



Statement on Mass Government Data Consolidation Efforts

June 2026

The United States Tech Policy Committee for the Association for Computing Machinery (ACM) expresses deep concern regarding recent efforts to consolidate [personal data](#), like demographics, personal income, public benefits utilization, personal health information, and more, from dozens of government agencies to create detailed, comprehensive profiles of individuals and use this information for purposes other than program administration.

In certain cases, limited, legal, and appropriate data sharing across government agencies can reduce administrative burden, enhance constituent experiences, improve coordination among agencies, enable research, and improve data quality; however, excessive data consolidation by government agencies diminishes public trust, increases significant security risks, and may violate the law.

As the premier global association of computing professionals, we find such initiatives raise serious ethical questions. Our Code of Ethics and Professional Conduct identifies many issues that should be considered before work begins, or in understanding the magnitude of what has been done.

ACM promotes the responsible use of computing through its published Code of Ethics and Professional Conduct. Responsible use includes adhering to ethical guidelines that avoid harm, respect privacy, and contribute positively to society and human well-being. Consolidating personal data by government agencies necessarily introduces risks to civil liberties and creates critical vulnerabilities that computing professionals have a duty to identify and address.

Ethical Principles at Stake

Our Code of Ethics establishes clear principles that should be considered in data consolidation efforts by government agencies:

Avoid Harm (Principle 1.2): Consolidating vast amounts of sensitive personal data creates what security experts recognize as a "single point of failure"—transforming what were once numerous, separate targets into a single, high-value prize for malicious actors and hostile foreign powers. The potential for harm from data breaches, system failures, and unauthorized access is not hypothetical, as [international case studies](#) from India, the Netherlands, Denmark, and Australia have demonstrated. Given how dangerous consolidation can be, computing professionals exhaust other methods before resorting to consolidation.

Respect Privacy (Principle 1.6): As ACM has [previously stated](#), personal information gathered for a specific purpose should generally not be used for reasons other than program administration without the person's consent, with targeted and limited exceptions (e.g. cooperation with an active investigation) For example, the Privacy Act of 1974, passed in the aftermath of the Watergate scandal, deliberately compartmentalized citizen data across agencies as a safeguard against government overreach and generally prohibits, except in limited circumstances, sharing personal information across agencies without the person's consent. Many federal and state laws that govern personal data collected and maintained by government agencies take a similar approach. Consolidation efforts that circumvent these protections violate this fundamental principle.

Be Honest and Trustworthy (Principle 1.3): Computing professionals should provide full disclosure of all pertinent system capabilities, limitations, and potential problems to appropriate parties. Systems that claim not to be "master databases" while functionally operating as such represent a violation of transparency and honesty. Any datasets containing sensitive material must include robust logs of who has permissions to said data, timestamps of when they access it, and what changes, if any, they make.

Give Comprehensive Evaluations of Risks (Principle 2.5): Computing professionals have a special responsibility to provide objective evaluations to the public. [Evidence](#) from other democracies shows that data consolidation, including for fraud detection, has led to false accusations, wrongful denial of benefits, and devastating consequences for vulnerable populations—particularly low-income families, ethnic minorities, and immigrants.

Design Robustly Secure Systems (Principle 2.9): Breaches cause significant harm. The great increase in attack surface created by data consolidation demands extraordinary security measures. Today, the federal government does not even allow the use of cloud-based password management systems – a basic protection. Extraordinary data consolidation requires extraordinary cybersecurity to protect personal data, and the federal government has [recently eliminated](#) much-needed resources aimed at strengthening state and local cybersecurity protections, raising doubts about whether government agencies can apply foundational cybersecurity practices like phishing-resistant multifactor authentication, password management tools, and only using software that is still supported and patched.

The Public Good Requires Careful Consideration, Public Discussion, and Deliberative Planning

Careful consideration, public discussion, and deliberative planning are vitally important for systems that are integrated into the infrastructure of society (Principle 3.7). Leaders in government have an added responsibility to be good stewards, establishing policies for fair system access and monitoring integration levels of these systems. Data consolidation that affects eligibility for benefits, immigration status, and fundamental rights requires the highest standards of care, transparency, and accountability, in addition to being accurate and reliable. Data consolidation should be seen as a last resort.



This consideration, public discussion, and deliberative planning should happen *before data are shared*, rather than after the fact. In fact, the harm from data consolidation is immediate and in many cases, irreparable.

When government agencies merge databases without robust safeguards, [data quality issues](#) lead to [incorrect determinations](#), [opaque systems prevent meaningful oversight and redress](#). Personal information collected for one purpose may be repurposed for surveillance and enforcement actions without public oversight or accountability, which could lead to large-scale abuses of power.

ACM's USTPC urges an immediate halt to any government data consolidation efforts and calls for an independent technical and ethical review before further implementation. Such a review must include:

- Comprehensive risk assessment by independent technical experts,
- Transparent disclosure of data sources, matching methodologies, and intended uses,
- Clear legal authority, accurate system of records notices (SORN), privacy impact assessments, and compliance with the Privacy Act,
- Robust mechanisms for individuals to access, correct, and challenge information,
- Meaningful oversight and accountability structures, and
- Public consultation and informed consent processes

Our Position

Advancements in government efficiency should not come at the expense of human dignity, autonomy, privacy, or safety. Computing professionals have both the expertise and the ethical obligation to ensure that the systems we build serve the public good rather than enabling irreparable harm.

USTPC urges policymakers to mandate the procedural safeguards, transparency measures, and independent oversight before any such systems are deployed or expanded.