The Protection of Data Privacy in Public Administration

Abstract

Public agencies increasingly collect, purchase, and link personal information to deliver services, manage programs, and evaluate outcomes. Without clear limits and transparent safeguards, these practices can weaken public trust, amplify inequities, and expose residents to harm. This expanded paper argues that government should adopt a stronger, ethics-forward and risk-based approach to data privacy grounded in the Privacy Act of 1974, contemporary constitutional jurisprudence, and widely accepted privacy frameworks. It expands upon these foundations by exploring the role of technology, the ethical responsibilities of administrators, and the integration of privacy frameworks into public decision-making. It concludes with practical policy recommendations for public managers to operationalize privacy as a core public value rather than a compliance checkbox.

Introduction

The U.S. public sector must do more to protect people's personal data in an age of rapid digital transformation. Government entities—from school districts and health departments to transportation agencies—routinely collect sensitive information and increasingly augment it with third-party datasets such as geolocation, biometric data, or commercial profiles to target services or evaluate performance. The digitization of public administration has created both opportunities and vulnerabilities. Residents are often unaware of the scope of these practices, which undermines legitimacy, transparency, and trust in government. Protecting privacy is not merely a technical issue but a public value central to democratic accountability. This expanded discussion examines the need for robust privacy governance frameworks within public administration to ensure accountability, procedural fairness, and ethical stewardship of personal data (Nissenbaum, 2004). When data are misused or inadequately safeguarded, citizens may lose confidence in the integrity of the institutions that serve them.

Public Administration Ethics and the Duty to Protect

Public administration is anchored in stewardship, accountability, and procedural fairness. An ethics-first perspective requires agencies to consider not only outcomes but also how data are acquired, processed, and shared. Nissenbaum's theory of contextual integrity explains that data practices can still be unjust when they violate the informational norms of a context, even if technically legal. This means that public administrators should assess whether data collection aligns with the public's expectations of privacy and the ethical duties of care that accompany administrative power. For instance, while an agency may lawfully analyze public health data, sharing those datasets with external contractors without meaningful consent or anonymization violates ethical expectations. Ethical stewardship requires intentionality and foresight—recognizing that data misuse can disproportionately harm marginalized populations, deepen inequities, or perpetuate surveillance. Therefore, administrators must approach privacy as a moral obligation embedded in the social contract between government and the governed (Solove, 2006). Ethical frameworks such as deontology and utilitarianism also offer valuable perspectives: deontological ethics emphasize duty and rules, while utilitarian reasoning evaluates the balance between benefits and harms. Public administrators should merge these ethical perspectives to ensure that data use advances collective welfare while respecting individual dignity.

Legal Foundations for Government Data Practices

Two major legal pillars shape public-sector privacy governance in the United States. The Privacy Act of 1974 regulates federal agencies' collection, maintenance, and dissemination of personal data, granting individuals rights of access and correction while restricting disclosure without consent (5 U.S.C. § 552a; U.S. Department of Justice, 2020). Although its provisions do not automatically extend to state or local governments, it establishes core fair-information principles that should guide all government entities. Additionally, landmark court cases such as Carpenter v. United States (2018) have extended constitutional privacy protections into the digital realm. In Carpenter, the Supreme Court held that prolonged government tracking of individuals' cell-site location data constitutes an unreasonable search without a warrant, emphasizing that privacy expectations persist even in technologically mediated environments. Public administrators should interpret these decisions as the ethical and legal floor—not the ceiling—for modern data practices. Moreover, new regulations like the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) illustrate global trends toward empowering citizens with data rights and mandating organizational accountability. Even if U.S. federal law lags behind, local agencies can voluntarily adopt similar standards as best practices for transparency and fairness.

Operational Risks in Modern Public Agencies

Public agencies face growing risks of mission creep, secondary data use, and equity violations. Mission creep occurs when data collected for one administrative purpose migrate into new analytic or enforcement contexts without renewed consent. Similarly, agencies increasingly purchase commercial datasets, believing this circumvents constitutional or statutory limits—a misconception that exposes them to ethical and reputational risks. For example, police departments and social services have purchased predictive analytics data from third parties that use social media or geolocation tracking, often without public oversight. Such actions may inadvertently target vulnerable groups or replicate historical biases, undermining the equity goals of public administration. Another emerging risk lies in algorithmic decision-making, where machine learning models are trained on biased datasets, leading to discriminatory outcomes in areas such as housing, benefits eligibility, and child welfare investigations. Therefore, administrators must implement privacy impact assessments, bias audits, and ethical review processes before adopting such technologies (Solove, 2006; Carpenter v. United States, 2018). Cybersecurity lapses also remain a serious operational concern. As seen in incidents involving health departments and unemployment agencies, a single breach can compromise the data of millions of citizens. Building public trust thus requires both ethical restraint and robust technical safeguards.

A Risk-Based Governance Model for Agencies

To operationalize privacy effectively, agencies can adopt the National Institute of Standards and Technology (NIST) Privacy Framework, which aligns privacy with enterprise risk management models already familiar to public managers (NIST, 2020). The framework's core functions—Identify, Govern, Control, Communicate, and Protect—guide organizations in understanding their data flows, evaluating risks, and communicating practices transparently. Integrating these steps into daily operations allows agencies to embed privacy protections into their workflows rather than treat them as one-time compliance activities. For example, the 'Identify' phase involves cataloging all personally identifiable information (PII) holdings, while the 'Control' and 'Protect' stages focus on technical safeguards and access controls. By framing privacy as a continuous process, public managers can align ethical duties with measurable performance indicators. This proactive approach also helps agencies prepare for potential data breaches or legislative changes, ensuring resilience and adaptability. Training programs and interagency collaboration further enhance privacy culture, making it a shared responsibility across departments rather than a specialized concern of IT personnel.

Policy Recommendations for Public Managers

Public managers can implement the following strategies to institutionalize data privacy as a governance priority:

1. Codify purpose limitation and data minimization: Programs must clearly define why data are collected and restrict reuse outside that purpose.
2. Implement privacy impact assessments: Before deploying new data systems or algorithms, assess ethical, legal, and equity risks.
3. Strengthen transparency: Provide public dashboards or reports detailing what data are collected, how they are used, and with whom they are shared.
4. Stablish accountability mechanisms: Designate privacy officers and require annual compliance audits and public disclosures.
5. Invest in training and capacity building: Equip staff with the knowledge to manage privacy responsibly.
6. Foster interagency collaboration: Share lessons learned and harmonize privacy practices across jurisdictions.

These actions help ensure that data governance reflects democratic values and reinforces the public’s trust. They also transform privacy from a reactive obligation into a proactive leadership function that supports both innovation and accountability.

Conclusion

Protecting data privacy is both an ethical obligation and a strategic necessity for modern governance. Public administrators must integrate privacy considerations into every stage of policymaking, from design to implementation. As technology continues to reshape service delivery, governments have an opportunity—and a responsibility—to ensure that innovation does not come at the expense of citizen rights. By grounding data practices in ethical theories, legal precedent, and structured governance frameworks, agencies can safeguard residents' information, strengthen institutional legitimacy, and maintain the trust essential for democratic governance. Ultimately, privacy protection must evolve alongside public administration itself, serving as a compass that guides agencies toward transparency, fairness, and respect for human dignity.

References

Carpenter v. United States, 585 U.S. ___ (2018).

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1), 119–157.

NIST. (2020). NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. National Institute of Standards and Technology.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–560.

U.S. Department of Justice. (2020). Overview of the Privacy Act of 1974. Office of Privacy and Civil Liberties.