Before the
National Telecommunications and
Information Agency
Washington, DC 20554

In the Matter of	)	
	)	
Privacy, Equity, and Civil Rights	)	Docket No.
Request for Comment	)	230103-0001
	)	
	)	

COMMENTS OF NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

David Morar
New America's Open Technology
Institute740 15th Street NW
Suite 900
Washington, DC 20005

March 6, 2023

Table of Contents

I. Introduction

New America's Open Technology Institute (OTI) files these comments in response to the National Telecommunications and Information Administration's (NTIA) Request for Comments on Privacy, Equity, and Civil Rights (RFC).[1] The main question of the RFC is about whether "modern data practices and business models" are "adequately addressed by the current U.S. privacy protection framework." As these comments will illustrate, they are not, and there is a need for swift action from all stakeholders, of whom, the United States government remains the most important.

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. OTI has a strong interest in ensuring that algorithmic and artificial intelligence models are fair and equitable, and benefit all communities, especially in the context of privacy rights.

OTI's comments will focus on two general topics on matters across the six major questions, while noting the specific question each paragraph is responsive to. First, under the banner of Harms, we will tackle the identification of the intersection between algorithms and systemic discrimination, with an emphasis on education, employment, and housing discrimination, as well as government use or purchase of data from commercial purposes. Second, under the banner of Action, our comments will respond to company action, as well as legislative action. Company action includes design choices, transparency, and audits. Legislative action highlights the current regime and its enforcement, the importance of public interest principles in crafting comprehensive privacy legislation, and legislative choices.

II. Harms

There is strong evidence that commercial data practices are likely progressively harming the agency and autonomy of those in marginalized communities.[2] Commercial data practices can enable, among other things, voter suppression, digital redlining, discriminatory policing, retail discrimination, digital inequity, the amplification of white supremacy, identity theft, and the endangerment of personal safety.[3] Even more, the use of data in automated decision-making and predictive tools can lead to discrimination against marginalized communities.[4] Data collected on bill payments and credit scores may be used to reject requests for bank loans,[5] which among other ways, leads to socioeconomic harm for specific groups of people who have historically been subject to discrimination. Wireless carriers have been found to sell customer location data

---

[1] 88 FR 3714

[2] See, e.g., Michele Gilman and Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization," *NYU Review of Law and Social Change* 42 (2018): 253-307 https://socialchangenyu.com/review/the-surveillance-gap-the-harms-of-extreme-privacy-and-data-marginalization/.

[3] "Letter to Congress on Civil Rights and Privacy," (Letter from Access Now et al., to the Federal Communications Commission, April 19, 2019) https://newamericadotorg.s3.amazonaws.com/documents/Letter_to_Congress_on_Civil_Rights_and_Privacy_4-19-19.pdf.

[4] See, e.g., Miranda Bogen and Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias,* (Washington, DC: Upturn, December 2018) https://www.upturn.org/reports/2018/hiring-algorithms/.

[5] Mikella Hurley and Julius Adebayo. "Credit Scoring in the Era of Big Data," *Yale Journal of Law and Technology* (2017). Vol. 18 (1), Article 5 https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1122&.

to third parties without requiring proof of lawful orders or customer consent.[6] While sensitive data are rightfully considered deserving of privacy protection generally, non-sensitive data may end up serving as proxies of protected classes in automated decision-making.[7]

A. Consumer Data Collection

Uses of data-intensive processes, such as AI and big data, have seen an upward trajectory across all sectors. In 2022: 91.7% of Fortune 1000 companies reported that they are increasing their investments in AI and data.[8] Vast amounts of personal data is used to train algorithms and to create outputs from those algorithms. With little transparency or accountability, both kinds of data use creates privacy and equity issues. Algorithmic systems can harm individual privacy through data collection in two ways: 1) in building the system, and 2) in using it afterwards since the outputs are created from the underlying data, coded instructions, and inferences by the algorithm itself. Unintended discrimination against specific groups is likely to occur as algorithms can reinforce the training data that may reflect historical biases.[9]

1. Education

The educational context is one where algorithmic decision-making can select what resources students receive and which curriculum to study. Educational data mining (EDM) technologies are now used in the process of ability grouping, dividing students into different groups based on their academic ability.[10] While EDM technologies can have positive influence on the education system,[11] the use of historical data in training data sets can reinforce patterns of discrimination along racial, gender and socioeconomic status.[12] (2c, 3a)

---

[6] Georgetown Law Center on Privacy & Technology, New America's Open Technology Institute, and Free Press, Informal Complaint against AT&T Corporation, T-Mobile U.S., Sprint Corporation, Verizon Wireless for Unauthorized Disclosure and Sale of Customer Location Information, Before the Federal Communications Commission, June 14, 2019 https://newamericadotorg.s3.amazonaws.com/documents/Informal_Complaint_re_Unauthorized_Disclosure.pdf.

[7] See, e.g., Samuel Yeom, Anupam Datta & Matt Fredrikson, Hunting for Discriminatory Proxies in Linear Regression Models, Proceedings of the 32nd Conference on Neural Information Processing Systems (2018), https://www.cs.cmu.edu/~mfredrik/papers/Yeom18-nips.pdf (finding that many variables combined in a predictive policing model together acted as a strong proxy for race but that no individual variable was a particularly strong proxy for race, thus concluding that "in practice multiple variables combine to result in a stronger proxy than any of the individual variables"); David Skanderson & Dubravka Ritter, Payment Cards Center Discussion Paper, Fair Lending Analysis of Credit Cards 28, https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussi on-papers/2014/D-2014-Fair-Lending.pdf.

[8] "Data and AI Leadership Executive Survey 2022" NewVantage Partners LLC (2022) https://www.newvantage.com/_files/ugd/e5361a_bc4200d11bfb42478c782ad863e983eb.pdf.

[9] See e.g., Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan, Cass R Sunstein, "Discrimination in the Age of Algorithms," *Journal of Legal Analysis*, 10, (April 2019), https://doi.org/10.1093/jla/laz001.

[10] Yoni Har Carmel, Tammy Harel Ben-Shahar, "Reshaping Ability Grouping Through Big Data, " Vanderbilt Journal of Entertainment & Technology Law, (May 2017) https://ssrn.com/abstract=2944743.

[11] Lindsey C. Page, Hunter Gehlbach, "How an Artificially Intelligent Virtual Assistant Helps Students Navigate the Road to College," AERA Open, December 12, 2017 https://journals.sagepub.com/doi/10.1177/2332858417749220#articleCitationDownloadContainer.

[12] Closing the Home Learning and Homework Gap: Innovative School and Community Wi-Fi Initiatives, New America's Open Technology Institute, June 25, 2020 https://www.newamerica.org/oti/events/closing-home-learning-and-homework-gap/.

2. Employment

Employment is another area where machine learning algorithms are used in order to make decisions. Without proper testing and assessment tools, algorithms can perpetuate historical biases and negatively affect certain minority groups in direct hiring processes. The use of online job ads can add another layer of potential discrimination, based on protected characteristics, such as gender and race.[13] Even when the tools are not designed to consider gender, or other sensitive categories, historical data use in training may lead to unintended outcomes related to employment.[14] (2c, 3a)

3. Housing

As OTI has noted in its response to the U.S. Department of Housing and Urban Development (HUD) notice of proposed rulemaking[15] on disparate impact standards, there is a clear understanding that algorithmic data practices in housing can lead to problematic and harmful results even if the models themselves don't take into consideration protected characteristics, or are objective and neutral.

> "Algorithms are being used to make decisions that impact the availability and cost of housing. These decisions include screening rental applicants, underwriting mortgages, determining the cost of insurance,[16] and targeting online housing offers. These models are seldom designed to take protected characteristics into account, yet they still have the

If algorithms rely on time spent on an educational resources, it will inadequately capture academic ability because of potential lack of internet access or other ways to access the resource.

[13] Colin Lecher, "Facebook drops targeting options for housing, job, and credit ads after controversy," The Verge, March 19, 2019 https://www.theverge.com/2019/3/19/18273018/facebook-housing-ads-jobs-discrimination-settlement.

[14] Jeffrey Dastin, "Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women," Reuters, October 9, 2018

[15] Spandana Singh, Eric Null, Sharon Bradford Franklin, OTI, Reconsideration of HUD's Implementation of the Fair Housing Act's Disparate Impact Standard, Docket No. FR-6111-P-02 https://newamericadotorg.s3.amazonaws.com/documents/New_Americas_Open_Technology_Institute_Comments_on_HUD_Proposed_Rule_FR-6111-P-02.pdf.

[16] See Robert Bartlett et al., Consumer Lending Discrimination in the FinTech Era 1 https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf.

capacity for protected-class discrimination.[17] The datasets and correlations on which they rely can reflect societal bias[18] in non-obvious ways that models may reproduce." [19]

"Biased data can generate problematic and harmful results. Algorithmic models that are based on correlations found in data from historically discriminatory systems will wrongfully perpetuate those patterns of discrimination. For example, research conducted on the use of algorithmic decision-making for pretrial "risk assessment" instruments has found that although these tools appear to be objective and neutral, they threaten to exacerbate unwarranted discrepancies and instances of discrimination in the justice system. This can result in a "misleading and undeserved imprimatur of impartiality for an institution that desperately needs fundamental change."[20] (2c, 3a)

B. Government use of data

Government surveillance programs and law enforcement agencies have directly accessed[21] or bought[22] data from commercial databases, without a warrant or probable cause, specifically targeting people of color. The U.S. military has purchased, through contractors, location data from a broker that compiled its data from apps designed specifically for Muslims, including prayer and dating apps[23]. The public-private partnership on data use goes both ways. According to Our Data Bodies (ODB) the conviction and incarceration data on individuals can be used as a barrier to employment, services and housing, with disproportionate effect on Black residents.[24] (3e)

---

[17] See, e.g., Bartlett et al., supra note 4, at 16 (finding that FinTech algorithms discriminated 40% less than face-to-face mortgage lenders but still charged Latinx and African-American applicants 5.3 basis points more in interest for purchase mortgages and 2.0 basis points more for refinance mortgages originated on FinTech platforms) ("[A]lgorithmic lending may reduce discrimination relative to face-to-face lenders, but algorithmic lending is not alone sufficient to eliminate discrimination in loan pricing.)

[18] Housing-related decisions and data in the United States are inevitably shaped by centuries of segregationist policies and institutional discrimination. See, e.g., Joseph D. Rich, Lawyers' Committee for Civil Rights Under Law, HUD's New Discriminatory Effects Regulation: Adding Strength and Clarity to Efforts to End Residential Segregation (May 2013) https://lawyerscommittee.org/wp-content/uploads/2015/08/HUDs-New-Discriminatory-Effects-Regulation.pdf.

[19] Spandana Singh, Eric Null, Sharon Bradford Franklin, OTI, Reconsideration of HUD's Implementation of the Fair Housing Act's Disparate Impact Standard, Docket No. FR-6111-P-02 https://newamericadotorg.s3.amazonaws.com/documents/New_Americas_Open_Technology_Institute_Comments_on_HUD_Proposed_Rule_FR-6111-P-02.pdf.

[20] Id.

[21] See, e.g., Eli Rosenberg, "Motel 6 will pay $12 million to guests whose personal data was shared with ICE," *Washington Post*, April 8, 2019 https://www.washingtonpost.com/nation/2019/04/06/motel-leaked-personal-data-guests-ice-officials-say-now-it-owes-them-million/?utm_term=.d6775c0fd3be.

[22] Lauren Sarkesian, Spandana Singh, "Your Dating App Data Might Be Shared With the U.S. Government" Slate, March 2021 https://slate.com/technology/2021/03/dating-apps-data-brokers-transparency-government.html.

[23] Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps" Vice.com, November 2020, https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

[24] "Charlotte," *Our Data Bodies*. In a state like North Carolina, this data practice has significant implications for racial equity, since Black residents are five times more likely than white counterparts to be incarcerated. https://www.odbproject.org/our-cities/charlotte/.

III. Action

Privacy harms that disproportionately affect marginalized communities happen in three main ways: 1) a company uses personal information to directly discriminate against marginalized communities, 2) they make it available to a third party who does so, including data brokers and their clients, or 3) they unintentionally design data processing practices in ways that cause discriminatory results. These are concerns that can be addressed through a range of actions, including voluntary changes at companies, and strong and enforceable legislation.

A. Company action

Algorithmic decision-making, relying solely on data and statistics may mitigate concerns about discriminatory decision-making since it is perceived to be less biased than human decision-makers, but testing can likely show unintended biased results, often because training data reflects the underlying biases and discrimination that exist in the physical world. A way to ensure positive use of the data collected and the algorithms used to collect it is to reframe the questions posed. Fundamentally, the outputs of the algorithms can show the biases inside of the institution and can be used to reform it, to examine why certain groups are less successful, be it an educational setting or in a corporate one.[25] (4h)

1. Design choices

Design choices play a crucial part in both potentially enabling and alleviating privacy harms, especially as they relate to marginalized communities. OTI researched the causes and potential recommendations for successful equity by design for both the production process and personnel.[26]

There are specific pragmatic ways to integrate equity principles into the production process from the inception of an idea to the release of a technological tool or product. First, formulating ideas and problem statements to account for identity-based experiences. Second, refining product roadmapping to identify equity concerns. Third, critically evaluating data to offset systemic inequities. Fourth, valuing diversity in selecting users for interviews, journey mapping, testing, and research. Fifth, taking steps to avoid repeating the previous mistakes.

Similarly, in terms of personnel, there are concerns that can be alleviated through an equity-by-design perspective. First, by committing to seeking out representatives of those voices missing from the project. Second, by fostering an inclusive environment where those impacted by the technology the team is developing feel empowered. Third, by consulting with external organizations who specialize in equity. (6d)

It is crucial that the entire tech policy ecosystem consider the voices of marginalized communities, not only companies or the government. Fundamentally, the tech policy ecosystem should seek to center the communities most affected by the civil rights harms that arise from commercial data practices. (6f)

---

[25] Rep. Yvette Clarke, A. Prince Albert III,Daniel Kahn Gillmor, Iris Palmer, Koustubh Bagchi, "Automated Intrusion, Systemic Discrimination," (Panel, Online, June 3, 2020) https://www.newamerica.org/oti/events/online-automated-intrusion-systemic-discrimination/.

[26] See Koustubh "K.J." Bagchi, Brittany Thomas, OTI, Equity by Design (April 2021) https://www.newamerica.org/oti/reports/equity-by-design/.

2. Transparency and audits

Another way to ensure that AI use fulfills its potential to be extremely valuable to society is through auditing, transparency and assessment mechanisms.

Transparency and impact assessments are crucial in order to understand potential risks *before* the implementation of the AI tool,[27] and regular audits need to be performed after an AI system is deployed, especially when a system is updated or has new training data.

To be meaningful, transparency mechanisms must be able to be delivered to multiple different audiences.[28] For instance, transparency efforts should be accessible to the average user without technical background or interest, thus presented in a straightforward way. Researchers and journalists often are interested in more granular and technical information, thus they would be better suited with access to more technical tools and audits (within the limitations of specific guardrails in order to remove any potential privacy consequences).[29] (6c)

While important for the companies to do voluntarily, legislation that imposes these requirements would be useful, particularly if these included additional safeguards for "high-risk information systems" like those that use data about sensitive characteristics including race, gender, biometrics and criminal arrests.[30]

B. Legislation

As OTI has argued before to the Federal Trade Committee (FTC), the notice and consent regime does not prevent harmful data practices and in fact places undue burdens on users.[31] While users want more control of their data, and care about their privacy, users find it difficult to properly interpret notices and data policies and truly protect themselves against practices they may not agree with. Enforcement is lacking, and companies should be held accountable for their privacy and civil rights transgressions. To that end OTI and several civil rights organizations have proposed principles that should be the basis for a new regime and legislation, and it is promising to see a majority of them adopted by a bill which has strong bipartisan support, thus a good chance at passage in both congressional houses.

1. Existing regime

The current level of information and privacy tools is inadequate to even make informed decisions, let alone properly assess and mitigate potential harms. If the notice and consent regime continues, straightforward notices to users from companies could be a first step to clearly make sense of the issues but would not be the only or best way to alleviate this concern. (1b)

---

[27] Palmer, Iris. "Choosing a Predictive Analytics Vendor: A Guide for Colleges." New America, September 5, 2018 https://www.newamerica.org/education-policy/reports/choosing-predictive-analytics-vendor-guide/

[28] "How Ranking and Recommendation Algorithms Influence How We See the World," video, posted by New America, July 14, 2020 https://www.youtube.com/watch?v=MaStEsqH1L0&.

[29] Id.

[30] Algorithmic Accountability Act, H.R. 2231, 116th Congress (2019) https://www.congress.gov/bill/116th-congress/house-bill/2231.

[31] Eric Null, Becky Chao, Sharon Bradford Franklin, OTI, Competition and Consumer Protection in the 21st Century Hearings: The FTC's Approach to Consumer Privacy, Docket No. FTC-2018-0098 https://newamericadotorg.s3.amazonaws.com/documents/Comments_of_New_Americas_OTI_Consumer_Privacy.pdf.

2. Current enforcement

It is crucial for the protection of users and their rights that more enforcement be brought[32] through the FTC, the NTIA, and state attorneys general, [33] as well as through private right of action. The agencies at the state and federal level should work to find ways to strengthen privacy protections as well as provide each other with guidance and aid. (4c, 5e)

While the FTC does not have general privacy authority, among the 82 statutes enforced by the FTC,[34] Congress has delegated to it the enforcement authority for several specific privacy statutes. The United States is the only country in the Organization for Economic Co-operation and Development (OECD) without a data protection agency, but the FTC fulfills some of the roles of such an agency. The FTC would need additional authority under the Administrative Procedure Act, and significant resources if it were to become the enforcer of a comprehensive federal privacy law. It is currently limited by both strict standards for rulemaking under the Magnuson-Moss Warranty Act,[35] and by its small number of staff dealing with data privacy.[36] While OTI is heartened to note the launch of the FTC's Office of Technology, this is only a necessary first step in increasing the agency's capacity and expertise.[37] (5e)

Because the FTC does not have a clear mandate, rules, or resources to function as an enforcement authority,[38] the FTC currently focuses on privacy harms which can be quantified through economic damage. This likely does not encompass the entire ecosystem of harms related to civil rights, which may end up cause social or political damage,[39] and does not fully intersect with its core jurisdiction, which is built around unfair or deceptive acts or practices. (4c, 5e)

3. Principles for a new regime

Legislation is crucial for protecting privacy and civil rights online, especially in the context of automated decision-making. As OTI and 33 other public interest organizations have said before, legislation should follow at least a basic set of public interest privacy principles, in order to ensure "basic fairness, prevent discrimination, advance equal opportunity, protect free

---

[32] Consumer Data Privacy: Examining the European Union's General Data Protection Regulation and the California Consumer Privacy Act, Hearing before the Senate Committee on Commerce, Science, and Technology (Oct. 10, 2018), Testimony of Laura Moy, https://perma.cc/3HDL-9ZY5 (at 10-14).

[33] Danielle Keats Citron, The Privacy Policymaking of State Attorneys General, 91 Notre Dame Law Review 747 (Feb. 16, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297.

[34] "Statutes Enforced or Administered by the Commission," Federal Trade Commission, December 8, 2013 https://www.ftc.gov/enforcement/statutes.

[35] "Magnuson Moss Warranty-Federal Trade Commission Improvements Act," Federal Trade Commission https://www.ftc.gov/enforcement/statutes/magnuson-moss-warranty-federal-trade-commission-improvements-act.

[36] "FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security," Federal Trade Commission, June 23, 2020 https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportresourcesprivacydatasecurity.pdf.

[37] FTC Launches New Office of Technology to Bolster Agency's Work (February, 17, 2023) https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-launches-new-office-technology-bolster-agencys-work.

[38] Elizabeth Banker, Blake Bee, Bob Gellman, Yosef Getachew, Dylan Gilbert, David Medine, "Enforcing a New Privacy Law," (Panel, Washington, DC, October 8, 2019) https://www.newamerica.org/oti/events/enforcing-new-privacy-law/.

[39] Id.

expression, and facilitate trust between the public and companies that collect their personal data."[40]

First, privacy protections must be strong, meaningful and comprehensive: mandating fairness in processing all personal data, respecting individuals' expectations for how data should be treated, providing for data portability, and including safeguards against misuse of data, including de-identified and aggregate data.[41]

Second, civil rights protections must be at the core of data practices, as well as preventing unlawful discrimination, and advancing equal opportunity. Automated decision-making should be legislated to be fair and transparent. The original document states:

> "Automated decision-making, including in areas such as housing, employment, health, education, and lending, must be judged by its possible and actual impact on real people, must operate fairly for all communities, and must protect the interests of the disadvantaged and classes protected under anti-discrimination laws. Legislation must ensure that regulators are empowered to prevent or stop harmful action, require appropriate algorithmic accountability, and create avenues for individuals to access information necessary to prove claims of discrimination. Legislation must further prevent processing of data to discriminate unfairly against marginalized populations (including women, people of color, the formerly incarcerated, immigrants, religious minorities, the LGBTQIA/+ communities, the elderly, people with disabilities, low-income individuals, and young people) or to target marginalized populations for such activities as manipulative or predatory marketing practices. Anti-discrimination provisions, however, must allow actors to further equal opportunity in housing, education, and employment by targeting underrepresented populations where consistent with civil rights laws. Moreover, decades of civil rights law have promoted equal opportunity in brick-and-mortar commerce; legislation must protect equal opportunity in online commerce as well."[42]

Thirdly, government at all levels should be a part of protecting privacy rights and in enforcing them. For enforcing comprehensive privacy legislation, agencies such as the FTC, or any newly-created agency, should receive enhanced authority, proportionate staff, resources and tools, as well as empowering state attorneys general and providing citizens with private rights of action.[43]

Fourth and final, privacy legislation should provide clear redress for privacy violations and not focus solely on financial injury, but make clear that "invasion of privacy itself is a concrete and individualized injury."[44] (5a, 5d)

---

[40] Public Interest Privacy Legislation Principles. https://newamericadotorg.s3.amazonaws.com/documents/Public_Interest_Privacy_Principles.pdf.

[41] Id.

[42] Id. Page 2.

[43] Id.

[44] Id. Page 3.

As part of a letter OTI and 26 civil society organizations sent to leaders in congress in 2019,[45] we have further identified 10 specific provisions that are an ideal baseline to prioritizing and directly addressing civil rights impacts arising from exploitation of personal information.

> "1) Prohibit the use of personal data to discriminate in employment, housing, credit, education, or insurance—either directly or by disparate impact.
> 2) Prohibit the use of personal data to discriminate in public accommodations and extend such protections to businesses that offer goods or services online.
> 3) Prohibit the use of personal data to engage in deceptive voter suppression.
> 4) Require companies to audit their data processing practices for bias and privacy risks.
> 5) Require robust transparency at two tiers: easy-to-understand privacy notices for consumers, and comprehensive annual privacy reports for researchers and regulators.
> 6) Enable researchers to independently test and audit platforms for discrimination.
> 7) Empower a federal agency with rulemaking authority, enforcement powers, and enough resources to address current and future discriminatory practices.
> 8) Provide individual rights to access, correct, and delete one's personal data and inferences made using that data.
> 9) Provide a private right of action, because marginalized communities historically have not been able to rely upon the government to protect their interests.
> 10) Establish baseline nationwide protections and allow states to enact stricter laws. Do not preempt state civil rights laws under any circumstances."[46] (5a)

4. Legislative choices

Shifting away from the notice and consent privacy regime to one with an emphasis on requirements for data minimization and use restrictions, as well as user rights to access, correct, delete or port data would be a better way to tackle privacy harms more directly. Specifically, data minimization reduces risks associated with data collection and storage, such as data breaches,[47] while also reducing the privacy risk of inappropriate secondary and discriminatory uses,[48] and reducing the cost for companies from extensive data collection and storage systems.[49] Even more, purpose limitations would be useful in order to preclude use of data to discriminate based on a protected class[50] while requiring more transparency in order to also help determine when such disparate impacts exist. Finally, users should be given direct data rights in order to truly

---

[45] Letter to Congress on Civil Rights and Privacy (April 19, 2019) https://newamericadotorg.s3.amazonaws.com/documents/Letter_to_Congress_on_Civil_Rights_and_Privacy_4-19-19.pdf.

[46] Id.

[47] See FTC Staff Report: Internet of Things: Privacy & Security in a Connected World, Federal Trade Commission (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november2013-workshop -entitled-internet-things-privacy/150127iotrpt.pdf (at IV)

[48] David Kravets, An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle, Wired (May 2, 2012), https://www.wired.com/2012/05/google-wifi-fcc-investigation/.

[49] Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

[50] Muhammid Ali, et al. (2019), Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes, https://arxiv.org/abs/1904.02095. See also Cassandra Jones Harvard, On the Take: The Black Box of Credit Scoring and Mortgage Discrimination, Pub. Int. L.J. 20 (2011): 271.

have control over their data, through easy-to-use, easy-to-find controls, and the right to access, correct, delete and port data a company has about or collected from them. (5d)

Further, a new privacy regime may also be bolstered by a private right of action, where individuals can sue companies for violating their privacy rights. Even with a fully-staffed and properly mandated FTC, there is a chance that federal agencies alone, even with the help of state attorneys general, may not be able to address some individual harms, so private right of action may be useful in cases of under-enforcement. Certainly, this would have to be designed with limits, both financial and procedural, in order to reduce frivolous lawsuits, as well as needing an authorizing agency, or intent requirements. (4c)

It is important to note that legislative action does not happen in a vacuum and is not immune to the political challenges of the day. As presented so far, it is absolutely clear that there is a strong imperative for action on every level in protecting the privacy and civil rights of all users, especially those in underserved or marginalized communities. However, ideal forms of action do not easily translate into potential action when faced with the necessity of compromise. With several bills introduced in the past few years, comprehensive federal privacy legislation had stagnated over political considerations on issues such as private right of action and federal preemption of state privacy bills.

In 2022 a compromise solution, in the form of the American Data Privacy and Protection Act (ADPPA),[51] emerged and has garnered strong support from both political parties, civil society members - including an overwhelming majority of the signatories of the above principles[52] - and showed great promise of passing. ADPPA is not the ideal bill, in that it may not fully satisfy concerns about federal preemption, private right of action, and any other apprehensions about specific policy pieces. It is, however, the closest the United States has gotten to actually making substantive and legitimate changes in order to address the many ways that commercial data practices, and the use of algorithmic decision-making, have harmed citizens and especially members of underserved or marginalized groups. OTI continues to support ADPPA passage as the first step in tackling privacy and civil rights harms online. (5a)

Beyond comprehensive privacy legislation, OTI supports the passage of the Fourth Amendment Is Not For Sale Act[53], introduced by Senators Ron Wyden (D-Ore.) and Jerrold Nadler (D-N.Y.) which would ban the federal government from purchasing data on individuals within the United States from data brokers without a warrant. By outlawing the purchase of data where a court order would otherwise be required, the Fourth Amendment Is Not For Sale Act would ensure that the government can no longer skirt Fourth Amendment rules.

---

[51] H.R. 8152 - Text of the bill is here: https://www.congress.gov/bill/117th-congress/house-bill/8152/text

[52] https://newamericadotorg.s3.amazonaws.com/documents/Coalition-Letter-Supporting-ADPPA_August-2022.pdf

[53] https://www.wyden.senate.gov/imo/media/doc/The%20Fourth%20Amendment%20Is%20Not%20For%20Sale%20Act%20of%202021%20Bill%20Text.pdf