Comments of New America's Open Technology Institute and the Electronic Privacy Information Center to the

Federal Trade Commission

On Consumer Injuries and Benefits in the Data-Driven Economy

February 26, 2026

New America's Open Technology Institute (OTI)[1] and the Electronic Privacy Information Center (EPIC)[2] submit these comments in response to the Federal Trade Commission (FTC)'s invitation for written submissions[3] to the Consumer Injuries and Benefits in the Data-Driven Economy Workshop.[4]

This workshop presents an important opportunity to take a more comprehensive view of consumer harm in the data-driven economy. EPIC and OTI have explored through litigation, research, and policy work how a more capacious approach to privacy could better capture the full spectrum of injuries associated with modern data practices. Privacy harms are both qualitative[5] and quantitative:[6] they implicate autonomy, dignity, and civil rights,[7] while also producing real economic externalities that are rarely measured.[8]

---

[1] New America's Open Technology Institute, *About*, https://www.newamerica.org/oti/about/.

[2] *About Us,* EPIC (2026), https://epic.org/about/.

[3] Federal Trade Commission, *Consumer Injuries and Benefits in the Data-Driven Economy* (Feb. 26, 2026), https://www.ftc.gov/news-events/events/2026/02/consumer-injuries-benefits-data-driven-economy. ("The Commission will consider all timely and responsive public comments, whether filed in paper or electronic form[.]").

[4] *Id.*

[5] *Updated EPIC Resources Highlight Data Broker Harms to Different Communities,* EPIC (Dec. 4, 2025), https://epic.org/updated-epic-resources-highlight-data-broker-harms-to-different-communities/; *Report: Privacy Harms from AI Necessitate Robust Risk Assessments*, EPIC (June 25, 2025), https://epic.org/press-release-report-privacy-harms-from-ai-necessitate-robust-risk-assessments/.

[6] Sydney Saubestre, *What's the Value of Privacy?*, New America's Open Technology Institute (Apr. 2021), https://www.newamerica.org/oti/briefs/whats-the-value-of-privacy/.

[7] Daniel J. Solove & Danielle Keats Citron, Privacy Harms, 102 B.U. L. Rev. 793 (2022), https://scholarship.law.gwu.edu/faculty_publications/1534/.

[8] Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 54 J. Econ. Literature 442, 444–47, 463–65 (2016), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf.

A central reason these harms are undervalued is that prevailing judicial, statutory, and regulatory frameworks tend to assess data-related injury too narrowly. Harms are frequently understood only in terms of immediate financial loss, overt deception, or risks consumers could reasonably avoid. But modern data practices frequently produce consequences that are diffuse, delayed, or structural[9]—such as loss of control over personal information, discrimination, reputational harms, or chilling effects on speech[10]—and not captured in this limited conception.[11]

The Commission's efforts to quantify and fully understand the costs and benefits of data practices should turn on consequences (including consequences distributed across society)[12] rather than remain confined to a narrow focus on labels or data categories. The relevant inquiry is whether business practices involving personal information create foreseeable risks of injury, distort consumer choice, or undermine legally protected interests. By broadening the scope of recognized harms, the FTC can better align enforcement with the realities of modern data-driven markets, where many injuries are incremental, probabilistic, and distributed across time and populations.

The FTC has recognized in recent enforcement actions that collecting and sharing certain types of data—such as granular location information—can create serious risks of harm, including in *FTC. v Kochava, Inc.*[13] That recognition reflects an important doctrinal evolution: injury may arise not only from realized misuses, but from practices that create significant and foreseeable risks.

Operationalizing these lessons about the quantitative dimensions of privacy harms will also require the FTC revisit its qualitative and legal understanding of what counts as an injury. Even as the *Kochava* case provides grounds for optimism, the Commission has too often held to an arbitrary conception of "substantial injury" and harm that is both in tension with the FTC Act and ineffective at protecting consumers in the digital era. The Commission should take the occasion of this workshop to move beyond its outdated focus on immediate pecuniary harm to acknowledge the broader spectrum of injuries that extractive data practices inflict.

---

[9]Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013), https://harvardlawreview.org/wp-content/uploads/2013/05/vol126_richards.pdf.

[10] Penney, Jonathon W., *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech. L.J. 117 (2016), https://doi.org/10.15779/Z38SS13.

[11] Ryan Calo, *Privacy Harm Exceptionalism*, 12 Colo. Tech. L.J. 361 (2014), https://ctlj.colorado.edu/wp-content/uploads/2014/11/Calo-website-final.pdf.

[12] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford Univ. Press 2019).

[13] Complaint, *Federal Trade Commission v. Kochava Inc.*, No. 2:22-cv-00377 (D. Idaho filed Aug. 29, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/86-SecondAmendedComplaint.pdf.

I. Quantitative valuation of privacy harms

From a quantitative perspective, privacy is economically significant even when it is routinely undervalued.[14][15] It shapes consumer trust, autonomy, and meaningful participation in economic and civic life. Individuals devote time, attention, and resources to managing data exposure, mitigating risk, and responding to misuse, reflecting real economic costs. Yet prevailing market practices and measurement tools treat privacy as if it were a marginal consumer taste rather than a foundational component of consumer welfare.[16] Firms, meanwhile, derive substantial value[17] from personal data through targeting, profiling, optimization, and risk scoring, translating granular information into revenue.[18] Despite this value exchange, privacy losses are rarely acknowledged in a measurable form beyond the relatively narrow context of assessing penalties and recovering ill-gotten gains when companies engage in unlawful business practices or a breach has occurred. ***When costs are diffuse, delayed, or difficult to quantify, they are often treated as negligible, producing an implicit assumption that privacy loss carries little economic weight.***

Market outcomes do not reflect the true value of privacy because the conditions necessary for efficient choice are absent. Individuals make disclosure decisions in environments defined by asymmetric information, opaque data flows, and downstream uses that are neither visible nor reasonably foreseeable.[19] Consumers cannot reliably forecast how data will be aggregated, inferred from, retained, or shared across entities and contexts, nor can they evaluate the probability, magnitude, or timing of future harms.[20] In this setting, observed behavior cannot be interpreted as evidence that privacy losses are costless or that individuals knowingly accept the risks associated with pervasive data collection.

---

[14] Acquisti, Taylor, & Wagman, *supra* note 8.

[15] Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. Legal Stud. 249 (2013).

[16] Benjamin E. Hermalin & Michael L. Katz, *Privacy, Property Rights and Efficiency: The Economics of Privacy as Secrecy*, 4 Quantitative Marketing & Economics 209 (2006), https://ideas.repec.org/a/kap/qmktec/v4y2006i3p209-239.html.

[17] Acquisti, Taylor, & Wagman, *supra* note 8.

[18] Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Online Advertising*, in Innovation Policy and the Economy 65 (Nat'l Bureau of Econ. Research 2011), https://www.nber.org/system/files/chapters/c14781/c14781.pdf

[19] Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, *Columbia Law and Economics Working Paper* No. 639 (Aug. 21, 2019), https://academiccommons.columbia.edu/doi/10.7916/d8-g10s-ka92.

[20] Alessandro Acquisti, Laura Brandimarte, & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 Science 509 (2015).

Structural constraints further depress the effective value of privacy. Participation in digital markets increasingly requires surrendering personal data as a condition of access to essential services, employment platforms, financial tools, education resources, and social communication. Privacy-protective alternatives, when they exist, often require additional payment, reduced functionality, or exclusion from dominant networks. Consumers therefore face a constrained choice set in which retaining privacy entails tangible losses, while disclosing information becomes the default path to participation.

From an economic perspective, privacy loss generates negative externalities that markets do not internalize. Firms capture the benefits associated with data collection, profiling, and monetization, while the risks and burdens of misuse, exposure, and loss of control are borne by individuals and society. These burdens include vulnerability to fraud and identity theft, time and resource costs associated with monitoring and remediation, unwanted intrusion, and erosion of trust necessary for healthy digital participation. At a societal level, diminished privacy can chill lawful expression, deter exploration and association, and weaken confidence in institutions.[21] These risks are not only cumulative over time and across contexts, but they also propagate through data externalities, where information provided by one consumer can reveal information about others, amplifying harm across populations.[22] Because these costs are dispersed and probabilistic, they rarely appear in prices or consumer decision-making.

Behavioral dynamics compound this undervaluation. Privacy decisions are frequently made under conditions of cognitive overload and interface designs[23] that favor swiftly approving—not meaningfully consenting—to information sharing.[24] Default settings, bundled consent, and layered policies obscure meaningful consequences. Individuals are asked to make complex tradeoffs repeatedly and in real time, even when potential

---

[21] A rich tradition of scholarship and judicial decisions support this point. *See, e.g.,United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."); *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958), https://www.law.cornell.edu/supremecourt/text/357/449 ("This Court has recognized the vital relationship between freedom to associate and privacy in one's associations.")

[22] Shota Ichihashi, Data Externalities and Information Design, Queen's University, Dec. 15, 2020, https://academiccommons.columbia.edu/doi/10.7916/d8-g10s-ka92.

[23] Federal Trade Commission, *FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick or Trap Consumers* (Sept. 7, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers.

[24] Geoffrey A. Fowler, *I Tried to Read All My App Policies. It Was 1 Million Words*, Wash. Post (May 31, 2022), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/; Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & Pol'y Info. Soc'y 543 (2008), https://kb.osu.edu/server/api/core/bitstreams/a9510be5-b51e-526d-aea3-8e9636bc00cd/content.

privacy implications are not clearly visible or explained to them.[25] These dynamics systematically bias outcomes toward data disclosure and should not be read as evidence of informed, welfare-maximizing choice.

Privacy harms are often incremental and dispersed, making them difficult to perceive in isolation. Individual disclosures may appear trivial, but repeated collection, aggregation, inference, and secondary use can create substantial risks, including loss of control, persistent tracking, unwanted exposure, and heightened vulnerability to manipulation or fraud. When these effects are evaluated atomistically, their significance remains obscured; when aggregated across time, populations, and downstream uses, their economic and social costs become visible. Developing frameworks for quantitative valuation of data use have a critical role to play in enabling this kind of aggregated assessment.

Judicious use of data can confer societal benefits like improved service delivery or innovation, particularly when paired with robust safeguards that are legally and/or technically enforceable. The presence of benefits, however, does not negate structural injury when privacy costs are obscured or displaced. Nor do they fully account for the many positive externalities associated with privacy, including innovation, for both individuals and firms.[26] When privacy externalities are not systematically surfaced, they are effectively assigned negligible weight in comparative analysis, skewing welfare assessments toward measurable short-term gains while obscuring distributed and long-term burdens.

Recognizing the structural undervaluation of privacy requires understanding that personal data is not always harmful in isolation but may create harm or risk through its use, combination, and deployment. Market structure, information asymmetries, behavioral constraints, and analytic inferences all shape risk, meaning privacy harms often emerge from context rather than a single act of disclosure. Understanding these dynamics is critical to accurately assessing consumer welfare and the full scope of injury when privacy is treated as costless.

II. Capturing the full spectrum of privacy harms

To account for the full scope of privacy and privacy-related injuries that businesses can inflict on consumers through unlawful business practices, the FTC must revamp not only its quantitative framework for valuing privacy losses but also its qualitative framework for understanding the types and character of those harms. Too often the Commission

[25] Acquisti, Brandimarte & Loewenstein, *supra* note 20.

[26] *See, e.g.,* Julie E. Cohen*, What Privacy Is For*, 126 Harv. L. Rev. 1904, 1919-1927 (2013), https://scholarship.law.georgetown.edu/facpub/2526/ (arguing that privacy is central not just to healthy liberal democracies, but also to societies capable of producing successful and varied innovations).

artificially restricts its understanding of consumer injuries to pecuniary losses and physical harm directly traceable to an offending business practice. Yet the wrongful collection, retention, processing, and disclosure of one's personal information can cause a far wider range of injuries—many of which have been recognized by our common law and constitutional traditions.

One notable example of these artificial restrictions is the term "substantial injury" as construed in the Commission's 1980 Policy Statement on Unfairness.[27] In that Policy Statement, the FTC established a three-part test to determine whether a business practice is "unfair" within the meaning of Section 5 of the FTC Act. The injury (1) must be substantial, (2) must not be outweighed by any countervailing benefits, and (3) must be an injury that the consumer could not have reasonably avoided.[28] The Policy Statement noted that many substantial injury cases involve monetary harms, coercive sales, and unwarranted health and safety risks. But the Commission opined that "trivial," "speculative," and "subjective types of harm" would generally not suffice to make a practice unfair.[29] In this latter category, the FTC listed "emotional impact" and "offend[ing] tastes or social beliefs."[30]

Though Congress later incorporated the Commission's definition of unfairness into the FTC Act in 1993, it did so with a notable exception. Consistent with the Policy Statement, Congress directed that "[i]n determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence."[31] But Congress declined to adopt the FTC's rubric for determining which harms constitute "substantial injury," advisedly leaving that term open to a broader construction than the FTC had given it in the Policy Statement.

With some notable exceptions, the Commission has generally spurned the congressional intent of this provision over the past three decades, hewing to its own narrower understanding of "substantial injury" and giving only occasional weight to established public policies. ***This has contributed to a systematic under-recognition of privacy harms in the Commission's regulatory and enforcement decisionmaking, which in turn has allowed unfair and otherwise harmful data practices to flourish. The result of this—and of related regulatory and legislative failures—is the data protection crisis we now face today.[32]***

---

[27] Federal Trade Commission, *Policy Statement on Unfairness* (1980), *available at* https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness.

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] 15 U.S.C. § 45(n).

[32] *Hearing before the Innovation, Data, and Com. Subcomm. of the H. Comm. on Energy &*

To stem the tide of harmful commercial data practices, the FTC must take full account of the many and varied injuries those practices frequently cause to consumers. These include but are not limited to discrimination and civil rights violations[33] (including the deprivation of equal access to information), loss of control (including the excessive collection and unwanted or unexpected secondary use of one's personal data),[34] emotional distress,[35] intrusion upon seclusion,[36] reputational harms,[37] harms from inadequate data security,[38] psychological harms,[39] thwarted consumer expectations,[40] chilling effects on speech,[41] autonomy harms,[42] the destruction of anonymity,[43] and the breach of a duty of care owed to a consumer.[44]

Taken together with a rigorous valuation of privacy loss, this enhanced understanding of "substantial injury" and harm stands to dramatically strengthen the Commission's regulatory and enforcement efforts and help the FTC to deliver on its statutory obligation to protect consumers.

***

We thank the Commission for organizing this workshop and providing an opportunity to submit written comments. We hope to continue engaging with the FTC on the subject of privacy harms. If you have any questions, please contact Sydney Saubestre (saubestre@newamerica.org) and John Davisson (davisson@epic.org).

Commerce, 119th Cong. (2024) (testimony of John Davisson), https://epic.org/wp-content/uploads/2024/09/EPIC-Testimony-FTC-Sept2024.pdf.

[33] Solove & Citron, *supra* note 7, at 855–59.

[34] EPIC & Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, 5 (Jan. 26, 2022), *available at* https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf; *see also* Calli Schroeder & Cobun Keegan, *Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms*, 15 J. of L., Economics and Policy 17–18 (2018), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4204208.

[35] Solove & Citron, *supra* note 7, at 841–44.

[36] *See*, *e.g.*, Pls.' Opp'n to Defs.' Mot. Dismiss at 3–9, *EPIC v. Office of Personnel Mgmt.*, 25-cv-255 (E.D.V.A. June 17, 2025) ("Improper access to sensitive records is textbook intrusion upon seclusion.").

[37] Solove & Citron, *supra* note 7, at 837–41.

[38] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex. L. Rev. 737 (2018).

[39] Solove & Citron, *supra* note 7, at 841–44.

[40] EPIC & Consumer Reports, *supra* note 34, at 6.

[41] Solove & Citron, *supra* note 7, at 854.

[42] *Id.* at 845–55.

[43] *Anonymity*, EPIC (2026), https://epic.org/issues/democracy-free-speech/anonymity/.

[44] *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1225–30 (2016).

Sincerely,

/s/ Sydney Saubestre
Senior Policy Analyst
New America's Open Technology Institute (OTI)

/s/ John Davisson
Deputy Director
Electronic Privacy Information Center (EPIC)

/s/ Prem Trivedi
Director
New America's Open Technology Institute (OTI)