The Privacy-Bias Tradeoff: Data Minimization and Racial Disparity Assessments in U.S. Government

Arushi Gupta  
Stanford University  
Stanford, California, USA

Victor Y. Wu  
Stanford University  
Stanford, California, USA

Helen Webley-Brown  
Massachusetts Institute of Technology  
Boston, Massachusetts, USA

Jennifer King*  
Stanford University  
Stanford, California, USA

Daniel E. Ho*  
Stanford Law School  
Stanford, California, USA

1 INTRODUCTION

While early work in algorithmic fairness has grappled with the fairness-accuracy tradeoff [32, 52, 70, 73, 120, 148], one of the emerging tradeoffs is between fairness and individual privacy [25, 67]. Much technical work, for instance, has shown the tension between applying differential privacy and achieving algorithmic fairness [51]. Differential privacy [40] can worsen disparate impact in model accuracy [13], such as for racial minorities or rural communities [27, 125, 144]; equalized odds as a fairness measure can disproportionately leak information for disadvantaged groups [25]; and the impossibility theorems that have vexed algorithmic fairness have similarly affected simultaneously achieving differential privacy and fairness [6]. Institutionally, leading work has shown how interpretations of privacy law and policy, such as the E.U.'s General Data Protection Regulation, have undermined the capacity to assess and mitigate bias in the private sector, as technical teams are not allowed to access protected attribute information such as race and ethnicity [9, 146]. Data minimization – the principle that entities should collect and retain only data minimally necessary to achieve their objectives – has meant that critical information needed to conduct fairness assessments is unavailable. We call this the emerging “privacy-bias tradeoff.” As companies and regulators turn toward protecting individuals’ information privacy via data minimization,1 we ask: How can we ensure that the lessons of algorithmic fairness are not ignored? How have institutions attempted to grapple with these tensions? And what practical policy options are available to navigate the tradeoff in the most grounded fashion?

What is less well-known is that since 1974, the U.S. government can be described as engaging in a large-scale data minimization experiment. The Privacy Act of 1974 mandates that federal agencies (a) collect personally identifiable information only as necessary to execute their statutory mandate, (b) use this information only for the purpose that justified its collection, and (c) refrain from data sharing or linkage [77]. Statutes like the Paperwork Reduction Act make it procedurally challenging for agencies to add new forms, or revisions thereof), typically requiring approval by the Office of Management and Budget (OMB) and a notice-and-comment process for public input when they do try to do so.

1The E.U.'s General Data Protection Regulation incorporated data minimization into its framework with its adoption in 2018. In 2022, the U.S. Federal Trade Commission signaled that it may be considering adopting data minimization provisions to regulate the private sector during its Advanced Notice of Proposed Rulemaking [29].
In this paper, we demonstrate that the “privacy-bias tradeoff” has become an important battleground for fairness assessments in U.S. government. On his first day in office, President Biden signed Executive Order (EO) 13,985, a racial justice initiative mandating that agencies conduct “equity assessments” of federal programs [48]. For the first time, agencies are required to assess disparities (e.g., along race and ethnicity) in accessing benefits and opportunities in federal policies and programs. Such assessments have been uniquely important for understanding disparities with the rise of algorithmic decision-making tools, as emphasized in the nondiscrimination principle of the Blueprint for an AI Bill of Rights [98], the Trustworthy AI Executive Order 13,960 [46], and the second racial justice Executive Order 14,091 [47]. Yet in practice, as we show, the Privacy Act has made the implementation of disparity or equity assessments profoundly difficult. As EO 13,985 itself notes, “Many Federal datasets are not disaggregated by race, ethnicity, gender, disability, income, veteran status, or other key demographic variables.”

We studied agency action plans filed in response to the EO and conduct a comprehensive assessment across high-volume claims agencies that provide a wide range of government services (e.g., food assistance, farm subsidies, patents, tax refunds, loan guarantees), as well as all agencies filing equity action plans under the EO. Our analysis demonstrates how the privacy-bias tradeoff has undercut efforts to implement equity assessments. First, we show that the public response has been uniformly positive toward conducting equity assessments, with virtually no pushback on privacy grounds, with many agencies proposing substantial efforts. Second, we demonstrate that in practice, the challenges posed by the tradeoff have been profound. Twenty-one of 25 agencies note the lack of demographic information as a challenge. Agencies may be affirmatively prohibited from linking demographic records under privacy provisions. The Internal Revenue Service, for instance, has indicated that it would require statutory changes to be able to link to Census data to conduct an equity assessment [58]. Implementation of the Privacy Act’s data minimization principle has led to pathological results: until 2022, for instance, the Food and Nutrition Service imputed race by “visual observation” by officials (e.g., the individual processing an application) when race was not self-reported to the Supplemental Nutrition Assistance Program [53]. Data minimization has meant that even where agencies want to acquire demographic information in principle, the legal, data infrastructure, and bureaucratic hurdles are severe. Third, we derive policy implications to address these barriers. Streamlining the approval for data collection for disparity assessments, restricting demographic data access to teams conducting an assessment (most ambitiously through the prototype National Secure Data Service (NSDS) [91] or the proposed National Artificial Intelligence Research Resource (NAIRR) [86]), and providing technical assistance to adapt the most appropriate methods would each enable disparity assessments, without seriously undermining individual privacy or the Privacy Act. Data minimization should not function as a license for blindness to disparities.

To our knowledge, this is the first paper to document the privacy-bias tradeoff at federal agencies. We make four distinct contributions. First, we conduct in-depth case studies to understand how federal agencies that affect large parts of the U.S. population have grappled with the privacy-bias tradeoff in practice. The federal experience with data minimization offers unique insights into the emerging tension between privacy and fairness. Second, we outline the range of distinct data approaches that have been taken — from record linkage, to amending forms, to commissioning a separate survey, to racial imputation methods — and discuss their legal and statistical challenges. Third, we identify the most common barriers to implementing equity assessments, which are centrally shaped by the data minimization approach taken under the Privacy Act of 1974, but also present a range of associated legal, data infrastructure, and bureaucratic land mines. Last, we provide a series of concrete and implementable policy recommendations to both protect privacy principles and enable equity — and algorithmic fairness — assessments.

We proceed as follows. Section 2 discusses primitive concepts and our research approach. Section 3 provides an assessment of data minimization at federal agencies, with detailed case studies in Appendix ??.

2 DEFINITIONS, CONCEPTS, AND RESEARCH APPROACH

Definitions and Concepts. We begin from the premise that race and ethnicity are socially constructed [14, 78]. Some might take the position that the government, as a result, should never attempt to measure (or classify) race or ethnicity, but that position is refuted by EO 13,985, legal reporting requirements, as well as by the algorithmic fairness literature, which has focused on “fairness through awareness” [39]. Precisely because race and ethnicity have measurable disparate impacts on individuals, it is seen as critical to understand racial disparities in federal programs meant to equally benefit all. We also note that equity assessments are important across intersections of demographic characteristics (e.g., race and gender) [10, 28], but without some way to measure race or ethnicity, intersectional assessments remain impossible [54].

The federal approach to measuring race and ethnicity has varied over time and across agencies. The Social Security Administration (SSA), for instance, made changes to their “race/ethnicity codes” over decades [127]. The agency began collecting race data from enrollees in the 1930s [127]. Through 1980, enrollees self-identified as belonging to one of three categories: “White,” “Negro,” or “Other” [127]. Government-wide standards for collecting data on race and ethnicity were established by the OMB’s 1977 “Standards for the Classification of Federal Data on Race and Ethnicity” and subsequently revised in 1997 [103, 104], but compliance with them has been uneven. On June 15, 2022, Dr. Karin Orvis, Chief Statistician of the United States, announced plans to review and revise the OMB standards to enable greater disaggregation of racial categories (e.g., representing subgroups of “Asian Americans”), but this effort is not expected to be completed until 2024 [113].

We use privacy throughout as shorthand to refer to informational privacy, namely the right of individuals to have a meaningful say in the way data about them is collected, stored, and used. There are multiple conceptions of privacy, such as the “right to be let
Table 2. Third, we assess formal agency responses filed to the EO severely restricting lenders’ power to ask applicants for protected characteristics [2], but the Consumer Financial Protection Bureau (CFPB) eased this decades-long ban in 2017 to permit demographic data collection in more cases [19]. Table 1 summarizes case studies across federal agency programs.

### 3 THE STATE OF DATA MINIMIZATION AT FEDERAL AGENCIES

Responses to EO 13,985 from federal agencies and nongovernmental stakeholders suggest there is widespread support for conducting disparity assessments, but that existing demographic data poses serious challenges. Even before the EO was issued, numerous efforts proposed increasing data collection for disparity assessments. For example, Section 4302 of the Affordable Care Act (2010) requires national, federal data collection efforts to include race, ethnicity, sex, primary language, and disability status in order to “improve assessment of healthcare disparities” [59]. The Office of Civil Rights, for instance, stated: “The collection of personal data is “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” [45].

**Research Approach.** To explore the tension between bias assessment and privacy protections in general, we take a three-part approach. First, we conduct detailed case studies of demographic data collection, bias assessment, and privacy protections in large claims agencies. As there are over 300 federal agencies, we focus on high-volume claims agencies that affect large numbers of individuals. We consider all agencies with more than 1,000 claims opened or filed in 2013 [4] and more than $200 billion in 2023 budgetary resources [137]. We also include other high volume claims agencies, like the US Patent and Trademark Office (USPTO). This leaves us with a relatively comprehensive list of high-impact federal claims agencies. Second, for each agency, we select at least one high-impact program to evaluate in detail. For each program, we attempt to answer the following questions: What is the current practice of collecting race and ethnicity data? What is the current approach to estimating disparities or implementing EO 13,985? Have there been statutory or regulatory attempts to improve the ability of the agency to assess racial disparities? And if so, what barriers stand in the way of these improvements? All agencies, programs, and results are reported in Table 2. Third, we assess formal agency responses filed to the EO 13,985 and study stakeholder responses to the federal governments request for information for implementing EO 13,985.

### 3.1 Data Collection in 10 Large Claims Programs

Despite the positive reception to EO 13,985, Table 2 demonstrates a stark reality: demographic data is rarely, inconsistently, and poorly collected, and prior attempts to improve such collection ran into substantial barriers. Of the ten agencies studied, none systematically collects demographic data linked to program performance metrics and only two agencies have established a data linkage process that does not require direct data collection. For other agencies, the law or longstanding policy restricts data collection outright in some cases, while in others, the data collected is inadequate to support rigorous analysis of bias.

In four of the ten agencies studied, legal barriers prevent data collection for some or all programs. For instance, ECOA is an explicit legal barrier to demographic data collection across agencies; it precludes data collection for many agricultural loans facilitated by the USDA (See I11 in Table 2, where we use the letter to refer to column and the number to refer to the row as short hand) as well as small business loans like those issued by the pandemic-era Paycheck Protection Program (See Row 13 in Table 2). A 2008 Government Accountability Office (GAO) report concluded that ECOA’s data limitations also complicate efforts to understand lending discrimination broadly and to identify specific lenders violating nondiscrimination requirements [145]. The Treasury Department’s interpretation of privacy law and other relevant legislation mean the IRS only collects demographic attributes explicitly allowed in the tax code, excluding race, ethnicity, and sex (See I5 in Table 2) [58]. In a fifth case, the USPTO’s standing practice also lacks demographic data questions in absence of a clear-cut statutory allowance for expanding data collection [61], despite an indirect call to “establish methods for studying the diversity of patent applicants” [68] (See Row 12 in Table 2).

Another three agencies attempt to collect demographic data, but lack the consistency and quality needed to support reliable bias assessments. The USDA is statutorily required by the 2008 Farm Bill to collect and publicly report demographic data for applicants to certain agricultural loans [107], but as one nonprofit, the Sustainable Agriculture and Food Systems Funders, notes, the website reporting USDA demographic data is “very badly out of date” and that “much of the data is missing” [133] (See I11 in Table 2). When applicants do not self-identify, USDA’s demographic data sometimes relies on office employees’ visual assessment of program applicants’ race and ethnicity, despite long standing questions about the ethics and reliability of such an approach and a 2011 departmental regulation prohibiting such visual observation2 [55]. Other USDA programs, such as the Supplemental Nutrition Assistance Program (SNAP), collect data more proactively but relied on visual observation when applicants did not self-report until 2021 [74] (See C10 in Table 2). Similarly, the Department of Veterans Affairs collects data from a variety of programs and sources but lacks “the complete and consistent collection of demographic data” that would support bias assessment [136] (See I3 in Table 2). In the case of Disaster Grants by

---

2A USDA report on the 2019 Market Facilitation Program notes that “departmental regulation prohibits the collection of race, ethnicity, and gender data based on a visual assessment, yet [Farm Services Agency] county office employees assigned race, ethnicity, and/or gender to producers through such means” [107].
the Department of Housing and Urban Development (HUD), only successful applicants provide demographic information, making an assessment of disparities in the application process impossible [57] (See I9 in Table 2).

The only agencies with a systematic approach to demographic data collection are SSA and HHS. Although neither directly collects race and ethnicity, SSA collaborates with other agencies, primarily Census, to link records from four different population surveys to determine race [79] (See C1 in Table 2). While HHS considers self-reported race and ethnicity to be the “gold standard” of accuracy [102], in practice it combines SSA’s data with independent imputation to evaluate Medicare for racial bias (See C2 in Table 2). Table 1 enumerates the approaches to demographic data collection and comparative strengths and weaknesses. Agencies have six predominant approaches to collecting information about race and ethnicity: record linkage, voluntary direct data collection, mandatory direct data collection, imputation, survey-based random sampling, and visual observation. Subtle tradeoffs exist between these approaches. Survey-based random sampling, for instance, might un tether bias assessment from legacy race and ethnicity categories, but stands to be significantly more costly than other approaches, particularly for small sample demographic groups. Imputation is much more cost-effective, but conventional methods rely on restrictive assumptions [26] that are ideally validated on auxiliary datasets [41]. While these tradeoffs can be subtle, one approach is nearly universally deprecated, but still present in federal datasets: visual observation [107].

3.2 Pre-Executive Order Attempts to Overcome Data Minimization

To understand how we arrived at this cacophony of race reporting, we now trace the barriers to improving data collection; improvements have been proposed for every program studied, except the Small Business Administration’s Paycheck Protection Program (See Row 13 in Table 2), prior to the issuance of the EO. While these proposals vary in seriousness, approach, and progress towards implementation, the number of proposed expansions highlights the general consensus that demographic data collection is a worthwhile goal. In half of the case studies (See Rows 2-8 in Table 2), the agency itself is pursuing a serious data collection proposal. Some, like the HHS pilot program (See H2 in Table 2), are more limited in scope, while others, like Treasury’s investment in imputation (See H5 in Table 2), intend to fully address the agency’s data needs. Of the remaining case studies, HUD and USDA have initiated some agency efforts to collect demographic data. As SSA’s bias assessment process is already relatively robust, changes to the long-standing record linkage process with Census have only been floated in passing by small advocacy groups (See H1 in Table 2). In contrast, several bills have proposed demographic data collection for USPTO, but none has passed and no active effort to obtain data exists (See H12 in Table 2).

Across agencies, we observe five recurring classes of barriers, each influenced by privacy interests in its own way. First, legal restrictions directly prevent data collection, such as the Privacy Act or ECOA, or delay implementation, such as the Paperwork Reduction Act’s notice and comment requirements (See I2 in Table 2).

Second, fragmented or outdated technical infrastructure and a lack of technical expertise make systematic bias assessment challenging. Privacy measures to prevent unauthorized disclosure, while essential, further increase the technical resources required. Third, proposed data collectors, either the federal agency or a private third party, resist data collection, and in some instances we document evidence that this stems from the public relations, political, or litigation risk of uncovering bias in program administration. For instance, employers reporting to EEOC and lenders reporting to CFPB cite privacy and cost justifications, even in light of substantial protective measures proposed by the agency (see Appendix ?? and ?? for details). Fourth, federal agencies worry that asking respondents to provide demographic data will raise privacy concerns for respondents, and thus increase non-response rates. Finally, agencies lack the dedicated financial and personnel resources to implement improvements. Other barriers like technical limitations or complex legal review requirements contribute to the resource gap. (For convenience, we denote these enumerated barriers in Column I of 2 in parentheses.)

3.3 EO 13,985 Equity Action Plans

To gauge the extent to which federal agencies are actively grappling with the privacy-bias tradeoff in response to EO 13,985, we conducted a content analysis of all 25 available equity action plans filed in response to the order (see Appendix ?? for details). We assess (a) whether the availability of demographic data is recognized as a barrier, and (b) what concrete solutions (e.g., record linkage, form collection, visual observation, imputation, and sample surveys) are proposed to cure the data deficit. Table 3 synthesizes our findings. The vast majority of agencies (21 of 25) highlight the lack of demographic data as a barrier to disparity assessments. The Treasury Department, for instance, states that the “right data to measure and advance equity is essential” but “challenges abound … since many federal datasets do not include race, ethnicity, or other key demographic variables.” Similarly, the Department of Veterans’ Affairs calls for expanded demographic data “to identify and eliminate disparities” [136]. The Federal Emergency Management Agency echoes this view: “The ability to collect demographic data …is imperative to achieving the intent and spirit of civil rights laws” [49]. While the wide acceptance of the role of demographic data in realizing anti-discrimination goals among federal agencies is certainly encouraging, far fewer equity plans supported their nominal recognition of the privacy-bias tradeoff with an concrete, actionable proposal of mechanisms to tackle it. Two agencies aim to run surveys; eight have committed to changing public-facing forms; four are proposing record linkage; and one is using imputation, but 13 agencies have at most partial or generic descriptions of any changes. Where an agency’s plan noted—a varying detail—an interest in increasing data collection, most pointed to some variety of form collection. The NSF plans to display demographic questions upon entry into Research.gov and the Department of Education will begin requesting demographic information as part of FAFSA. The Treasury’s limited demographic data sharing agreement with the Census Bureau, which supports cross tabulations of economic impact payments (EIP) data by race and ethnicity, is an affirmative
example of innovative inter-agency work to both actively recognise and concretely address the privacy-bias tradeoff.

Stakeholders, too, agree on the importance of collecting demographic data. A comprehensive review of each of the 531 responses to the OMB’s Request for Information on EO 13,985 revealed nearly universal calls for increased data collection, sharing, and disaggregation of existing statistics. As Code for America summarized, “accurate and comprehensive demographic data” is essential because “you can’t fix a problem you can’t see” [75]. While a handful of organizations touch on privacy, cautioning that “data collection efforts must also be balanced with the importance of confidentiality and privacy, especially for vulnerable communities whose data may be disproportionately collected and shared,” they still conclude that disaggregated data is “incredibly valuable, including as evidence of disparate impact, to help target resources, and to measure success” [87]. The Leadership Conference on Civil and Human Rights, the nation’s oldest civil rights coalition, notes that even though “privacy is a real concern” that should be addressed, it “should not be used as a red herring to avoid collecting, disaggregating, or reporting data with the appropriate protections in place” [134]. This input highlights the potential for privacy concerns with government data collection to obstruct anti-discrimination efforts, while affirming that demographic data is essential and can be compatible with privacy interests.

4 STRUCTURAL BARRIERS TO EQUITY ASSESSMENTS

In this section, we synthesize the barriers we observed across case studies to discuss the statutory limits of federal privacy law and three types of obstacles associated with putting fairness assessments into practice: resistance from third parties, agencies’ desire to maintain public trust, and infrastructural issues.

4.1 The Privacy Act

The Privacy Act of 1974 places significant limitations on the collection and use of personally identifiable information by government agencies. Passed in the wake of the Watergate scandal and amid growing concerns over government abuses of power and use of technology, the Act guards against the creation of a centralized federal database [109] through the adoption of a set of principles that were later enshrined into the Fair Information Practices: data minimization, purpose limitation, no disclosure without consent, rights of access and correction, and transparency (e.g., no secret data systems) [23]. Agencies can only collect information that is “relevant and necessary to accomplish a purpose of the agency” [77, §552(a)(b)(1)], and they are prohibited from disclosing personally identifiable information “to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains” [77, §552(a)(4)]. The statutory exceptions to the limits on disclosure often build on three general justifications: enabling statistical research [77, §552(a)(b)(5)], benefiting an agency’s mandate (the agency has a “need to know” [77, §552(a)(b)(1)]), or “routine use” that is otherwise compatible with the purpose for which the data was collected [77, §552(a)(7)]. Addressing bias is not explicitly acknowledged as a valid exception and is not easily justified through these standard avenues.

Table 1: Approaches to demographic data collection

<table>
<thead>
<tr>
<th>Data collection method</th>
<th>Description</th>
<th>Strengths</th>
<th>Weaknesses</th>
<th>Self-reported</th>
<th>SCRN</th>
<th>Notice &amp; comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record linkage</td>
<td>Agency records are linked with existing race and ethnicity data (e.g., Census, Social Security Administration)</td>
<td>No new data collecting required. Responses already vetted through prior administrative records. Large population coverage.</td>
<td>Express statutory restrictions to protect privacy. Need for technical infrastructure and expertise. Nonresponse to administrative data. Record linkage error.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Form collection (voluntary)</td>
<td>Demographic data fields are included on registration forms for government services, but providing data is clearly voluntary and will not affect eligibility for benefits or services</td>
<td>Opt-out provides more assurance to respondents. Direct population of interest.</td>
<td>Nonresponse bias. Respondent time. Respondent concerns about use of race/ethnicity in program.</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Form collection (mandatory)</td>
<td>Mandatory demographic data fields are included on registration forms for government services</td>
<td>Direct population of interest, with no nonresponse bias.</td>
<td>Lower response or participation rates. Respondent time. Respondent concerns about use of race/ethnicity in program.</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Visual observation</td>
<td>Enumerators or program administrators assess what they believe to be the race, ethnicity, or gender of program participants.</td>
<td>Opt-out provides more assurance to respondents. Direct population of interest. Elimination of non-response bias without requiring respondents to answer.</td>
<td>Data reliability. Training of officials conducting observation. Available only for in-person enrollment.</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Imputation</td>
<td>Demographic characteristics are inferred using statistical techniques, based on names, zip codes, and other predictive information</td>
<td>Can be performed for a near-full population. Only uses existing data and minimal public data.</td>
<td>Statistical bias. Results are more difficult to validate.</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Survey-based random sampling</td>
<td>A random subset of program recipients (or of the population) is randomly sampled and surveyed by researchers to determine demographic characteristics</td>
<td>Reduces reporting burden. Reduces respondent concerns over misuse of demographic data. Flexibility as to reporting categories.</td>
<td>Expensive, as separate data collection required. Nonresponse bias. Need to oversample small demographic groups.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Table 2: Data collection practices across federal agencies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>A. Sector</strong></td>
<td><strong>B. Agency</strong></td>
<td><strong>C. Collection</strong></td>
<td><strong>D. Source of Data</strong></td>
<td><strong>E. Method of Collection</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Social Security</td>
<td>SSA</td>
<td>No collection</td>
<td>Form collection</td>
<td>Record linkage, Census</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Medicare</td>
<td>HHS</td>
<td>No collection</td>
<td>Form collection</td>
<td>Record linkage, Census</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Veterans benefits</td>
<td>VA</td>
<td>Partial collection</td>
<td>Form collection</td>
<td>Record linkage, Census</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Non-mortgage</td>
<td>CFPB</td>
<td>No collection</td>
<td>Form collection</td>
<td>Record linkage, Census</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Mortgage lending</td>
<td>CFPB</td>
<td>No collection</td>
<td>Form collection</td>
<td>Record linkage, Census</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Wage discrimination</td>
<td>EEOC</td>
<td>Partial collection</td>
<td>Form collection</td>
<td>Mandatory collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Community development</td>
<td>HUD</td>
<td>Partial collection</td>
<td>Form collection</td>
<td>Record linkage, Census</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Food stamps</td>
<td>USDA</td>
<td>Visual</td>
<td>Form collection</td>
<td>Mandatory collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Farm subsidies</td>
<td>USDA</td>
<td>Visual</td>
<td>Form collection</td>
<td>Mandatory collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Patents</td>
<td>USPTO</td>
<td>None</td>
<td>Form collection</td>
<td>Mandatory collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Farm subsidies</td>
<td>USDA</td>
<td>Visual</td>
<td>Form collection</td>
<td>Mandatory collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12. Paycheck Protection</td>
<td>SBA</td>
<td>Partial collection</td>
<td>Form collection</td>
<td>Mandatory collection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The IRS offers an instructive example: “[t]itles 13 [providing Censuses’ privacy and confidentiality restrictions] and 26 [the Internal Revenue Code] of the United States Code limit the ability of Censuses and IRS to share data” and “Treasury officials report that laws protecting confidentiality prohibit IRS from acquiring demographic data from Census” [58, pp. 16-17] that could be used systematically to link data and evaluate bias. While Census and Treasury do enter project-based statistical research data sharing agreements, the necessary legal reviews require significant time and resources [58, p. 17]. One strength of imputation, Treasury’s favored approach, is that it does not require large-scale data sharing, and thus legal review. The limitations imposed by privacy law and practice are summarized by a respondent to the Commission on Evidence-Based Policymaking’s Survey of Federal Agencies and Offices, who says: “many agencies have restrictive requirements or restrictive interpretations of confidentiality laws and regulations that make it difficult to access valuable supplemental data.” Another respondent goes further, asserting that “the most critical barrier to data exchange is legal and disclosure limitations” [90, p. 17]. Finally, as mentioned above, a legacy of the Privacy Act that continues to hamper data sharing efforts is the fear of centralized government data resources. While a decentralized approach may protect the public’s privacy by making it difficult, if not impossible, for individuals to be tracked easily across agencies, this emphasis on decentralization reduced any perceived need for interoperable data infrastructure. Thus, inconsistencies in technical infrastructure proliferate and further obstruct data sharing, which in turn deprives interoperability. The proposal for the National Secure Data Service (NSDS), for example, attempts to work around the concerns of a centralized database while enabling data sharing for evidence building: “[t]he Evidence Commission rejected a large-scale data warehouse model due to its untenable privacy risks and practical limitations for implementation. Instead, the experts encouraged the establishment of a National Secure Data Service as a shared service for conducting temporary data linkages for exclusively statistical purposes” [91].

4.2 External Resistance to Data Collection by Agencies

In cases where agencies consider expanding data collection requirements for third party service providers, these third parties have
reacted with privacy concerns. For example, the CFPB issued policy guidance in 2018 regarding loan-level data collected under the Home Mortgage Disclosure Act (HMDA), which requires lenders to collect demographic data from mortgage applicants [20, p. 18]. The guidance recommended that loan-level data should be modified before public releases to prevent individual borrower re-identification. CFPB noted several industry comments which argued that privacy measures “did not sufficiently address” the risks of disclosure, but these comments “offered little evidence or analysis to support their views.” Some industry commenters stated that the CFPB should only release aggregate-level data, or not release any data to protect borrowers’ privacy. One commenter stated, “if there is ‘any chance’ that HMDA data could be used for criminal purposes, the benefits of disclosure could not outweigh the privacy risks.” In contrast, consumer advocates argued that loan-level data has “long been publicly disclosed without any evidence the data has been used to harm applicants and borrowers.” CFPB concluded that the risks—which are nonzero—“are justified by the benefits in light of HMDA’s purposes” [20]. A similar tension when the Equal Employment Opportunity Commission (EEOC) considered collecting pay data in addition to demographic data to target wage discrimination. During the initial research process in 2012, employers’ representatives expressed concerns about protecting individual privacy in aggregate data releases, so the EEOC re-examined statistical confidentiality standards to ensure tables with small cell-counts would be kept private [43]. After a multi-year, intensive research process, OMB decided in 2016 to begin collecting pay data. In 2017, OMB abruptly changed course, staying pay data collection on the grounds that it “lacks practical utility, is unnecessarily burdensome, and does not adequately address privacy and confidentiality issues” [116]. After worker groups sued, a federal judge reinstated pay data collection in 2019, finding OMB’s decision arbitrary and capricious and reiterating the value of pay data for self-monitoring and enforcement purposes [129]. Even so, in 2020, Congresswoman Virginia Foxx (R-NC) said in a hearing “that the commission has no way of keeping [pay data] confidential” [84]. These cases illustrate the tension between protecting individual privacy and collecting and releasing data necessary for bias assessment. Even in cases where federal agencies institute technical privacy protections to mitigate concerns, the question of how privacy risks should be weighed against the benefits of data collection remains.

4.3 Structural Barriers to Direct Data Collection by Agencies

While data sharing with other agencies is cumbersome, direct data collection raises concerns that the public may respond negatively. Even if individual privacy is not substantively threatened and collection would be permitted by law, agencies worry the public may feel threatened due to unfamiliarity with existing privacy protections, a lack of awareness of the collective benefits of demographic data collection, or distrust of the data collectors. When the justification for data collection under privacy law is murky, agencies are especially likely to behave conservatively to maintain public trust. The USPTO sought public comment on a data collection proposal for bias assessment for a 2012 study on diversity among patent applicants. It found that “the ability of mandatory surveys to generate individual demographic diversity data of acceptable quality and reliability is in tension with the lack of public support for mandatory surveys due to privacy concerns under current law” [135, p. 3] One commenter noted that voluntary surveys would “reassure” respondents about their privacy [135, p.3].

Although voluntary survey questions may maintain respondents’ sense of trust, they also pose the risk of lower response rates. A USDA report on the Market Facilitation Program (MFP), a program that distributed $25 billion to farmers hurt by retaliatory tariffs in 2018 and 2019, found that less than a third of recipients self-reported their race [99]. Minority groups often exhibit higher nonresponse rates for surveys in general [7, 50, 72] (though see Lee et al. 76), validating the USPTO’s concern that voluntary response may produce “statistical bias arising from self-selection among respondents” if the non-response is not random [135, p.3]. CBAMS Survey and Focus Groups document high levels of mistrust in the government and public institutions, particularly among marginalized groups, offering one explanation for low response rates and suggesting disparate nonresponse bias [81]. Some have suggested offering monetary incentives to boost response rates for government surveys, though this solution comes with its own set of problems [128].

For these reasons, mandatory data collection does not appear to be a favored choice amongst agencies. As USDA moves away from using visual observation when respondents do not self-identify, it has suggested states should “encourage [participants] to self-identify and self-report” through education about the use of demographic data for bias assessment, and should find “other data sources or statistical tools to account for the times when participants choose not to self-identify” [53].

Mandatory data collection is seen to create risk with program participation. Tax experts, for instance, agree that adding demographic data questions to Form 1040 risks reduced tax compliance [58]. Even if tax auditors are denied access to race data, eliminating any possibility of express discrimination, interviewees concur that people may not file taxes if they perceive the government to be overreaching and potentially discriminating [58, p. 14]. Comments from a Treasury statistician suggest the need to manage public perception may affect Treasury particularly acutely; other agencies worry that even sharing data with Treasury could depress survey response rates by creating a perception that responses could be used to enforce tax compliance [115]. The effect of demographic questions on response rates to government surveys is difficult to predict and likely varies by context and demographic characteristic of interest. Based on research conducted by the Census Bureau, questions asking about sexual orientation and gender identity don’t significantly depress responses [112], but serious concern about the safety, security, and integrity of the Census does exist, particularly amongst racial and ethnic minority groups [81]. Finally, a 2018 study by the Census Bureau identified the proposed reintroduction of a citizenship question on the 2020 census as a “major barrier” to participation, due to the political discourse surrounding immigration, and fears of retaliation against specific ethnic groups by the government [140]. Multiple studies suggest that a citizenship question would induce significant non-response [65]. Other agencies like the Center for Medicare Services intend to explore the
impact of demographic questions on non-response and program participation, but this research is not yet complete [102].

Direct data collection demonstrates the challenge of public trust and privacy. Generalized distrust of the federal government, ongoing concerns about government surveillance, and perhaps, lack of public awareness of federal privacy protections, especially in comparison to the private sector’s lack of privacy regulation, all pose challenges to federal agencies navigating the requirements of the EO while maintaining public trust.

4.4 Fragmented Federal Infrastructure
A last major barrier to disparity assessments lies in the state of federal data infrastructure. Legacy systems, limited provisions for interoperability, lack of technical expertise, and administrative burdens can make data collection and sharing costly. Many scholars document the technical limitations that obstruct data sharing and linkage; O’Hara and Medalia specifically note a lack of staff, interoperability requirements, and over-specificity in funding “even when sharing is advantageous” [108].

One example of a deficit in technical infrastructure damaging data collection is the USDA’s failed attempt to update demographic data collection for agricultural lending through the Market Facilitation Program. Even though a 2011 departmental regulation prohibited employees from using visual observation to determine race and ethnicity, the USDA’s customer data management system continued to require that employees enter a value for demographic fields as late as 2019, so over two-thirds of race records for the program were still determined by employees’ assessments. After the USDA realized the flaws in their data management system, they committed to remediying them, but still noted that fully updating their data management to make race and ethnicity optional would take months [107].

The Veterans Affairs administration faces similar obstacles; despite a desire to evaluate their programs using demographic data, the VA lacks the technical, personnel, and financial resources to update their fragmented infrastructure. VA data is maintained by a range of data stewards, leading to what some University of California San Francisco researchers call a “sometimes-confusing alphabet soup of data partners” [24]. In response to a bill proposing mandatory data collection [62], the VA noted that while demographic data is already collected, funds should be directed towards “improving existing collection, storage, management and analytics efforts” [16]. Rather than investing in a new form collection process, the VA’s data officer calls for transforming the existing VA Profile system into a centralized data hub. The VA response to EO 13,985 recognizes that inconsistent data collection damages VA’s “ability to assess where potential disparities or barriers exist” and calls for a “Data for Equity strategy...that will synchronize VA’s data on health care, disability benefits, other veteran-facing services, and address data gaps in demographic information” [136]. Here, even with the desire to collect and use demographic data, a range of programs and data managers create a technical barrier.

The Commission on Evidence-Based Policymaking’s survey of federal agency employees found that variation in agencies’ technical infrastructure poses a significant challenge, noting specifically that agencies may struggle to “conduct disclosure reviews” and institute “disclosure avoidance protocols” [90, p.4] While statistical agencies are better equipped to collect, link, and analyze data while adhering to privacy standards, they are “less likely to view the purpose for which they collect data to be as a resource for evaluating programs” due to the restrictions of laws like CIPSEA, which limit disclosure of personally identifiable information for statistical agencies [90, p.4]. Beyond the well-documented technical and resource constraints on data management, bias assessment efforts can be specifically stymied by lacking technical infrastructure and expertise required to implement privacy protections.

5 SOLUTIONS
The problem at the heart of this paper is the privacy-bias tradeoff. Finding resolution inescapably requires a balance between how the U.S. government (a) protects individual privacy rights and (b) addresses structural problems of institutional bias. Ironically, the primary concerns motivating the passage of the Privacy Act—e.g., profiling and surveillance of individuals by the government—have proliferated in the private sector, providing a counterpoint of the perils of unchecked data collection and use [118]. We emphasize that our proposed solutions do not advocate for abandoning either data minimization or the Privacy Act. Congress amended the Act in 1988 with procedural safeguards to acknowledge the need of agencies to engage in some forms of record matching, while protecting privacy [118]. Similarly, our proposals attempt to enable the assessment of disparities in government programs while preserving the principles of the Privacy Act.

First, Congress should consider adding an exception to the Privacy Act that permits inter-agency record linkage specifically for bias assessment subject to the protections we suggest below. Alternatively, the Privacy Act’s exceptions for “statistical research” and “routine uses” [95] can be interpreted to subsume bias assessment, but such an interpretation could restrict the use of such data for programmatic improvement. As Xiang [147] notes, the UK’s Information Commissioner’s Office issued guidance that demographic data should be collected for bias mitigation. The UK Data Protection Act supports an exception to the E.U.’s GDPR to allow data collection for bias assessment “with a view to enabling...equality to be promoted or maintained” [11]. While the collection of demographic data may not be strictly required to administer a program, it is necessary to ensure fair administration and to discharge legal obligations under EO 13,985. The Privacy Act’s purpose specification requirement ([77, §§52(a)(c)(b)(C)]) would obligate an agency to disclose on a form the “principal purpose or purposes for which the information is intended to be used,” as well routine uses, which would supplant our fifth recommendation below. Inter-agency record sharing for bias assessment has the fewest methodological challenges of available approaches (see Table 1) and would solve the first order barrier for agencies to conduct disparity assessments.

Second, while such inter-agency data sharing would enable disparity assessments, we also recommend institutional protections to guard against misuse of demographic data. The internal “separation of functions” (e.g., between investigatory and adjudicatory functions) has long been a mainstay of administrative law [12, 36] and was one of the original recommendations from the 1973 Department of Health, Education, and Welfare report that preceded
the Act[110]. A similar internal separation of functions should be available only to offices conducting the disparity assessment, and such offices should be distinct from offices processing claims [83, 132]. This separation would be consistent with the Privacy Protection Study Commission’s conclusion that “no record … collected or maintained for a research or statistical purpose … may be used in individually identifiable form to make any decision or take any action directly affecting the individual to whom the record pertains” [100, 111]. For instance, Census demographic information could be made exclusively available to the Treasury Department’s Office of Tax Analysis, not IRS’s audit units, which is consistent with the current approach by Treasury [58]. Such separation of functions would insulate sensitive data from enforcement offices, building public trust and ensuring fair and equal treatment.

Third, to overcome substantial resource and data infrastructure challenges, Congress should increase support of initiatives like the NSDS [91], the NAIRR [63, 86], and other mechanisms to enable privacy-protecting sharing of administrative data for disparity assessments [90, 108]. The CHIPS and Science Act of 2022 funded a limited five-year trial of NSDS demonstration projects and the National Science Foundation has recently attempted to broker partnerships between academic researchers and agencies to implement EO 13,985 [88]. Such initiatives have significant potential to address data infrastructure, computing, and human capital gaps to conduct disparity assessments. Our case studies also revealed numerous instances where the apparent agency resistance stemmed from lack of technical resources to incorporate demographic data into agency systems. Congress and the President should explore mechanisms, such as GSA’s 18F consultancy, the U.S. Digital Corps, or the U.S. Digital Service, to provide technical assistance for IT modernization to incorporate demographic data collection and restrict access to teams requiring that information.

Fourth, Congress should amend the Paperwork Reduction Act to provide a streamlined process for capturing demographic data on federal forms or running auxiliary surveys. Particularly as Census and OMB update their data standards for race reporting, there is no need for each agency to undergo a separate OMB review process and notice and comment to collect race and ethnicity information in a manner already approved as a general data standard. To be sure, public input can be valuable, but procedural requirements can significantly impede the ability of agencies to collect information relevant to assessing racial disparities.

Fifth, in developing data strategies for disparity assessments, federal agencies should expressly address public concerns about forms, such as concerns about invasiveness and reduction of voluntary compliance [58, p.14-15]. Agencies should strategically select from the options enumerated in Table 1 to develop the most appropriate data strategy and communicate their rationale. For example, the USDA Food and Nutrition Service noted that programs “should continue explaining the importance of this data to participants as they encourage them to self-identify and self-report” [74]. Forms should clearly and simply explain how demographic data will be used and protected. For instance, if IRS were to collect race and ethnicity, it should clarify that such information would not be used to select audits.

Because our research reveals substantial institutional challenges, our recommendations focus on those dimensions. Privacy enhancing technologies such as differential privacy and secure multi-party computation are of course quite important here for enabling secure and private inter-agency data sharing, but we emphasize that they are unlikely a complete solution. Other agencies may follow the Census Bureau’s adoption of differential privacy in 2020 [18], but Drechsler [38] notes that public sector requirements (e.g., for reproducibility, final data users, and data sharing) can be “fundamentally different from [those] in industry.” Government data, for instance, is intended to be used over many decades, making the calculation of privacy budgets on a query system challenging. Privacy enhancing technologies may and should, of course, still be adapted consistent with our proposals that are aimed to enhance the current data deficit in demographic data for disparity assessments.

6 CONCLUSION

Nearly fifty years after the passage of the Privacy Act, the law remains both an exemplar of government privacy protections as well as a third rail in evolving privacy discussions. Over the years, the Act has been strengthened, and there are no serious discussions to weaken it. Ongoing concerns regarding the government’s efforts to purchase data about individuals from the private sector has led to calls to eliminate loopholes [121]. Data minimization as policy is broadly viewed as a success; proposed rulemaking by the Federal Trade Commission in 2022 [29] as well as proposed bipartisan privacy legislation both embraced its adoption by the private sector [119]. And yet, our analysis highlights weaknesses with this half-century experiment. Concerns about exposure and knowledge of individuals by the government has resulted in a lack of visibility into the impact of policymaking on subgroups. We achieved individual privacy at the expense of collective knowledge, yielding conditions ripe for allowing disparate impacts to proliferate unchecked.

ACKNOWLEDGMENTS

We thank the Public Interest Technology University Network (PIT-UN) for generous support and Dawson Verley for research assistance. We are grateful to Chris Hoofnagle for his helpful comments.

REFERENCES

1. [n. d.]. Questions and Answers Related to CACFP 11-2021, SFSP 07-2021 Collection of Race and Ethnicity Data by Visual Observation and Identification in the Child and Adult Care Food Program and Summer Food Service Program – Policy Rescission.


Appendices with detailed case studies are available in the online version of this paper.