No. C-4538 (Sept. 3, 2015) (complaint).
[62] *FTC v Echometrix,* No. CV10-5516 (Nov. 30, 2010) (complaint).
[63] *In re Gateway Learning Corp.*, No. C-4120 (Dec. 28, 2004) (complaint).
[64] *See* Ann Cavoukian, "Privacy by Design: The Seven Foundational Principles," Information and Privacy Commissioner of Ontario (Aug. 2009), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (directing that privacy-by-design should be: "Proactive not Reactive; "Preventative not Remedial;" "Privacy as the Default Setting;" "Privacy Embedded into Design;" "Full Functionality- Positive-Sum, not Zero-Sum," "End-to-End Security- Full Lifecycle Protection;" "Visibility and Transparency- Keep it Open;" "Respect for User Privacy- Keep it User-Centric."); *See also* EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 at Article 25(1) (directing controllers to implement privacy-by-design and by-default safeguards including pseudonymization and data minimization, in Article 25).
[65] Manoj Hastak & Mary J. Cullen, "Online Behavioral Advertising 'Icon' Study," FPF (Jan. 25, 2010) at 4, https://fpf.org/wp-content/uploads/2016/06/Ad_Icon_Study.pdf.
[66] *Id.*

3. ***Prominent Accessibility*:** Data use policies should be easily accessible by all users. At a minimum, the policy is provided in a user's preferred language whenever possible, as well as in machine-readable format.[67] As Commissioner Bedoya has noted, "non-English language communities are disproportionately targeted [for fraud and other abusive data practices] in the offline world," and this case is true online as well.[68] Providing data use policies in a user's own language gives them the tools to understand the policy, and may help to protect non-English speaking communities from fraud and other abusive data practices. Making documents machine-readable and searchable can bolster universal design aimed at cultivating accessibility for all, including persons with disabilities.[69]

4. **Organizational Context**: Balancing conciseness, understandability, and accuracy is not an easy task for businesses. Large corporations with resources have tried many approaches for crafting data use policies, oftentimes with mixed outcomes.[70] As noted in the Commission's 2012 staff report "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," assessing adequate disclosures must account for variations in business models across different industry sectors, and prescribing a rigid format for use across all sectors is not appropriate, particularly for emerging technologies.[71] For instance, Immersive technologies such as virtual reality (VR) and augmented reality (AR), present a unique tension between transparency and technological function.[72] Data use policies for connected car data present unique

[67] Machine-readable text is written in standard computer language that can be read automatically by a web browser, rather than English text.

[68] Alvaro M. Bedoya, "Statement of Commissioner Alvaro M. Bedoya: Regarding the Commercial Surveillance Data Security Advance Notice of Proposed Rulemaking," FTC (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Bedoya%20ANPR%20Statement%2008112022.pdf.

[69] In the context of privacy policies, regulatory bodies have aimed implement machine-readability requirements as far back as 2001, when the Platform for Privacy Preferences (P3P) was introduced as a World Wide Web Consortium (W3C) recommendation, with an aim towards making "privacy policies machine-readable, opening complex privacy policies to automated analysis and matching against user preferences." However, P3P was never mandated or widely adopted, and as such, the most prevalent source of mandated machine readability comes within the government context, by way of Executive Order 13642 and the Open Government Data Act of 2019. These laws mandate government agencies to ensure that all documents they create and publish are machine readable.

[70] *See, e.g.* Geoffrey A. Fowler, "I checked Apple's new privacy 'nutrition labels.' Many were false," The Washington Post (Jan. 29, 2021), https://www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/.

[71] "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," FTC (Mar. 2012), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[72] Immersive technologies refers to the collection of hardware and software that enable enhanced multi-faceted interaction with an environment and potentially those in it, and that substitute, enhance, or alter users' individual, physical-world experiences; Yeji Kim, "Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent," California L. Rev. 110, Vol. 1 (Feb. 2022), at Sec. III-D, https://www.californialawreview.org/print/virtual-reality-data-and-its-privacy-regulatory-challenges-a-call-to-move-beyond-text-based-informed-consent/#clr-toc-heading-10. In order to maintain users' immersion,

challenges because connected car data is vast, implicates those beyond the owner of the vehicle, and are often needed for car function and usability, but utilizing "just in time" notices may present safety risks.[73]

2. Require businesses to implement reasonable security measures, including data minimization

The FTC should codify a requirement for businesses to implement reasonable security measures to safeguard consumers' personal information from unauthorized access, where failure to do so constitutes an unfair trade practice. It is well-documented that security breaches harm businesses and consumers alike and are becoming increasingly costly. The rapid adoption of mobile devices, wearable technology, connected vehicles, and smart homes have increased the amount and

---

virtual reality providers use a vast amount of user data and inferences to make the experience as personalized and natural to users as possible, however, providers face difficulty in displaying notice in a way that does not disturb the user's immersion. In either event there is a decreased likelihood the user will see the notice. Erin Egan, "Charting a Way Forward: Communicating About Privacy: Towards People-Centered and Accountable Design," Facebook (July 2020), at 6, https://about.fb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf. Even if providers can display notice to a user without disturbing their sense of immersion, it is unclear whether these disclosures adequately convey the purposes for which personal data can and will be used. Joseph Jerome & Jeremy Greenberg, "Augmented Reality + Virtual Reality: Privacy & Autonomy Considerations in Emerging, Immersive Digital Worlds," FPF (Apr. 2021), at 25, https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf. This is particularly true for bystanders whose data is inadvertently captured by an immersive technology device–it is unlikely these individuals would be given notice about the data collection. Therefore, immersive technology providers, in seeking to address these shortcomings in providing clear notice and obtaining informed consent, will need to experiment with more interactive, experiential methods of doing so. *Id.*; *see also* As an example, Yale School of Medicine developed the Virtual Multimedia Interactive Informed Consent (VIC) model, which seeks to provide patients a clearer, more interactive way to understand the decisions regarding their clinical care. *See* Geoffrey Lowell Chupp, Sandra Alfana, & Peter Natale Peduzzi, "Virtual Multimedia Interactive Informed Consent (VIC)," Yale School of Medicine, https://medicine.yale.edu/lab/abujarad/projects/vic/ (last visited: Nov. 8, 2022).

[73] A "connected car" is powered by wireless technologies that share data to networks inside and outside of a vehicle to facilitate vehicle safety and performance features and sync occupants' smartphones and applications. *See, e.g.*, "What is the connected car?," Alliance for Automotive Innovation, https://www.autosinnovate.org/initiatives/innovation/connected-vehicles (last visited: Sep. 30, 2022); Gyorgy Halmos & Jayne Golding, "Securing privacy for the future of connected cars," IBM (2019) at 2, https://www.ibm.com/downloads/cas/D8LEB3AQ. Connected cars can generate up to 25 gigabytes of data per hour, and collect data types ranging from driver data (biometric and behavioral) to location data, as well as account data created by the vehicle owners. Otonomo, "A Privacy Playbook for Connected Car Data," FPF (Oct. 2019) at 7, https://fpf.org/blog/a-privacy-playbook-for-connected-car-data/; *See* "Data and the Connected Car," FPF (2017), https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf; *See also* "Personal Data in Your Car," National Auto Dealers Association & FPF (2017) at 3-4, https://fpf.org/wp-content/uploads/2017/01/consumerguide.pdf. According to a 2017 Government Accountability report, "most notices [with connected cars] [could] not describe all of the types and purposes of the connected vehicle data that were being collected" and due to low consumer awareness, the majority of reviewed experts expressed a "lack of sufficiently informed consent." Id. Therefore, connected car manufacturers are exploring various avenues to provide clear notice and obtain informed consent, including through purchase agreements, user manuals, and on screen displays. *Id.*

sensitivity of data collected about consumers, and the risks arising from a data breach or unauthorized disclosure. While there are a myriad of reasons for a company to retain data–such as to provide services, improve products, or comply with legal requirements–the impact of a personal data breach is often significantly worse if a company retains personal data without appropriate controls.

The Commission has previously found specific security failures to constitute unfair trade practices, such as those that fail to provide basic protection for sensitive information,[74] or organizations that have taken inadequate steps to test for, protect against, or respond to known security threats and vulnerabilities.[75] A failure to comply with an organization's own written policies and statements in regard to security has also been a ground for FTC enforcement action.[76]

Potential Harms from Lax Data Security

A global study of 550 organizations impacted by data breaches between March 2021 and March 2022 found that data breaches in the U.S. were the costliest in the world for the twelfth year in a row, with the average total cost of a data breach being $9.44M, a 4.3 percent increase from the previous year.[77] Consumers often pay for these losses in the form of higher prices, according to 60 percent of the global survey respondents.[78]

For consumers, data breaches can result in harms stemming from identity theft, eroded trust in companies and data controllers, mental and emotional stress and trauma, reputational injury, and unexpected costs as a result of fraudulent transactions.[79] While data breach notification rules, present in all 50 States, have helped in providing some accountability for certain types of compromised data, they are not uniform and many apply only to financial and/or identifying information, as opposed to other types of data that consumers may feel is of equal or greater sensitivity. Further, credit or identity theft monitoring can mitigate some financial risks, consumers may have less recourse available in regard to compromised info that may have a mental and emotional, but not financial, impact.[80]

---

[74] *FTC v. Wyndham Worldwide Corp*., No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012) (complaint), *In re LightYear Dealer Tech., LLC*, No. C-4687 (Sept. 6, 2016) (complaint).
[75] *FTC v. Wyndham Worldwide Corp*., No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012) (complaint); *In re CafePress*, Nos. C-4768 & C-4769 (Jun. 24, 2022) (complaint); *In re LightYear Dealer Tech., LLC*, No. C-4687 (Sept. 6, 2016) (complaint).
[76] *In re CafePress*, Nos. C-4768 & C-4769 (Jun. 24, 2022) (complaint); *FTC v. Wyndham Worldwide Corp*., No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012) (complaint).
[77] "Cost of a Data Breach Report 2022," IBM (2022) at 10, https://www.ibm.com/reports/data-breach.
[78] *Id.* at 13.
[79] Danielle K. Citron & Daniel Solove, "Risk and Anxiety: A Theory of Data Breach Harms," 96 Texas L. Rev. 737 (2018).
[80] Gilden, Andrew, "The Queer Limits of Revenge Porn," Boston College L. Rev. (September 21, 2022), https://ssrn.com/abstract=4226079.

Security breaches often disproportionately impact vulnerable and marginalized individuals. This includes racial minority groups, women, LGBTQ+ individuals, and young people. For instance, one study found that non-white individuals are more likely to have their identities stolen than white people (21 percent compared to 15 percent), and non-white individuals are the least likely to avoid financial impact due to cybercrime (47 percent compared to 59 percent of all respondents).[81]

Considerations for a Reasonable Data Security Rule

In promulgating a trade regulation rule requiring reasonable security practices, rather than mandating prescriptive (and likely rapidly outdated) requirements, the Commission should rely upon decades of more adaptable standards requiring organizations, for instance, to maintain and implement data security programs.[82]

Adhering to reasonable security standards is fundamentally a risk analysis. Reasonable decisions made prior to a breach in security can look imprudent in hindsight, and poor practices can appear justified simply by the lack of a known security or privacy incident. While the specific elements of a reasonable security program will always be context-dependent, certain measures should be required for any reasonable program, such as data minimization, data obfuscation through means such as encryption, and adoption of user multi-factor authentication.[83] The Commission's long history of remedial data security practices mandates in Consent Decrees and existing federal cybersecurity regulations like the Gramm-Leach-Bliley Act's Safeguards Rule establish specific security requirements that the Commission should consider in a new consumer protection rule.[84] For example, both the Safeguards Rule and FTC Consent Decrees generally require businesses to:

- Designate personnel to coordinate an information security program.
- Conduct periodic risk assessments identifying internal and external risks to the unauthorized access or misuse of consumer information.
- Design, implement, and maintain the safeguards to control the risks identified in the periodic risk assessments.

---

[81] "Demographics of Cybercrime Report," Malwarebytes (Sept. 27, 2021), https://www.malwarebytes.com/resources/2021-demographics-of-cybercrime-report/index.html.

[82] *See, e.g.*, *In re HTC Am. Inc.*, No. C-4406, at 5 (Jul. 2, 2013) (consent order); *States v. Rental Research Servs., Inc.*, No. 072 3228 (D. Minn. Mar. 5, 2009) (consent order); *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012) (consent order).

[83] *See also*, Article 32(1) of the EU General Data Protection Regulation providing several suggested "technical and organizational measures" that organizations might consider – including "pseudonymization or encryption of personal data; *In re CafePress*, Nos. C-4768 & C-4769 (Jun. 24, 2022) (complaint).

[84] Obviously, Safeguards apply to large portions of an entire industry, whereas Consent Decrees apply case-by-case. But decades of Consent Decrees form an informal body of regulatory law enforcement, revealing common requirements on Respondents which closely track with the information security programs mandated by Safeguards.

- Regularly test and monitor program effectiveness.
- Evaluate and oversee service providers.
- Evaluate and adjust the information security program.
- Review policies and procedures to minimize unnecessary data retention.[85]

Additional elements and considerations for potential rulemaking are detailed below:

1. ***Documentation***: Regulators need documentation of security efforts prior to an incident in addition to a record of responses to possible and actual breaches. Organizations must be assured that their actions will not be viewed only through the lens of hindsight after a negative outcome. Similarly, regular assessments or audits are generally required by FTC consent decrees to evaluate the effectiveness of technical and organizational measures.[86]

2. ***Contextual Analysis***: Risk analysis also differs based on the volume, sensitivity, and complexity of data to be protected as well as the nature of the industry.[87] Few of these factors can be known with perfect certainty, and organizations need flexibility to select an appropriate set of tradeoffs that protect consumer data while meeting business needs.

3. ***Encourage Businesses to Leverage Established Cybersecurity Frameworks:*** In order to provide clarity into context-appropriate assessment, facilitate small and medium organizations to take advantage of established work, and drive the adoption of reasonable security practices, the Commission could identify and affirm existing frameworks for cybersecurity planning and decision-making.[88] Frameworks such as the NIST Cybersecurity Framework or the ISO IEC 27001 standard are general enough to

[85] GLBA Safeguards Rule, 16 C.F.R. § 314; *In re CafePress,* Nos. C-4768 & C-4769 (Jun. 24, 2022) (case pending), see also *In re Drizly, LLC*, FTC File No. 2023185 (Oct. 24, 2022) (case pending) (containing the second data minimization requirement under the Commission's Section 5 authority).

[86] *See*, Article 32(1)(d) of the GDPR, which requires "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

[87] *See, e.g.*, Article 32(1) of the EU's General Data Protection Regulation, requiring that data controllers take "into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons … shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk." Essentially, Article 32 requires a comprehensive, risk-based analysis as the underlying baseline for determining what security measures are sufficient for any given data processing activity. This risk assessment must particularly consider risks presented by "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed."

[88] These frameworks provide means and methods to allow organizations to address security and privacy concerns and document their approach in advance of an incident. *See, e.g.*, Article 32(3) of the EU's GDPR conditionally authorizes "adherence to an approved code of conduct or certification mechanism" as a possible way of satisfying the general obligation to ensure appropriate data security imposed in Article 32(1), so long as the code of conduct or certification follows separate GDPR requirements for the authorization of such tools.

apply to most businesses.[89] Other frameworks, such as the New York Department of Financial Services's guidance for cybersecurity in finance, are domain specific.[90] The U.S. Cybersecurity and Infrastructure Security Agency (CISA) even provides guidance for organizations in particular domains seeking to improve cybersecurity based on general frameworks.[91] Frameworks are also created by non-governmental organizations seeking to improve security practices in broad technical domains.[92]

After an incident, organizations that have documented decision-making and physical, technical, and organizational security measures that are consistent with an affirmed security framework should be a significant, though not dispositive, factor in a reasonableness analysis, with a commensurate effect on any subsequent enforcement action. In contrast, organizations unable to provide documentation detailing their implementation of an affirmed security framework, should generally be viewed more critically.[93]

3. Require businesses to comply with their privacy and security promises

The Commission should require organizations to honor any promise, guarantee, or other commitment made in regard to the processing of personal data. FTC enforcement actions reveal

---

[89] *See* "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; "ISO/IEC 27001 Information Security Management," International Organization For Standardization,https://www.iso.org/isoiec-27001-information-security.html (last visited: Nov. 17, 2022). As discussed above, several state laws allow affirmative defenses for companies who demonstrate adherence to industry-recognized cybersecurity frameworks. *See* Ohio Rev. Code Ann. § 1354.02 (2018); Conn. Public Act No. 21-119 (2021); and Utah Code. Ann. § 78B-4-702 (2021).

[90] "Cybersecurity Resource Center," New York State Department Of Financial Services, https://www.dfs.ny.gov/industry_guidance/cybersecurity (last visited: Oct. 14, 2022).

[91] "Cybersecurity Framework," Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/uscert/resources/cybersecurity-framework (last visited: Oct. 14, 2022). For example, CISA has guidelines for healthcare sector organizations seeking to implement the cybersecurity practices consistent with the NIST Cybersecurity Framework while explicitly accounting for differences brought about by operating primarily with healthcare-related data. "Healthcare Sector Cybersecurity Framework Implementation Guide," Cybersecurity & Infrastructure Security Agency (May 2016), https://www.cisa.gov/uscert/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

[92] *See, e.g.,* "CSA Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, https://cloudsecurityalliance.org/research/guidance/ (last visited: Oct. 14, 2022).

[93] Failure to plan for security incidents at all is unreasonable, but narrow exceptions inevitably exist where novel business models do not cleanly fit standard security frameworks. Cybersecurity frameworks will not eliminate the need for auditing and assessment in response to an information security incident, but they may streamline the process. Many security consulting firms provide standard assessments of organizational implementation of cybersecurity frameworks. By affirming a select set of cybersecurity standards, the FTC can focus third party efforts on producing a repeatable, consistent auditing process that is less expensive for small or midsize businesses while simultaneously being accessible to security professionals outside the big auditing firms.

that some businesses make statements about their privacy and security practices that they subsequently fail to uphold.[94] When businesses do not live up to their data protection commitments,[95] it can erode consumer trust,[96] expose consumers to unbargained for privacy and security risks,[97] and harm businesses competitiveness.[98] Companies shouldn't be discouraged from making guarantees in their privacy policies, such as pledges to refrain from disclosing personal information to third parties,[99] to only collect data that was consistent with the company's privacy policy,[100] and to maintain the anonymity of consumer's personal data.[101] However, promises must be accurate.

When companies make statements, including in marketing materials, consumers can, and do, rely on this information, and when those statements are false or inaccurate, the consumer may be

---

[94] *See* Solove & Harzog, "The FTC and the New Common Law of Privacy," at 628 (noting that "[m]uch of the FTC's privacy jurisprudence is based upon a deception theory of broken promises....such as when a company violates its own privacy policy," and providing numerous examples of this.); *See also "*Cooley Privacy Talks: Overview of Privacy Enforcement Actions in the US and EU*,"* Cooley Cyber/Data/Privacy Insights (Feb. 17, 2022), https://cdp.cooley.com/cooley-privacy-talks-overview-of-privacy-enforcement-actions-in-the-us-and-eu/ (noting that the FTC's 2021 enforcement activity focused on deceptive conduct by companies, often around representations about data retention or privacy and security practices) *and* Clay Posey & Mindy Shoss, "Research: Why Employees Violate Cybersecurity Policies*,"* Harvard Business Review (Jan. 20, 2022), https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies (finding that, over a 10 day period, 67% of the employees studied violated their company's cybersecurity policies at least once).

[95] Solove & Harzog, "The FTC and the New Common Law of Privacy," at 628.

[96] *See e.g.,* Venky Anant, Lisa Donchak, James Kaplan, & Henning Soller, "The Consumer-Data Opportunity And The Privacy Imperative," McKinsey & Company (Apr. 27, 2020), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative (finding that historical data breaches and privacy abuses have eroded consumer trust in businesses to protect their personal data across a broad range of industries).

[97] *See, e.g.,* Anna Maria Oritz *et al.*, "Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services*,"* U.S. Government Accountability Office (Mar. 27, 2019), https://www.gao.gov/products/gao-19-230 (discussing that data breaches have exposed hundreds of millions of people to the risk of identity theft); Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, & Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*,"* Pew Research Center (Nov. 15, 2019) https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (noting that "[s]ome 81% of the public say that the potential risks they face because of data collection by companies outweigh the benefits.").

[98] *See, e.g.* Alessandro Acquisti, Allan Friedman, & Rahul Telang, "Is There a Cost to Privacy Breaches? An Event Study" ICIS Proceedings (2006) at 94, https://aisel.aisnet.org/icis2006/94 (finding "a negative and statistically significant impact of data breaches on a company's market value on the announcement day for the breach."); Timothy Morey, Theodore "Theo" Forbath, & Allison Schoop, "Customer Data: Designing for Transparency and Trust*,"* Harvard Business Review (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (observing consumer mistrust about corporate data use can harm businesses ability to compete in the marketplace).

[99] *See, e.g. In re Eli Lilly & Co.*, 133 F.T.C. 763 (2002) (complaint) (charging company with breaking privacy agreement by disclosing customers' personal information).

[100] *See, e.g. In re Microsoft Corp.*, 134 FTC 709, 715 (2002) (complaint) (charging company with collecting information beyond that provided for in stated privacy policy).

[101] *See, e.g. In re Genica Corp.*, No. C-4252 (Mar. 16, 2009) (complaint).

harmed. In fact, positive public statements by an organization may cause a consumer to feel overly confident or secure in that organization's data processing, encouraging them to take action or reveal information that they would not otherwise, putting them at higher risk of greater harm than would otherwise be the case.[102] For instance, users may save or transmit personal or sensitive documents through a service when they believe, accurately or not, that no third party is able to access that data. The Commission has previously pursued cases where companies have represented that they used better security than was actually deployed.[103]

Considerations for a Business Representations Rule

The Commission should consider the form of representations as well as the surrounding context, including written policies, marketing materials, and self-regulatory commitments.

1. ***Form of Representation***: The Commission should consider "representations" regarding a business' privacy and security practices to include self-regulatory commitments as well as statements included in corporate policies and other public-facing corporate materials.[104] Often, the material commitments that businesses make to consumers extend beyond the four corners of a privacy policy. Companies routinely make promises externally, through blog posts, public statements, advertisements, in user interfaces, and through communications with customers.[105]

2. ***Context of the Consumer****:* Consumer expectations are important, and the Commission's existing jurisprudence makes clear that privacy and security promises need to be considered in the context of the consumer. This means that the assurances that businesses make to consumers should always be appropriately contextualized. The FTC takes consumers as it finds them, "full of preexisting expectations, contextual norms, and

[102] Very secure systems may actually make the problem worse, if the presence of these mechanisms falsely encourages people to entrust critical information to such systems. *See* "Computers at Risk: Safe Computing in the Information Age," National Academies of Sciences, Engineering, and Medicine (The National Academies Press 1991), https://doi.org/10.17226/1581.
[103] Daniel Solove & Woodrow Hartzog, "The FTC Zoom Case: Does the FTC Need a New Approach?," Teach Privacy (Nov. 11, 2020), https://teachprivacy.com/the-ftc-zoom-case-does-the-ftc-need-a-new-approach/.
[104] At the state level, voluntary compliance with certain specified "industry recognized cybersecurity frameworks" is an affirmative defense under Ohio law against tort claims in court that allege that the failure to implement reasonable information security controls resulted in a data breach. Ohio Rev. Code Ann. § 1354.02. Under this statute, a covered entity's cybersecurity program conforms to an industry recognized cybersecurity framework in one of three ways: 1) the program "reasonably conforms" to one of six frameworks which include the NIST Framework for Improving Critical Infrastructure Cybersecurity; 2) the program reasonably conforms to the entirety of the HIPAA Security Rule, GLBA, HITECH, or the Federal Information Security Modernization Act of 2014; or 3) the program reasonably complies with both the Payment Card Industry Data Security Standard and an industry framework specified in (1). *Id.* § 1354.03.
[105] *See, e.g. In re Everalbum*, No. C-4743 (May 7, 2021) (complaint); *In re Rite Aid Corp*, No. C-4308 (Nov. 22, 2010) (complaint); *In re US Search Inc.,* No. C-4317 (Mar. 25, 2011) (complaint).

cognitive limitations, and prohibiting companies from exploiting these assumptions and rational ignorance."[106]

4. Prohibit companies from circumventing individuals' clearly expressed and widely adopted privacy preferences without explicit permission from the individual

The Commission should adopt rules that clarify when failing to abide by the clearly expressed privacy preferences of a user constitutes a deceptive trade practice. By providing consumers with control over account privacy settings, companies convey that the preferences they select will govern data collection, use, and transfer. Consumers can be harmed when companies do not honor consumer privacy setting selections, which has been detailed by numerous Commission enforcement actions.[107] Among other harms, the FTC determined that the failure to honor consumer preferences has resulted in the disclosure of personal data to "individuals against whom…[consumers] had obtained restraining orders; abusive ex-husbands…and recruiters they had emailed regarding job leads."[108] Similarly, the Commission has found that a company's inference of consumer geolocation information even when consumers had turned off location collection on their device, "undermined consumers' ability to make informed decisions about their location privacy and to control the collection and use of their location information."[109] These are clear examples of unavoidable and substantial consumer injuries that can be mitigated through a trade regulation rule that sets forth clear obligations and guidance for businesses providing consumers choice over their personal information.

Considerations for an Anti-Circumvention Rule

The Commission should consider the following five factors in developing a rule, which asks businesses to consider the context within which consumers express their preferences, offer straightforward mechanisms for consumers to express their preferences, and limit technical workarounds that contradict consumers' reasonable intentions.

1. ***Recognizing Privacy Preferences:*** A trade regulation rule should establish standards for what types of consumer action can be objectively recognized as a clearly expressed privacy preference. Privacy preferences may be exercised through the controls and options provided to the consumer by a business, such as through privacy dashboards, consent flows, and opt-out toggles or buttons.[110] In the future, as technology, law, and

[106] Solove & Hartzog, "The FTC and the New Common Law of Privacy," at 667.
[107] ***E.g.*** *In re Google Inc*., No. C-4499 (Dec. 5, 2004) (complaint).
[108] *Id.* at 5.
[109] *Id*.
[110] See, e.g. *In re Flo Health,* No. C-4747 (Jun. 22, 2021) (complaint); *In re Mobi*, No. 3:16-cv-3474 (Jun. 6, 2016) (complaint); *In re Paypal,* No. C-4651 (May 24, 2018) (complaint); *In re Everalbum,* No. C-4743 (May 7, 2021) (complaint).

business practices continue to develop, businesses may be able to objectively determine that a privacy preference has been clearly expressed through other avenues, including through authorized user agents, technological signals, and registries. In particular, emerging state laws are recognizing a new class of privacy tools commonly referred to as "opt-out preference signals," which emerged as a topic of discussion at the FTC's rulemaking public forum on September 8, 2022.[111] These mechanisms permit consumers to signal their privacy preferences (typically to opt-out of data sales or targeted advertising) to businesses in an automated manner. Preference signals may ease the burdens of privacy "self-management," allowing consumers to express their privacy choices on a default basis, rather than exercising rights on controls with each individual business with which they interact. However, at present businesses face many challenges in determining whether the receipt of a signal represents a clearly expressed privacy preference. These difficulties and ambiguities must be considered in any trade regulation rule on the topic.

Examples of challenges include:

- *What preference is being expressed?* Current signal preferences purport to express a variety of related privacy requests, such as not to "track," use data for "targeted advertising," "sale," "share," and "limit the use and disclosure of sensitive personal information." Sometimes these have legal bases and other times not. At present it may be unclear what specific privacy preferences a signal is intended to convey.
- *Does the signal represent a consumer preference?* Certain web browsers and plug-ins send preference signals by default, and may prevent consumers from disabling the signal, either on a universal or case-by-case basis, making it unclear whether or not a signal represents a genuine consumer preference.
- *What if a signal conflicts with other expressions of choice?* Businesses may receive both an unambiguous, informed consent from a consumer for particular data processing, as well as a conflicting signal. The establishment of a "consent hierarchy" between different forms of consumer expression of policy preferences is a difficult question that existing state laws have taken varying approaches to.
- *What is the intended scope of a signal?* For signals sent in particular mediums (such as browser settings), it is unclear whether a preference signal can be associated with information that is outside the context (such as information collected in a physical retail store). Even if a signal can be associated with such separate sources of data, it may not be clear that a consumer intends for a signal to apply to those disparate datasets.

[111] "Transcript of the FTC Commercial Surveillance and Data Security Public Forum," FTC (Sept. 8, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/CommercialSurveillanceandDataSecurityRulemakingTranscript09.08.2022.pdf.

2. ***Types of Preferences:*** It is important for regulations to recognize that a consumer's privacy preference can take many forms of intended control over data collection, use, retention, and disclosure. Existing enforcement actions have encompassed a range of privacy preferences including: limiting the visibility or availability of certain content to particular audiences,[112] prohibiting the collection or requesting the deletion of certain data held by a business,[113] or placing limitations on the use of data for specific processing activities, such as the unrestricted sales to third-party entities[114] or processing data for the purposes of enabling cross-context behavioral advertising.[115] Widely available consumer privacy choices common to U.S. and global privacy regimes should be accounted for in any trade rule.

3. ***Circumvention of Clearly Expressed Privacy Preferences:*** A trade regulation rule should ensure that when a user expresses a clear intent to limit the collection, retention, or use of certain data, companies may not circumvent that preference by the means of alternative data streams or uses. Examples of illegal circumvention of privacy choices might include inferring the information at issue from other data sets, purchasing that information from a third party, or using technological workarounds. The FTC's enforcement activity offers clear grounds to prohibit the collection that a user has sought to restrict using alternative methods, such as separate sources of the information,[116] inferences,[117] and where privacy preferences have been expressed on other products or services.[118]

4. ***Interface Design:*** A trade regulation rule should also should provide clarity on illegal, unlawful, or manipulative design choices that subvert a consumer's expressed privacy preferences.[119] The Commission has a long history of enforcement against design

[112] *In re Facebook*, No. C-4365 (Aug. 10, 2012) (complaint) (after finding that Facebook shared user's data with Platform Applications accessed by their friends despite representing to user's that they could restrict access to their data to "Friends" or "Friends of Friends," requiring Facebook to obtain express, informed consent before sharing any nonpublic user information with third parties).
[113] *In re Everalbum*, No. C-4743 (May 7, 2021) (consent agreement) (requiring that Everalbum, a photo storage app, delete all photos and videos collected from users who deactivated their Everalbum accounts).
[114] *In re Flo Health*, No. C-4747 (Jun. 22, 2021) (consent agreement) (requiring that Flo Health not sell or share user health information with third parties without informed, express consent).
[115] *U.S. v. Twitter, Inc.,* No. C-4316 (May 25, 2022) (consent agreement), at 4 (ordering that Twitter not use user phone numbers or email addresses collected for account security purposes for the purpose of serving advertisements).
[116] *See*, *In re Turn Inc.*, No. C-4612 (Apr. 21, 2017) (complaint) (alleging that Turn Inc. had tracked consumers through a X-UIDH header).
[117] *In re Mobi*, No. 3:16-cv-3474 (Jun. 6, 2016) (complaint) (asserting that the company used WiFi network information to infer consumers' precise latitude and longitude).
[118] *In re Zoom,* No. C-4731 (Feb. 1, 2021) (complaint) (claiming that a company covertly deployed a web server on consumers' computers as a means to bypass a privacy and security safeguard that would have asked users to affirm whether they wanted to launch the app).
[119] A recent FTC report called design practices that "obscure or subvert consumers' privacy choices" a "pervasive dark pattern." "Bringing Dark Patterns to Light," FTC (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

practices that obfuscate or subvert consumer privacy choices or lead consumers to share more or different information than they may intend.[120] Additionally, where a reasonable consumer would believe that they have taken an action on a platform that will cause a privacy preference to be honored, the Commission should codify adherence to that preference without requiring a consumer to complete additional steps.[121] Businesses should neither ignore the preferences consumers express in the settings the business makes available, nor should they make settings overly confusing or difficult for consumers to use effectively.

5. ***Necessary and Compatible Processing Activities:*** Finally, as discussed in Section IV(B), the Commission should recognize that certain collection and processing of consumer information is necessary in order to provide a product or service in a secure, lawful, and/or effective manner. For example, location information can be needed to effectuate the delivery of a physical product, and processing or retention of data may be required to meet certain legal obligations, conduct socially beneficial research, or to take action to monitor and prevent various forms of fraud and abuse. Furthermore, depending on the privacy choice a user seeks to invoke and nature of the expression, varying standards for business authentication of a request may be required in order to reasonably protect data subjects. Where the use of data is consistent with consumer expectations and clearly disclosed to a consumer as a condition of using a particular product or service, a consumer consent to such uses may be legitimately inferred. Such expectation-consistent data use can occur when a mapping app collects and uses user's location data for navigation purposes or when a health app collects and processes user health data for purposes related to the app's functionality.

[120] For example, in *In re Path*, Path, a "smart journal[ing]" app, represented to users that they could "Add Friends" through three different mechanisms: by allowing the app to "[f]ind friends from your contacts;" "[f]ind friends from Facebook;" or "[i]nvite friends to join Path by email or SMS." In reality though, no matter what option a user selected, the app "automatically collected personal information from users' mobile device contacts (also known as the user's "address book") and stored the personal information on Defendant's servers." In its enforcement action against Path, the Commission determined that this was a deceptive practice that violated the FTC Act. *In re Path Inc.,* No. C-130448 (Feb. 1, 2013) (complaint) *See also,* Harry Brignull, FTC Dark Patterns Workshop Transcript at 14-15 (Apr. 29, 2021), available at https://www.ftc.gov/system/files/documents/public_events/1586943/ftc_darkpatterns_workshop_transcript.pdf. While such practices are sometimes called "dark patterns" this is an overbroad and imprecise term that is unlikely to be useful in the context of a trade rule.

[121] See, *In re PayPal,* No. C-4651 (May 24, 2018) (complaint) (in which Commission alleged that requiring the use of multiple distinct settings in order to actually limit the public disclosure of a consumer's financial activity "has the effect of overriding [a consumer's] clearly expressed privacy preferences")

B. The Commission should articulate when discriminatory algorithmic decision-making constitutes an unfair trade practice under Section 5.

Algorithmic decision-making technologies, including technologies that employ machine learning and artificial intelligence, are increasingly used by digital services to personalize user experiences, serve ads, and otherwise power products like health risk scoring, workplace assessments, ridehail trip assignments, and vehicle crash-avoidance systems. Algorithmic technologies drive products and services used by millions of consumers, while also creating clear risks - including risks of discrimination against marginalized individuals and communities.

The FTC's recent settlement in *FTC vs. Passport Automotive Group* and recent Commissioners' statements indicate the Commission's willingness to use its unfairness authority to combat discrimination.[122] A clear rule regarding the intersection of antidiscrimination efforts, algorithmic technologies, and the Commission's unfairness authority would help ensure that individuals and communities are well protected, and businesses have clarity regarding their obligations.

Such a rule should:

1. identify the types of harms that give rise to a finding of unfair discrimination (e.g. financial, physical, reputational, or other harms);
2. state the Commission's standard for analyzing and assessing when unfair discrimination occurs (e.g. disparate treatment, disparate impact, or another standard);
3. distinguish between harmless commercial practices that differentiate between individuals and unfair discrimination that harms individuals or communities; and
4. state how the Commission's approach aligns or differs with related anti-discrimination regimes enforced by the Commission, other U.S. agencies, and global frameworks. We urge the Commission to codify an approach that is consistent with existing U.S. and global frameworks, which focus on algorithmic decisions that affect individuals' access to critical opportunities in the market, such as financial services, housing, insurance, employment, education, and other essential goods or services.

[122] *FTC v. Passport Automotive Group, Inc.,* FTC File No. 2023199 (Oct. 18, 2022); Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter In the Matter of Napleton Automotive Group Commission, No. 2023195 (Mar. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Statement%20of%20Chair%20Lina%20M.%20Khan%20Joined%20by%20RKS%20in%20re%20Napleton_Finalized.pdf; Statement Of Commissioner Alvaro M. Bedoya Regarding The Commercial Surveillance Data Security Advance Notice Of Proposed Rulemaking, FTC (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Bedoya%20ANPR%20Statement%2008112022.pdf; Statement Of Commissioner Rohit Chopra In the Matter of Liberty Chevrolet, Inc. d/b/a Bronx Honda Commission No. 1623238 (Aug. 11, 2022), https://www.ftc.gov/system/files/documents/public_statements/1576002/bronx_honda_final_rchopra_bronx_honda_statement.pdf.

Algorithmic Technologies Create Clear Benefits for Consumers and the Market, as well as Clear Risks - Including Risks of Discrimination Against Marginalized Individuals and Communities.

FPF has highlighted how harms caused by unfair and deceptive algorithmic processing activities can perpetuate and exacerbate discriminatory impacts and historical divides that persist today.[123] These discriminatory impacts can come in the form of differential access to job opportunities,[124] benefits, housing,[125] credit,[126] healthcare,[127] and education, as well as economic loss, social detriment, or loss of liberty.

At the same time, algorithmic technologies can help detect cancer earlier in patients and identify areas in need of assistance after natural disasters.[128] Also, they can save companies millions of dollars and help consumers get goods and services faster and more reliably than human

---

[123] *See e.g.,* "Unfairness by Algorithm: Distilling the Harms of Automated Decision-making," Future of Privacy Forum (Dec. 11, 2017), https://fpf.org/wp-content/uploads/2017/12/FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf; Yeshimabeit Milner and Amy Traub, "Data Capitalism and Algorithmic Racism," Demos (May 2015), https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf; Annette Bernhardt, Reem Suleiman & Lisa Kresge, "Data and Algorithms at Work: The Case for Worker Technology Rights"*, UC Berkeley Labor Center* (Nov. 3, 2021) https://laborcenter.berkeley.edu/data-algorithms-at-work/; John Villasenor & Virginia Foggo, "Algorithms And Housing Discrimination: Rethinking Hud's New Disparate Impact Rule," *Brookings* (Mar. 5, 2021), https://www.brookings.edu/blog/techtank/2021/03/05/algorithms-and-housing-discrimination-rethinking-huds-new-disparate-impact-rule/; *and* Ryan S. Baker & Aaron Hawn, "Algorithmic Bias in Education"*,* Int. J. Artif. Intell. Educ. 32, 1052–1092 (2022), https://doi.org/10.1007/s40593-021-00285-9.

[124] Jenny R. Yang, "Three Ways AI Can Discriminate in Hiring and Three Ways Forward," Urban Institute (Feb. 12, 2020), https://www.urban.org/urban-wire/three-ways-ai-can-discriminate-hiring-and-three-ways-forward.

[125] United States Department of Housing and Urban Development v. Facebook, Charge of Discrimination, FHEO No. 01-18-0323-8 (Mar. 28, 2019) *available at* https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf; Linda Morris & Olga Akselrod, "Holding Facebook Accountable for Digital Redlining," ACLU (Jan. 27, 2022), https://www.aclu.org/news/privacy-technology/holding-facebook-accountable-for-digital-redlining; Terry Gross, "A Forgotten History of How the U.S. Government Segregated America," NPR (May 3, 2017), https://www.npr.org/2017/05/03/526655831/a-forgotten-history-of-how-the-u-s-government-segregated-america.

[126] Emmanuel Martinez & Lauren Kirchner, "The Secret Bias Hidden In Mortgage-Approval Algorithms," Ap News (Aug. 25, 2021), https://apnews.com/article/lifestyle-technology-business-race-and-ethnicity-racial-injustice-b920d945a6a13db1e1aee44d91475205.

[127] Kellie Owens & Alexis Walker, "Those Designing Healthcare Algorithms Must Become Actively Anti-Racist," Nature Medicine (Sept. 9, 2020), https://www.nature.com/articles/s41591-020-1020-3.

[128] NCI Staff, "Can Artificial Intelligence Help See Cancer in New, and Better, Ways?," National Cancer Institute (Mar. 22, 2022), https://www.cancer.gov/news-events/cancer-currents-blog/2022/artificial-intelligence-cancer-imaging; Ben Monique M. Kuglitsch, Ivanka Pelivan, Serena Ceola, Mythili Menon, Elena Xoplaki, "Facilitating adoption of AI in natural disaster management through collaboration," 1579 Nature Communications 13 (2022), https://doi.org/10.1038/s41467-022-29285-6.

systems.[129] In some circumstances, data analysis can be used to combat discrimination.[130] The Commission should weigh the harms and benefits of algorithmic technologies - including likely future impacts - with respect to these systems. FTC rules regarding unfair discrimination should distinguish between harmful and beneficial commercial practices.

The Commission's rules should be informed by an understanding of the ways in which algorithmic discrimination produces disparate outcomes for individuals and groups. Harmful outcomes often arise from inaccurate predictions based on unrepresentative data, faulty interpretations, and algorithmic design flaws.[131] These flaws can subject consumers to financial and physical harms, and emerging technologies and practices can mitigate these risks in some circumstances.

The FTC's Recent Settlement and Commissioners' Statements Indicate the Commission's Willingness to Use its Unfairness Authority to Combat Discrimination

In *Passport Automotive*, the FTC settled claims that Passport's automobile financing practices constituted an unfair trade practice under Section 5 because the company "unlawfully discriminate[d] on the basis of race, color, and national origin by imposing higher costs on Black and Latino consumers on average than non-Latino White consumers."[132] The Commission alleged that Black and Latino consumers were substantially injured, the injuries could not be reasonably avoided, and there were no countervailing benefits for consumers or the market.[133]

Passport follows previous statements by Commissioners and staff that the FTC considers Section 5's unfairness authority to be an independent legal basis in actions involving discriminatory practices that harm consumers.[134] This approach builds on the Commission's decades-long work

[129] Thomas H. Davenport & Randy Bean, "Companies Are Making Serious Money With AI," MIT Sloan Management Review (Feb. 17, 2022), https://sloanreview.mit.edu/article/companies-are-making-serious-money-with-ai/.
[130] "BIG DATA: A Tool for Fighting Discrimination and Empowering Groups," FPF & The Anti-Defamation League (Sept. 2014) https://fpf.org/wp-content/uploads/2014/09/Big-Data-A-Tool-for-Fighting-Discrimination-and-Empowering-Groups-FINAL1.pdf.
[131] *See* Rebecca Kelly Slaughter, "Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission," Yale Tech. L. J. (August 2021),.
[132] *FTC v. Passport Automotive Group, Inc.,* No. 2023199 (Oct. 18, 2022) (consent decree).
[133] *Id.*
[134] Statement of Chair Lina M. Khan Joined by Commissioner Rebecca Kelly Slaughter, FTC File No. 2023195 (Mar. 31, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Statement%20of%20Chair%20Lina%20M.%20Khan%20Joined%20by%20RKS%20in%20re%20Napleton_Finalized.pdf; Statement Of Commissioner Alvaro M. Bedoya, FTC (Aug. 11, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Bedoya%20ANPR%20Statement%2008112022.pdf; "Statement Of Commissioner Rohit Chopra" File No. 1623238 (Aug. 11, 2022), https://www.ftc.gov/system/files/documents/public_statements/1576002/bronx_honda_final_rchopra_bronx_honda_statement.pdf; "Statement Of Commissioner Rohit Chopra" at 2 n.6 ("For example, if a rideshare app's pricing algorithm systematically charges higher prices to women requesting rides at night, compared to similar ride requests for men, this could constitute a violation of the FTC Act's prohibition on unfair acts

combatting discriminatory financial practices under its Equal Credit Opportunity Act (ECOA),[135] and the Fair Credit Reporting Act ("FCRA")[136] authorities.

While the Commission "has addressed machine-based credit underwriting models for decades," and "has long experience dealing with the challenges presented by the use of data and algorithms to make decisions about consumers,"[137] the use of the FTC's Section 5 unfairness authority as an independent legal basis to police discriminatory algorithmic practices is relatively new. Clear rules regarding the nature and scope of that authority would be helpful to the general public, individual consumers, and businesses. Further guidance is needed to help clarify the standards under which the Commission would consider a particular algorithmic system discriminatory.

In some ways, the Commission's use of its unfairness authority represents a re-invigoration of the FTC's pre-1964 approach to anti-discrimination enforcement. In *In Re First Buckingham Cmty Inc* and *Kirchner v. FTC*, the Commission based anti-discrimination actions on its Section 5 authority.[138] The Commission ultimately dismissed those cases due to the passage of the Civil Rights Act of 1964,[139] and other agencies - such as the Equal Opportunity Employment Commission and the Department of Housing and Urban Deveopment - have played important roles in combatting unlawful discrimination. But the Commission recently stated that "where Congress passes laws prohibiting conduct that also violates the FTC Act, the FTC often charges violators with the full range of law violations, including Section 5. Section 5 does not wilt when Congress legislates."[140] Some experts have welcomed the FTC's approach, arguing that it can fill

---

or practices."); Elisa Jillson, "Aiming for truth, fairness, and equity in your company's use of AI," Federal Trade Commission (Apr. 21, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai (stating that the sale or use of racially biased algorithms is prohibited by the FTC Act).

[135] *See* Section 701(a)(1) of the Equal Credit Opportunity Act (ECOA), 15 U.S.C. § 1691(a)(1) (prohibiting a creditor from discriminating against an applicant with respect to any aspect of a credit transaction on the basis of race, color, religion, national origin, sex, marital status, or age (provided the applicant has the capacity to contract)); and Section 704(c) of the ECOA, 15 U.S.C. § 1691c(c) (empowering the Commission to enforce the ECOA).

[136] "The FCRA and Unlawful Discrimination: A Possible Foreshadowing of FTC Enforcement Priorities," National Law Review (Dec. 11, 2020), https://www.natlawreview.com/article/fcra-and-unlawful-discrimination-possible-foreshadowing-ftc-enforcement-priorities.

[137] Andrew Smith, "Using Artificial Intelligence and Algorithms," Federal Trade Commission Business Blog (Apr. 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

[138] *See, ex., In re First Buckingham Cmty Inc*, 73 FTC 938 (1968).

[139] Id; *Kirchner v. FTC*, 337 F.2d 751 (9th Cir. 1964).

[140] Id.; *See also* Majority Statement in *FTC v. Passport Automotive Group, Inc.,* No. 2023199 (Oct. 18, 2022) ("The fact that harmful conduct may be subject to other legal or regulatory regimes does not in itself limit (or lessen) the FTC's responsibility to use all of our available authorities to target such conduct. Where Congress passes laws prohibiting conduct that also violates the FTC Act, the FTC often charges violators with the full range of law violations, including Section 5. Section 5 does not wilt when Congress legislates.").

a gap in existing protections,[141] while others caution against the broad application of unfairness authority in anti-discrimination cases.[142]

When crafting rules, the FTC should pursue an approach that is consistent with existing U.S. frameworks, such as those established by the 1964 Act, EEOC, HUD, and the Consumer Financial Protection Bureau. An FTC trade regulation rule also presents an opportunity to align anti-discrimination protections with global frameworks, such as Europe's GDPR, which offers protections against discriminatory algorithmic decisions that have "legal or similarly significant effects."[143] The GDPR may offer particularly relevant guidance in the context of risk analysis and mitigation strategies.[144]

Rules Regarding Unfair Discrimination Should Identify Actionable Harms

In its recent enforcement actions and statements regarding unfair discrimination, the Commission focused on commercial practices that produced clear financial harm. In *Passport Automotive*, Black and Latino car buyers paid more than non-Latino White consumers for similar products and services. As noted in Section II, this sort of economic harm, along with "unwarranted health and safety risks," has been a primary focus of the Commission's unfairness enforcement. The Commission has been more skeptical of emotional or other harms in the context of its unfairness authority.

---

[141] "What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities," Electronic Information Privacy Center (Jun. 2021), https://epic.org/wp-content/uploads/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf; Stephen Hayes & Kali Schellenberg, "Discrimination Is 'Unfair:' Interpreting UDA(A)P to Prohibit Discrimination," Protect Borrowers (Apr. 2021), https://protectborrowers.org/wp-content/uploads/2021/04/Discrimination_is_Unfair.pdf; *See also* "Introductory Remarks of Commissioner Rohit Chopra," National Fair Housing Alliance - 2020 National Conference (Oct. 6, 2020), available at https://www.ftc.gov/system/files/documents/public_statements/1581594/final_remarks_of_rchopra_to_nfha_v3.pdf.

[142] "Unfairness and Discrimination: Examining the CFPB's Conflation of Distinct Statutory Concepts," Buckley LLP InfoBytes (Jun. 2022), https://buckleyfirm.com/sites/default/files/Buckley%20Infobytes%20-White%20Paper%20on%20CFPB%20UDAAP%20Authority%20-%202022.06.28.pdf/.

[143] Sebastião Barros Vale and Gabriela Zanfir-Fortuna, "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities," FPF (May 2022), https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf.

[144] For example, the GDPR requires that controllers engaged in any processing "that is likely to result in a high risk to the rights and freedoms of natural persons" (as well as a smaller list of explicitly identified activities) conduct a data protection impact assessment prior to the processing to assess whether the activity is "necessary and proportionate" and properly "assess[es] the risks to the rights and freedoms of data subjects." Moreover, automated decision-making systems are included by national regulators in the EU on their lists of processing operations that always require a DPIA to be conducted. See, e.g. Article 35, EU General Data Protection Regulation 2016/679; Barros Vale &, Zanfir-Fortuna, "Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities," at p. 25-27.

The Commission's rulemaking can clarify what types of harms it considers when analyzing allegations of unfair discrimination. Some algorithmic discrimination falls squarely within the Commission's traditional interest in economic and physical harms. For example, potentially discriminatory health risk scores can raise the price of health insurance coverage or deny coverage altogether,[145] and some vehicle anti-collision systems can perform more poorly when detecting pedestrians with darker skin tones.[146] Some have called on the Commission to consider other harms, including emotional or reputational harms, when analyzing claims of unfair discrimination. A Commission rule could provide needed clarity.

The Commission's rulemaking can also clarify what sorts of countervailing benefits to individuals and the market it considers when analyzing allegations of unfair discrimination. For example, companies, patients, and the market typically benefit when insurance rates are set efficiently and accurately, and vehicle anti-collision systems can enhance safety for all pedestrians - even if the benefits are unequally distributed.[147] Further, human decisionmaking is not without bias, and algorithmic decisions can potentially deliver less biased outcomes; algorithmic analysis can also be used to affirmatively identify and mitigate bias.

Rules Regarding Unfair Discrimination Should State the Commission's Standard of Analysis

The Commission's approach in *Passport Automotive* and related matters appears to be consistent with other civil rights laws, which recognize disparate impact claims - challenges to a seemingly neutral practice that "caused or predictably will cause a discriminatory effect."[148] However, uncertainty remains. *Passport Automotive* does not explicitly identify disparate impact as the Commission's operative theory, and does not resolve whether the FTC views its unfairness authority to include other traditional civil rights claims, such as disparate treatment. Furthermore, disparate impact claims are typically adjudicated using a complex burden-shifting analysis and

[145] Marshall Allen, "Health Insurers Are Vacuuming Up Details About You – And It Could Raise Your Rates," ProPublica (July 17, 2018), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates; Geoffrey R. Hileman, Syed Muzayan Mehmud, & Marjorie A. Rosenberg, "Risk Scoring in Health Insurance," Society Of Actuaries (July 2016), https://www.soa.org/4937c5/globalassets/assets/files/research/research-2016-risk-scoring-health-insurance.pdf; Paul Campos, Abigail Saguy, Paul Ernsberger, Eric Oliver, & Glenn Gaesser, "International Journal of Epidemiology," Vol. 35, Issue 1, (Feb. 2006) at 55–60, https://doi.org/10.1093/ije/dyi254.

[146] *See* Benjamin Wilson, Judy Hoffman, and Jamie Morgenstern, "Predictive Inequity in Object Detection," Cornell University Computer Vision and Pattern Recognition (Feb. 21, 2019), https://doi.org/10.48550/arXiv.1902.11097.

[147] Advancing a more equitable society in many cases warrants legislation or ethical standards to protect individuals from unequal costs, even if inequalities would make the overall market more efficient.

[148] *Texas Dep't of Hous. and Cmty. Affairs v. Inclusive Communities Project, Inc.*, 576 U.S. 527 (2015).

balancing test.[149] It is not clear whether, or how, the Commission borrows from that framework when analyzing discrimination claims under its unfairness authority.

In part, the Commission's unfairness authority seeks to combat practices that undermine "essential precondition[s] to a free and informed consumer transaction, and, in turn, to a well-functioning market."[150] This aligns with a less discussed, but equally important, theory central to the civil rights movement – that an integrated society is one that is more economically secure, and one of the cardinal economic harms of segregation is that discriminatory conduct is an inherent market inefficiency. This view is embodied in independent, but interconnected, federal regimes that embody the longheld belief that a more integrated society is one that is more affluent and secure.[151] The Commission's approach in *Passport Automotive* is consistent with this view, but consumers and businesses need greater certainty regarding the FTC's analytical framework in order to benefit from and comply with protections established under such a theory.

A clear statement of the Commission's standard of analysis is particularly important in the context of algorithmic decisions. Experts have identified more than 20 different measures of algorithmic fairness, many of which are mutually incompatible.[152] And algorithmic decisionmaking often involves multiple entities, including organizations that provide training data, vendors that develop algorithms, and companies that use the algorithms to make decisions about individuals. A Commission rule could clearly state the relevant standards and identify which parties are responsible for particular aspects of ensuring fair data processing.

---

[149] *Texas Department of Housing and Community Affairs v. Inclusive Communities Project Inc.*, 576 U.S. 519, 527 (2015) ("[T]he plaintiff "has the burden of proving that a ch allenged practice caused or predictably will cause a discriminatory effect." . . . After a plaintiff does establish a prima facie showing of disparate impact, the burden shifts to the defendant to "prov[e] that the challenged practice is necessary to achieve one or more substantial, legitimate, non-discriminatory interests." . . . Once a defendant has satisfied its burden at step two, a plaintiff may "prevail upon proving that the substantial, legitimate, nondiscriminatory interests supporting the challenged practice could be served by another practice that has a less discriminatory effect."").

[150] "FTC Policy Statement on Unfairness," FTC (Dec. 17, 1980).

[151] *E.g.* Title VII (employment), Title II (public accommodations), Title IV (equal protection of students) of the Civil Rights Act of 1964, the Equal Credit Opportunity Act, the Americans with Disabilities Act, and the Fair Housing Act.

[152] Sahil Verma and Julia Rubin,"Fairness Definitions Explained," ACM/IEEE International Workshop on Software Fairness (2018), https://fairware.cs.umass.edu/papers/Verma.pdf.

Rules Regarding Unfair Discrimination Should Distinguish Between Harmful and Beneficial Commercial Practices

Experts have argued that a wide range of practices could give rise to unfair discrimination claims: price differention between customers or communities;[153] disparate monetization for content creators on platforms;[154] discriminatory ad practices;[155] and the disparate pricing of goods for those in economically disadvantaged neighborhoods.[156]

At the same time, algorithmic decisions can help promote affirmative action programs, display more representative content in advertisements and recommendations when serving diverse communities, and uncover otherwise hidden bias in automated decisions - indeed, some form of data collection for marginalized communities is likely a necessary component of self-testing for bias in algorithms.

In many circumstances, data-driven technologies make decisions about individuals that do not affect core rights, even when those decisions impact individuals and communities differently. For example, online ads routinely promote particular skincare products to Black women,[157] streaming services often highlight classic films and music to older users, and retailers promote training programs and athletic gear to users who are interested in sports or fitness.

Regulations regarding discriminatory processing activities and automated systems should differentiate between discrimination that results in a loss of opportunity by a protected class versus uses of protected class status for greater societal benefit. The frameworks set forth by

[153] Ray Fisman and Michael Luca, "Fixing Discrimination in Online Marketplaces," Harvard Business Review (Dec. 2016), https://hbr.org/2016/12/fixing-discrimination-in-online-marketplaces; Jaravel, Xavier, "The Unequal Gains from Product Innovations: Evidence from the US Retail Sector," Quarterly Journal of Economics (December 26, 2016), https://ssrn.com/abstract=2709088; Max Ehrenfreund, "The Poor Are Paying More And More For Everyday Purchases, A New Study Warns," The Washington Post (May 20, 2016), https://www.washingtonpost.com/news/wonk/wp/2016/05/20/the-poor-pay-more-for-everyday-purchases-and-its-getting-worse-a-new-study-warns/?wpmm=1&wpisrc=nl_wonk.

[154] Shoshana Wodinsky, "Exclusive: How TikTok scrutinizes and scores the creators on its shopping platform," Market Watch (Nov. 9, 2020), https://www.marketwatch.com/story/exclusive-how-tiktok-scrutinizes-and-scores-the-creators-on-its-shopping-platform-11668003397?reflink=mw_share_twitter; "Executive Summary," Creator Economy Report (2022), https://takecreativecontrol.org/wp-content/uploads/2022/08/ExecutiveSummary-Final.pdf.

[155] Piotr Sapiezynski, Avijit Ghosh, Levi Kaplan, Aaron Rieke, & Alan Mislove, "Algorithms that 'Don't See Color': Measuring Biases in Lookalike and Special Ad Audiences," Northeastern University (May 2022), https://arxiv.org/pdf/1912.07579.pdf.

[156] Erik Eckholm, "Study Documents 'Ghetto Tax' Being Paid by the Urban Poor," The New York Times (Jul. 19, 2006), https://www.nytimes.com/2006/07/19/us/19poor.html.

[157] Jada Jackson, "Beauty's Next Big Opportunity: Melanin-Rich Skincare," Vogue Business (Oct. 31, 2022), https://www.voguebusiness.com/beauty/beautys-next-big-opportunity-melanin-rich-skincare.

ADPPA[158] or the Lawyers Committee for Civil Rights Under Law provide helpful starting points.[159] Such a rule should identify the circumstances in which automated decisions are unlikely to impact core rights and trigger unfairness concerns under Section 5.

IV. Guiding Principles and Considerations

When crafting specific rules, we recommend that the Commission consider several guiding principles and overall considerations. Each is deeply rooted in the legal and policy foundations of data protection, and has the potential to impact all aspects of future rulemaking:

- First, it is essential to recognize that personal data exists on a broad spectrum of identifiability, rather than in binary categories of "personal information" or "not personal information." This creates complexities when crafting rules concerning consumer control, such as the rights to access, delete, and consent or object to the processing of data.
- Second, standards for evaluating the fairness of "secondary uses" of data should define the boundaries of what secondary uses are compatible or incompatible with the purpose for which the data was collected, based on a careful evaluation of context, expectations, harms, and benefits of processing, including to competition.
- Third, it is especially important to consider the harms that sensitive data use can create, the manner in which those harms impact marginalized communities, and the heightened protections that may be appropriate to mitigate those harms.

A. Recognition that Data Exists on a Spectrum of Identifiability

Personal information exists within a broad range of practical identifiability in the commercial marketplace. This characteristic of data impacts almost all aspects of commercial privacy and data protection, including: the accuracy of mandated disclosures, measures that companies take to reduce risk, Privacy by Design (PbD) and Data Protection by Design (DPbD); and compliance with individual access, deletion, and consent (opt-in and opt-out) rights.

Some data is explicitly personal, such as a home address, most phone numbers, an unredacted medical record, or information in a verified user account. Likewise, some data is explicitly non-personal. Non-personal information includes information that does not relate to persons (e.g.

---

[158] The American Data Privacy and Protection Act ("ADDPA"), H.R. 8152, 117th Cong. (2022).

[159] *See, e.g.*, "The Online Civil Rights and Privacy Act of 2019," Lawyers Committee for Civil Rights Under Law (2019) https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf (stating that, "[i]n specifying additional unfair or deceptive practices, the Commission shall consider...(7) Methods for fairly promoting equal opportunity in housing, employment, credit, insurance, education, or healthcare, through targeted outreach to underrepresented populations in a fair and non-predatory manner; (8) How to increase diversity and inclusion by fairly promoting content generated by and small businesses owned by members of underrepresented populations).

environmental or industrial sensor data), or data that has been sufficiently aggregated, obscured, or modified that it no longer reasonably relates to any specific person.

De-Identification and Privacy Enhancing Technologies

Identifiability depends on a wide range of factors, including the specific social context and the existence of outside information and external threats. For example, a database that includes "first and last name" is almost always personal – yet information associated with the name "John Smith, USA" could likely be published without risk of revealing information about any specific person. In other circumstances, even aggregated statistics can indirectly reveal information about individuals if the population is small, contains outliers. For example, "*Fifth-grade Asian students in County X are underperforming relative to national standards*" might be an aggregated statistic, but the information would not be properly de-identified if County X had only one Asian Fifth-grade student. For these reasons, the U.S. Census Bureau publishes statistical information about geographic areas only after "injecting noise" into the data, so that it can be used for a wide range of valuable policy decisions, while reducing the risk that the data could reveal information about any specific household.[160]

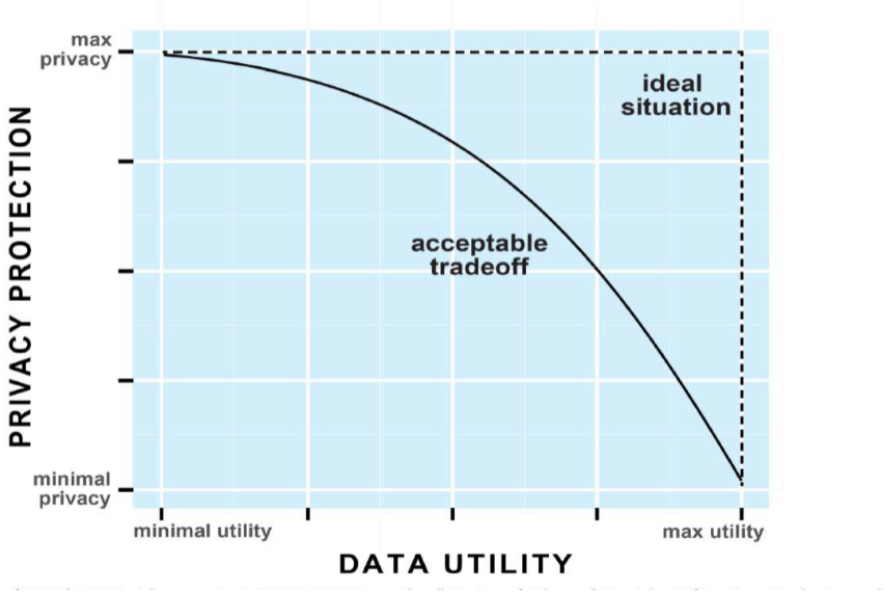


Figure 1. Privacy-Utility Trade-Off.[161]

[160] "Understanding Differential Privacy," United States Census Bureau, https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance/differential-privacy.html (last visited: Nov. 14, 2022).

[161] Lucy Mosquera, "State of Play of De-identification Techniques," FPF & CPCD (2022), https://www.cpdpconferences.org/events/fpf-masterclass; *See also* Alex Berke & Dan Calacci, "The Tradeoff Between the Utility and Risk of Location Data and Implications for Public Good," MIT Media Lab (Mar. 24, 2019) https://www.media.mit.edu/publications/the-tradeoff-between-the-utility-and-risk-of-location-data-and-implications-for-public-good/.

Given the inherent policy trade-off in large datasets between utility of data and disclosure avoidance (demonstrated in Figure 1), most U.S. legal approaches to de-identification have emphasized reasonable technical, legal, and administrative processes to reduce risk of identifiability, rather than seeking to eliminate all risk. For example, medical records can be used to conduct valuable healthcare research across populations, if de-identified in accordance with HIPAA standards by removing direct and indirect identifiers to reduce risk of identifiability.[162]

"Indirect identifiers" are information that can be used to re-identify individuals when combined with external information: information such as dates, demographic information (race, ethnicity), or socioeconomic variables (occupation, salary). Although they introduce risk, indirect identifiers are often critical to the utility of data. They can help identify or measure the spread of disease, the performance of schools, discrimination against specific ethnic groups, failure of services in specific regions, or vectors for fraud. Minimizing these indirect identifiers requires an inherent policy trade-off that balances benefits and risks, with controls tailored to ensure a fair balance.

In recent years, a nascent industry has emerged for the development and implementation of Privacy Enhancing Technologies (PETs). Examples of PETs include differential privacy, advanced cryptographic techniques, federated learning, and other evolving technologies.[163] The use of PETs to reduce risks associated with data has clear and immediate benefits for consumers, insofar as PETs can reduce the material risks of data breaches and facilitate gaining valuable insights from data while minimizing (or eliminating) invasions of privacy.[164] Yet, according to a 2021 Future of Privacy Forum study, "the lack of common understanding about privacy terms is limiting the growth of the privacy tech industry."[165]

In the midst of this uncertainty, the FTC has a crucial opportunity to set fair rules for individuals and businesses. It can do so by ensuring, for example, that companies describing data as

---

[162] "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule," U.S. Department of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited: Nov. 18, 2022).

[163] *See*, *Proceedings on Privacy Enhancing Technologies Symposium*, https://petsymposium.org/ (last visited: Nov. 18, 2022).

[164] For example, an AI-training approach called 'federated learning' involves training an AI model using multiple data sets housed on different servers without that data being shared across those servers, thus preserving privacy. A University of Pennsylvania Medical School model trained using this federated learning has recently proven extremely effective at helping doctors better identify and treat brain tumors. "New Machine Learning Method Allows Hospitals to Share Patient Data Privately," Penn Medicine Press Release (July 28, 2020), https://www.pennmedicine.org/news/news-releases/2020/july/new-machine-learning-method-allows-hospitals-to-share-patient-data-privately.

[165] "Privacy Tech's Third Generation: A Review of the Emerging Privacy Tech Sector," FPF & Privacy Tech Alliance with Tim Sparapani and Justin Sherman (Jun. 2021), https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf.

"de-identified" are in fact adhering to a high technical and administrative standards that minimize risks of identification, while recognizing the benefit risk trade-off involved and the slide scale of rights commensurate. [166]

Definitions of De-identified Data:

- Data that has been perturbed or otherwise altered using leading technical methods to make it difficult or impossible to re-identify individuals. This information is typically subject to a combination of technical, administrative, and legal controls.[167]
- In a 2012 report, the FTC described data as not "reasonably linkable" to individual identity to the extent that a company: (1) takes reasonable measures to ensure that the data are de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data (the "Three-Part Test").[168]

The benefits of establishing strong national standards for de-identification would include greater clarity for regulated businesses, better protect consumers, and further facilitate the development and adoption of PETs in the rapidly growing privacy technology sector.

See Appendix A for a table with more information regarding practical de-identification.

Less Readily Identifiable Personal Information

In contrast to efforts to fully de-identify data – i.e. through altering, perturbing, aggregating, and otherwise modifying data to reduce or eliminate any information about individuals – data that fuels the modern ecosystem for digital products, content, and services is typically not "de-identified."

As an example, device identifiers and similar indirectly linkable information are almost always considered "personal information" in privacy law, because of the ability to use such data to create

[166] For example, a 2020 report revealed that while the widely-used family safety app Life360 "states it anonymizes the data it sells, [the company in fact] fails to take necessary precautions to ensure that location histories cannot be traced back to individuals." John Keegan & Alfred Ng, "The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users," The Markup (Dec. 6, 2021), https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.

[167] Simson L. Garfinkel, "De-Identification of Personal Information," National Institute of Standards and Technology (Oct. 2015) at 2, http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

[168] "Protecting Consumer Privacy In An Era of Rapid Change," FTC (Mar. 2012) at 21, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. State laws provide similar definitions. *See* The Colorado Privacy Act Colo. Rev. Stat. § 6-1-1301(11); The California Privacy Rights Act (CPRA) Cal. Civ. Code § 1798.140(m).

detailed, comprehensive profiles of a person's online and offline behavior, which can allow for the singling out of individuals, targeting of content, and the potential to use external information or look-up databases to directly identify individuals. When such identifiers are widely shared or sold without controls, the risk of identification is clear. However, with significant restrictions and controls, especially for sensitive data, it may be feasible to reduce the risk of identification, provide consumer controls, and otherwise tailor protection to different scenarios based on utility, risk and the capability of reliably providing specific rights.

USER AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36

Figure 2. A "User Agent" is information automatically sent by your browser to every website's server in order to communicate information about your browser and its version, and allow the website to load content and otherwise function properly for that browser.[169]

Consider, for example, the wide range of technical information that must be communicated between browsers and website servers in order to access the modern internet or "open web." *See Figure 2.* Most websites, advertising networks, and analytics providers have long relied on the transfer and sale of such device and browser-specific information to deliver and measure the effectiveness of advertisements and other online content. Such data can also be used for purposes such as detecting fraud or enabling third-party content (fonts, widgets, comment features on news sites).[170]

In practice, a company that solely processes device or network information often lacks the ability to reasonably authenticate or verify consumer requests. Without first-hand knowledge of the identity of online visitors, such commercial entities may take a wide variety of risk-based approaches to complying with consumer access rights under applicable state and global laws.[171] For highly sensitive information, such as precise geo-location, this might include requiring very high levels of authentication (such as asking the individual to join a video call and share a copy of

[169] "Panopticlick," The Electronic Frontier Foundation, https://coveryourtracks.eff.org (last visited: Nov. 14, 2022).

[170] *See, ex.*, K. Vengatesan, A. Kumar, S. Yuvraj, V. D. Ambeth Kumar, and S. S. Sabnis, "Credit Card Fraud Detection Using Data Analytic Techniques," 3 Advances in Mathematics: Scientific Journal 9 (2020), https://www.research-publication.com/amsj/uploads/papers/vol-09/iss-03/AMSJ-2020-N3-43.pdf; P. Huston, , V.L. Edge, and E. Bernier, "Reaping The Benefits Of Open Data In Public Health," Canada Communicable Disease Report (Oct. 2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6781855/. 45(11):252-256. doi: 10.14745/ccdr.v45i10a01. PMID: 31647060; PMCID: PMC6781855. Examples

[171] *See, ex.,* "Managing, responding, and fulfilling data subject access requests (DSARs)," TerraTrue (Jun. 2, 2022), https://terratruehq.com/privacy/managing-responding-handling-data-subject-access-requests-dsars/ (noting that, "[w]ith the advent of important new privacy laws around the U.S. and across the globe…people have been empowered with new rights to the ownership and management of their personal data. Organizations worldwide are developing processes for managing the way people can access these rights… [h]owever, many of these new legal requirements can be confusing and are so new that best practices are still developing. Even the words we use to describe these rights can differ from organization to organization, state to state, country to country.").

a drivers' license or passport), or simply refusing to give access, given the risk of data exfiltration to the wrong person, such as an investigator or abusive partner.[172]

Other individual controls, such as deletion and consent management requests, while not raising concerns over data exfiltration, may prove equally difficult to implement in practice. For example, a strict requirement to obtain consent for future uses of such data will often prove impossible to effectuate for a company solely processing device identifiers, because there will be no practical means of contacting the person to whom the data relates.[173] In some cases, this may be the desired outcome – for example if the future uses are considered wholly incompatible with the original reasons for collecting the data or otherwise "unfair."[174]

As a result, substantive controls that go beyond individual self-management are particularly important for this type of data due to the challenges inherent in providing traditional mechanisms of access and control. For example, when less readily identifiable, non-sensitive data is shared and used for personalization, targeting, or profiling, a fairness standard could require a variety of substantive controls, such as:

- limiting secondary uses of data that are incompatible with the original purpose of the data collection, such as behavioral profiling that creates harm or goes beyond marketing uses (see below, Part IV, Subpart B);

---

[172] *See, ex.,* "What should we consider when responding to a request?," UK Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/what-should-we-consider-when-responding-to-a-request/#ID (last visited: Nov. 15, 2022) (noting that, when responding to a data subject access request under the GDPR, "[t]he level of [identity] checks you make may depend on the possible harm and distress that inappropriate disclosure of the information could cause to the individual concerned."); Piotr Foitzik, "How to verify identity of data subjects for DSARs under the GDPR," International Association of Privacy Professionals (Jun. 26, 2018), https://iapp.org/news/a/how-to-verify-identity-of-data-subjects-for-dsars-under-the-gdpr/ (underscoring that, "[t]he more sensitive the data, the more effort to authenticate is expected. This is in accordance with the risk-based approach, and you can justify asking for more information or more critical or sensitive information if you do this to protect the data subjects against possible risks to their rights and freedoms."); Mariano Di Martino, Pieter Robyns, Winnie Weyts, Peter Quax, Wim Lamotte, and Ken Andries, "Personal Information Leakage by Abusing the GDPR 'Right of Access'," Fourteenth Symposium on Usable Privacy and Security, USENIX Association (Aug. 2019) (demonstrating that publicly available information can be used to impersonate data subjects and request their sensitive personal information).

[173] *See, ex., "*Comment 0000000041," Colorado Privacy Act Written Comments (Apr. 14, 2022), https://comments.coag.gov/s/comment/a0kt0000001zxTOAAY/comment-0000000041 (describing some companies' difficulties complying with deletion requests because their data comes from third party sources).

[174] *See* Adam J. Andreotta, Nin Kirkham, and Marco Rizzi, "AI, Big Data, And The Future Of Consent," AI & Society (Aug. 2021) at 1720, https://doi.org/10.1007/s00146-021-01262-5.
"Can We Use Data For Another Purpose?" The European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en#examples (last visited: Nov. 16, 2022).

- requiring the adoption of processing agreements or other accountability measures that can ensure accountability when data is shared;
- requiring that companies provide individuals with an effective method of objecting to collection and use, for example through standardized tools, such as the deployment of decentralized opt-out signals;
- requiring industry-wide retention limits for particular purposes;
- requiring that companies conduct internal audits to identify potential discrimination or disparate impact of collection or uses for vulnerable or marginalized communities;

The Commission should also recognize that efforts to create methods of reporting and tailoring advertising that rely on privacy enhancing technologies are rapidly developing and could address many of the concerns about today's advertising markets, if advanced in ways that also ensure competition in this market.

B. Incompatible Secondary Uses

The Commission should adopt a principle of distinguishing between "compatible" and "incompatible" secondary uses of personal data as a framework to differentiate between secondary uses that are economically or socially beneficial from those that are harmful or create unnecessary risks without countervailing benefits. We propose the concept of "compatibility" because it is well-established in both privacy scholarship and global data protection law, and has benefits for market regulation that go beyond more limited frameworks relying on consumer expectations.

As a threshold matter, it is clear that the Commission should adopt some standard for identifying unlawful secondary uses of data in its rulemaking, in order to meet its goals of addressing the harms discussed in the ANPRM while providing clarity for regulated businesses. The concept of "commercial surveillance" – described for decades in privacy scholarship as "panoptic" or "corporate surveillance"[175] and "public surveillance"[176] – cannot be addressed without a standard distinguishing between fair and unfair secondary uses of data.

It would be overbroad to consider all secondary uses of data – i.e. uses that are necessary to providing a service requested by a consumer – as "unfair" and prohibit them as a matter of law.[177] This approach would significantly limit many clearly beneficial data uses that are strictly speaking "secondary," including: commercial research and development; detection of fraud or other

[175] *See* "The Panoptic Sort: Surveillance Q&A with Oscar Gandy," University of Pennsylvania Annenberg School for Communication (July 7, 2021), https://www.asc.upenn.edu/news-events/news/panoptic-sort-surveillance-qa-oscar-gandy.
[176] Helen Nissenbaum, "Privacy as Contextual Integrity," 79 Wash. L. Rev. 119 (2004).
[177] "How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking," Consumer Reports and Epic (Jan. 6, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

harmful or illegal activities; assisting with public safety or public health efforts; studying the impact of platforms and technology on society; developing real world evidence-based medicine; developing and studying artificial intelligence and machine learning models; and even addressing bias and discrimination.

Significantly, the Commission also faces challenging policy decisions about the extent to which secondary uses of personal data for advertising and marketing should play a role in supporting modern publishers and enabling competition. Supporting advertising, including data driven advertising because of its role in providing consumers with information about choices in the marketplace and new entrants, while preventing deception or unfairness has long been central to the FTC's mission. At the same time, an approach that permits all secondary uses so long as a company discloses them with accurate disclosures would fall very short. The fundamental right to private life is not only deeply rooted in our history and legal tradition, but forms an essential part of how individuals can engage fairly and on equal terms in the marketplace.[178]

Benefits of Compatibility

The notion of "compatibility" has emerged from decades of leading privacy scholarship, and is now well-established in global data protection law. Its primary benefit, as an element of overall "fairness" in data processing, is the ability to balance competing interests and directly weigh the benefits of data processing against its potential for harm and invasions of privacy. In this balancing test, the individual's consent is an important but not dispositive factor.

In the United States, many decades of legal scholarship have explored this concept, often but not always framed around individual and societal expectations. For example, leading scholar Helen Nissenbaum has introduced a related concept of "contextual integrity." According to Nissenbaum, the appropriate treatment of personal data should depend on social context, such that "information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it."[179]

Globally, the legal standard for "compatible" secondary uses is well-established in the European General Data Protection Regulation and global laws.[180] In addition to helping U.S. companies benefit from regulatory clarity and consistency, this means that there is a considerable body of guidance and case law available to evaluate the effectiveness of the approach.

---

[178] Ryan Calo, "Privacy and Markets: A Love Story," 91 Notre Dame L. Rev. 2 (2016) (laying out a "framework [which] understands privacy as a crucial ingredient of the market mechanism, while simultaneously demonstrating how markets enable privacy to achieve its most important functions.").
[179] Nissenbaum, "Privacy as Contextual Integrity," at 119.
[180] Information Commissioner's Office (ICO), *Principle (b): Purpose limitation*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (last visited: Nov. 18, 2022).

For example, there is a legal presumption under the GDPR that pseudonymized data may be lawfully processed for secondary scientific research purposes. Such processing does not require individual consent, a measure that can often introduce bias or otherwise affect the quality of the dataset.[181] Under the GDPR, pseudonymized data is still personal data, and has been processed "in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual."[182] In cases involving scientific research, there has been a clear policy decision that the benefits of such processing outweigh the potential for harm so long as the data is protected by technical, legal, and administrative safeguards.

In other cases, the balancing of compatible and incompatible secondary uses may be more challenging.[183] The European Commission has issued guidance to regulated businesses asking "Can we use data for another purpose?" and offers the following factors:

- the link between the original purpose and the new/upcoming purpose;
- the context in which the data was collected (what is the relationship between your company/organisation and the individual?);
- the type and nature of the data (is it sensitive?);
- the possible consequences of the intended further processing (how will it impact the individual?);
- the existence of appropriate safeguards (such as encryption or pseudonymisation).

Going Beyond Consent and Consumer Expectation

In many cases, it will be appropriate for a compatibility or similar analysis to take into account consumers' reasonable expectations, particularly when utilizing the Commission's deception authority. For example, a modern consumer might reasonably expect that when she provides an email address to receive a digital receipt or shipping updates from an online retailer at check-out, that the email address will only be used for that purpose. Additional purposes (for example, to add the email address to the company's list-serv for marketing) should typically require an additional disclosure and request for consent.

However, a standard resting solely on "consumer expectations" would be effective only in these kinds of market interactions, where there is a first-party relationship and some form of consumer

[181] Khaled El Emam and Mike Hintze, "Does anonymization or de-identification require consent under the GDPR?," International Association of Privacy Professionals (Jan. 29, 2019), https://iapp.org/news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/ (noting that, "there is compelling evidence that obtaining consent can result in bias, which, in certain circumstances, can affect the outcome of the analysis.").
[182] General Data Protection Regulation (GDPR), Art. 4(3b)
[183] For example, the current debates around medical research that are ongoing in the EU. See "The General Data Protection Regulation1: Secondary Use of Data for Medicines and Public Health Purposes," European Medicines Agency (2020), https://www.encepp.eu/events/documents/Discussionpaper.pdf.

market transaction occurring for which an average consumer can reasonably make a well-informed decision. In many situations, asking a consumer to have informed expectations or preferences with respect to online advertising, data brokerage, and emerging technologies, is impossible or impractical, given the frequent lack of first-party relationships and deep asymmetries in information. For example, the experience of being asked to consent to cookie banners due to the ePrivacy Directive has been widely considered ineffective insofar as most individuals lack the time, resources, and knowledge to adequately assess hundreds of varying advertising and other use cases for cookies, leading to exhaustion, "consent fatigue," and general ambivalence.[184] Similarly, a consumer may not contemplate fraud related uses when transacting with a business, let alone the sharing of this data for fraud uses across multiple businesses, yet such uses may be compatible due to the necessity of such use to the integrity of that market.

Finally, a compatibility standard would better protect consumers from harms related to novel or emerging technology. For example, the Commission has expressed that consumers have reasonable expectations around the use of televisions – specifically, that TV watching behavior should not be tracked and shared identifiably with third parties without adequate choice.[185] This expectation may be reasonable for a device that has been common in most American households for many decades, pre-dating the Internet age. But what is a reasonable consumer expectation for a novel piece of consumer technology, such as a voice-assisted smart speaker, Ring doorbell, or delivery robot? Many of our intuitions and expectations around such devices are fundamentally unsettled, with extreme variances across demographics and age groups.[186]

In all, a stronger legal and normative approach would be to adopt a distinguishing principle of "compatibility" that would take into account the full considerations of the FTC's fairness authority, by carefully weighing and balancing competing interests, including benefits to consumers and competition, against countervailing harms and invasions of privacy.

---

[184] *See, ex.,* Hana Habib, Megan Li, Ellie Young, and Lorrie Faith Cranor, "'Okay, whatever': An Evaluation of Cookie Consent Interfaces," Carnegie Mellon University (May 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/PrivacyCon-2022-Habib-Li-Young-Cranor-Okay-whatever-An-Evaluation-of-Cookie-Consent-Interfaces.pdf; Oksana Kulyk, Nina Gerber, Annika Hilt, and Melanie Volkamer, "Has The Gdpr Hype Affected Users' Reaction To Cookie Disclaimers?," 6 Journal of Cybersecurity 1 (Dec. 24, 2020), https://doi.org/10.1093/cybsec/tyaa022.

[185] *F.T.C. vs. Vizio, Inc.*, No. 162 3024 (Feb. 3, 2017) (complaint) (characterizing Vizio's failure to disclose that its "Smart Interconnectivity" feature tracked consumer viewing behavior as deceptive).

[186] Omer Tene and Jules Polonetsky, "A Theory of Creepy: Technology, Privacy and Shifting Social Norms," 16 Yale Tech. L. J. 59 (Sept. 16, 2013); Nathaniel Fruchter and Ilaria Liccardi, "Consumer Attitudes Towards Privacy and Security in Home Assistants," Association for Computing Machinery (Apr. 20, 2018), https://dl.acm.org/doi/10.1145/3170427.3188448; Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," PEW Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

C. Heightened Protections for Sensitive Data That Impacts Youth and Marginalized Communities

Harmful data processing activities can have a disproportionate impact on youth and marginalized communities. FTC rules should account for uniquely sensitive data that impacts specific vulnerable populations. In particular, the Commission may consider heightened protections for data implicating these groups and stronger accountability for misuses of this kind of data.[187]

Children and teenagers require additional data privacy protections as uniquely important groups. The Commission has a long history of privacy and security precedent to protect children,[188] stating that children are a "special, vulnerable group" as they "lack the analytical abilities and judgment of adults."[189] Commission enforcement actions on matters concerning children often focus on the risk of child predation as the preeminent harm arising from unfair or deceptive data processing practices. However young people's privacy also matters "to enable other values," including "the ability to grow, develop, experiment, test new ideas, try on new identities, and learn, while being free from the chilling effects of being watched or having information from their childhood used against them later when they apply to college or apply for their first job."[190] Though the Children's Online Privacy Protection Act (COPPA) does not apply to individuals over 12 years old,[191] the data privacy values and risks faced by children do not cease once they become teens. In fact, teens arguably face different and heightened risks, such as a normalized

---

[187] Forms of heightened accountability include heightened penalties, algorithmic disgorgement and executive responsibility. The Commission should make clear that the ramifications of violating the rule could include harsh penalties, such as the algorithmic disgorgement that the agency recently imposed on Kurbo. *United States v. Kurbo Inc. & WW International, Inc*., No. 22-CV-946 (N.D. Ca. March 2022) (consent decree).

[188] *See, e.g., FTC v. R.F. Keppel & Bro*., Inc., 291 U.S. 304 (1934); *In the Matter of GeoCities,* 127 F.T.C. 94 (Feb. 5, 1999); *In the Matter of Apple, Inc.*, No. C-4444 (March 2014); *FTC and the People of New York v. Google, LLC and Youtube, LLC*, No. 1:19-cv-02642 (D.D.C. Sept. 2019); *United States v. Kurbo Inc. and WW International, Inc.*, 22-CV-946No. 3:22-cv-00946-TSH (N.D. Ca. Mar. 2022).

[189] "Privacy Online: A Report to Congress," FTC (1998) at 12, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[190] Stacey Gray (FPF), "Testimony at the FTC Commercial Surveillance and Data Security Public Forum," FTC (Sept. 8, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/CommercialSurveillanceandDataSecurityRulemakingTranscript09.08.2022.pdf.

[191] Early drafts of COPPA defined children as anyone under the age of sixteen. *See* Taylor Callery, "How 13 Became the Internet's Age of Adulthood," The Wall Street Journal (Jun. 18, 2019), https://www.wsj.com/articles/how-13-became-the-internets-age-of-adulthood-11560850201. However, due to ramifications of requiring parental consent, the final text limited the protections to individuals under 13 years old. More regulatory regimes are moving towards extending some youth privacy protections to teens, such as the Age-Appropriate Design Code. *See* "Introduction to the Age Appropriate Design Code," UK Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/ (last visited: Nov. 10, 2022) *and* The California Age-Appropriate Design Code Act, AB 2273 *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273.

lack of privacy, body image and mental health issues, and creating a larger digital footprint than intended.[192] At the same time, teens stand to derive greater benefits from online services, including: services that help teens learn, socialize with peers, distant family, and communities, and access resources like health information and remote counseling. The Commission's rulemaking should consider the heightened risks and benefits that can accrue to teens in the context of data-driven services. In doing so, it is critical to be aware of the substantial overlap between services used by older teens and adults, and the impact on the privacy of all users if general sites are obligated to authenticate or verify teen users.[193]

Similarly, unfair or deceptive data processing activities that target marginalized communities or implicate data regarding an individuals' protected class status (including race, ethnicity, sexual orientation, disability, and related categories) must be considered in a trade regulation rule. As highlighted throughout this Comment, many of the risks detailed in the Commission's ANPR can impact marginalized communities in unique or heightened ways. Such risks can include: algorithmic discrimination,[194] manipulative design patterns,[195] hiring discrimination,[196] housing discrimination,[197] employment discrimination,[198] credit and lending discrimination,[199] discrimination

[192] "A Roadmap for Considering Teen Privacy & Safety," The Center for Industry Self-Regulation (Apr. 2022), https://industryselfregulation.org/docs/librariesprovider5/default-document-library/tapp_roadmap.pdf.
[193] For example, experts have opined that online businesses may need to begin using biometric face scans in order to authenticate the age of users after California's Age-Appropriate Design Code was recently passed. *See, e.g.*, Vallari Sanzgiri, "Businesses To Brace Themselves For California's Age-Appropriate Design Code," MediaNama (Oct. 12, 2022), https://www.medianama.com/2022/10/223-summary-california-age-appropriate-design-code/.
[194] Nicol Turner Lee, Paul Resnick, Genie Barton, "Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms," Brookings (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.
[195] Staff Report, "Bringing Dark Patterns to Light," FTC (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.
[196] Anja Lambrecht & Catherine Tucker, "Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads," SSRN (Oct. 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260.
[197] Eva Rosen, Philip M.E. Garboden, and Jennifer E. Cossyleon, "Racial Discrimiantion in Housing: How Landlords Use Algorithms and Home Visits to Screen Tenants," 86 American Sociological Association 5 (Aug. 20, 2021), https://journals.sagepub.com/doi/10.1177/00031224211029618.
[198] Alex Engler, "For Some Employment Algorithms, Disability Discrimination by Default," Brookings (Oct. 31, 2019), https://www.brookings.edu/blog/techtank/2019/10/31/for-some-employment-algorithms-disability-discrimination-by-default/.
[199] Robert Bartlett, Adair Morse, Richard Stanton, & Nancy Wallace, "Consumer-Lending Discrimination in the Fin Tech Era," Hass School of Business at U.C. Berkeley (Nov. 2019), http://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf.

in education,[200] healthcare,[201] and even the targeting of communities by nation states.[202] Nonetheless, the interplay between technology and marginalized communities is complex and nuanced. Technologies that treat individuals and communities differently can offer benefits to individuals and the market. For example, online services can help promote affirmative action programs to diverse individuals, display more representative content in advertisements and recommendations when serving diverse communities, and uncover otherwise hidden bias in automated decisions. Further, human decision-making is not without bias, and algorithmic decisions can potentially deliver less biased outcomes.[203] The Commission's rulemaking should consider the heightened risks and benefits that can accrue to marginalized communities in the context of data-driven services.

V. Conclusion

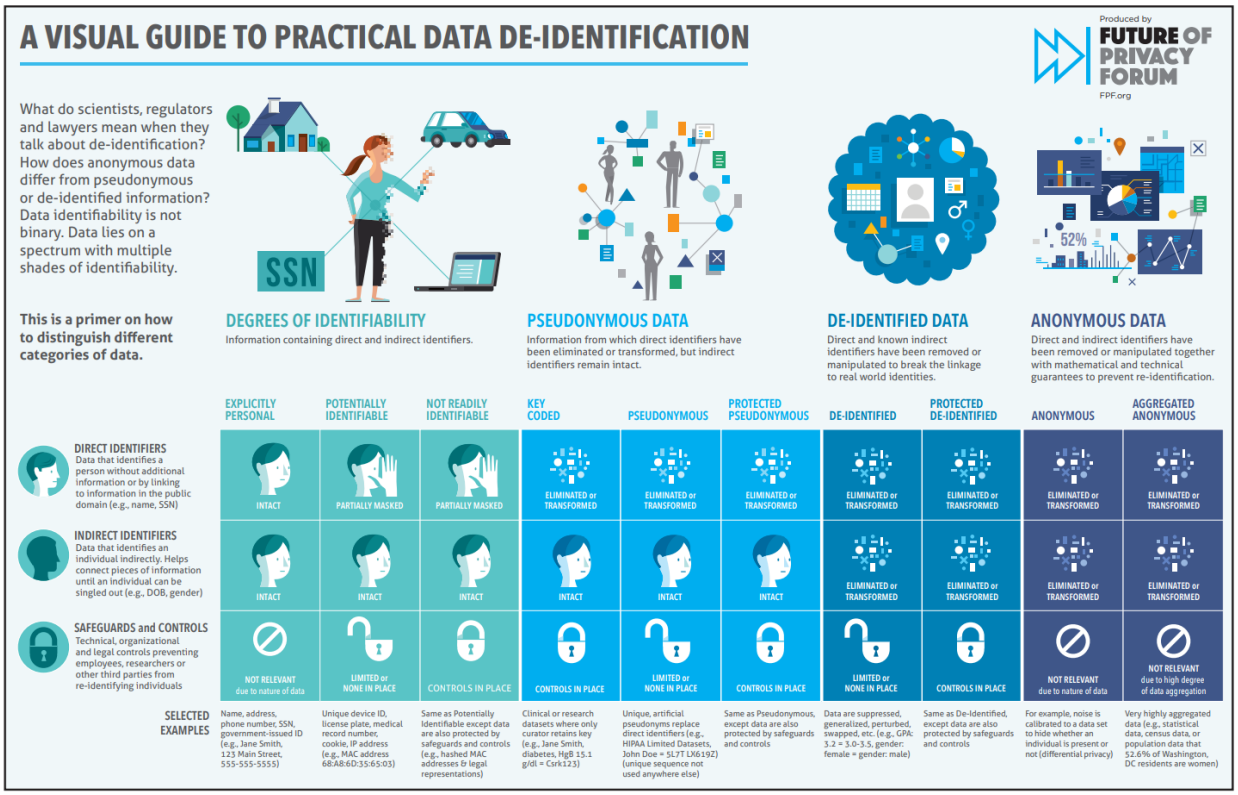
The Future of Privacy Forum appreciates this opportunity to comment on these issues and the Federal Trade Commission's efforts to provide individuals with strong, enforceable rights and companies with greater clarity about their obligations under Section 5 of the FTC Act.

We welcome any further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact Tatiana Rice at trice@fpf.org (cc: info@fpf.org).

Sincerely,
The Future of Privacy Forum
https://fpf.org/

[200] Rashida Richardson & Marci Lerner Miller, "The Higher Education Industry Is Embracing Predatory and Discriminatory Student Data Practices," Slate (Jan. 13, 2021), https://slate.com/technology/2021/01/higher-education-algorithms-student-data-discrimination.html.
[201] Karessa Weir, "Artificial Intelligence in Medicine May Increase Exclusion," Michigan State University (Oct. 18, 2022), https://polisci.msu.edu/news-events/news/bracic-ai.html.
[202] Select Committee on Intelligence United States Senate, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views," U.S. Senate (Nov. 10, 2020), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.
[203] Bo Cowgill, "Bias and Productivity in Humans and Machines," Upjohn Institute Working Paper (Aug. 2019), https://dx.doi.org/10.2139/ssrn.3433737.

Appendix A



https://fpf.org/blog/a-visual-guide-to-practical-data-de-identification/