

***User Rights Without Remedies:  
Transparency, Redress, and the Structural  
Limits of U.S. Data Privacy Governance***

**Anna Templeton**

*Master of Arts in Policy Studies*

*School of Interdisciplinary Arts & Sciences*

*Advisor: Jin-Kyu Jung*

*Second Reader: Keith Nitta*

*August 17, 2026*

## ***I. ABSTRACT***

This capstone examines whether the U.S. sectoral approach to data privacy provides users with genuine transparency, control, and redress over personal data, using the European Union's General Data Protection Regulation (GDPR) as a comparative benchmark. A convergent mixed-methods design combines secondary analysis of the Pew Research Center's 2023 American Trends Panel (N = 5,101) with semi-structured interviews with five professionals in data governance, privacy consulting, and corporate technology. Quantitative results show that perceived personal agency over data is positively associated with trust in companies, while concern about data misuse is negatively associated with it. Interview findings show that consent functions as a compliance exercise rather than a substantive protection, that trust tracks a company's business model more than its stated policies, and that redress remains structurally inaccessible even to professionals with direct expertise in the field. The study concludes that U.S. procedural protections exist on paper but are difficult to interpret, exercise, or enforce in practice, and proposes federal legislation modeled on the GDPR.

## ***II. ACKNOWLEDGEMENTS***

I would like to thank Professor Jin-Kyu Jung, my capstone advisor, for his eagerness to engage with the subject of data privacy and for the expertise and guidance he offered throughout the research and writing process. I am equally grateful to Professor Keith Nitta, who served as my second reader and as Graduate Director of the Master of Arts in Policy Studies program, for his support and thoughtful feedback at each stage of this project. I am also grateful to Professor Charlie Collins for his guidance in cleaning the Pew Research Center dataset and in documenting statistical analysis appropriately, and to Professor Martha Groom for her help with the research design process and her editing guidance. Thank you to Bruce Kochis, Senior Lecturer (Retired), for teaching me how to be a good writer and for helping me find pride and ownership in my own authentic work. Finally, thank you to Stephanie Lê, Graduate Programs Manager, who has been an excellent academic advisor and mentor throughout this program, and who has become a friend along the way.

I am deeply grateful to the five professionals who participated in this study's interviews. Each generously gave their time to share their lived experience navigating data privacy in both their personal and professional lives, offering insight that no dataset alone could have provided. This capstone would not have been possible without their willingness to speak candidly about their experiences with data privacy.

### **III. TABLE OF CONTENTS**

|       |                                                                                              |    |
|-------|----------------------------------------------------------------------------------------------|----|
| I.    | Abstract .....                                                                               | 2  |
| II.   | Acknowledgments .....                                                                        | 3  |
| III.  | Table of Contents .....                                                                      | 4  |
| IV.   | Glossary of Key Terms .....                                                                  | 6  |
| V.    | Introduction .....                                                                           | 8  |
|       | A. Research Question                                                                         |    |
|       | B. Sub-Questions                                                                             |    |
|       | C. Hypotheses                                                                                |    |
| VI.   | Statement of Problem .....                                                                   | 10 |
| VII.  | Purpose of Study .....                                                                       | 11 |
| VIII. | Review of Literature .....                                                                   | 13 |
|       | A. The Structural Foundation: U.S. and EU Privacy Frameworks in Conflict                     |    |
|       | B. When Rights Exist on Paper: Enforcement Gaps in U.S. and Transnational Privacy Governance |    |
|       | C. The Limits of Notice and Consent: When Transparency Stops Working                         |    |
|       | D. Municipal Data Governance and the One Seattle Data Strategy                               |    |
|       | E. The Missing Perspective: User Experience in Privacy Governance Research                   |    |
| IX.   | Methodology .....                                                                            | 22 |
|       | A. Quantitative Component                                                                    |    |
|       | 1. Data Source                                                                               |    |
|       | 2. Variables                                                                                 |    |
|       | 3. Analytic Strategy                                                                         |    |
|       | B. Qualitative Component                                                                     |    |
|       | 1. Sample and Recruitment                                                                    |    |
|       | 2. Ethics and Procedures                                                                     |    |
|       | 3. Interview Structure                                                                       |    |
|       | 4. Analytic Strategy                                                                         |    |
| X.    | Limitations .....                                                                            | 28 |
| XI.   | Findings .....                                                                               | 30 |
|       | A. Quantitative Findings: Pew American Trends Panel Analysis                                 |    |
|       | B. Qualitative Findings: Semi-Structured Expert Interviews                                   |    |
|       | 1. Theme 1: Consent as Performative                                                          |    |
|       | 2. Theme 2: Business Model as the Primary Trust Signal                                       |    |
|       | 3. Theme 3: Privilege Gap — Privacy as a Purchasable Good                                    |    |
|       | 4. Theme 4: EU vs. U.S. Framing — Fundamental Right vs. Fragmented System                    |    |
|       | 5. Theme 5: Perceived Threats and Structural Vulnerability                                   |    |
|       | 6. Theme 6: Calls for Structural Reform                                                      |    |
| XII.  | Conclusion .....                                                                             | 40 |

|       |                                               |    |
|-------|-----------------------------------------------|----|
| XIII. | Recommendations .....                         | 42 |
| XIV.  | Appendix .....                                | 44 |
|       | A. Data Preparation and Variable Construction |    |
|       | B. Interview Recruitment Email                |    |
|       | C. Interview Opening Script                   |    |
|       | D. Interview Questions                        |    |
| XV.   | Bibliography .....                            | 50 |

#### ***IV. GLOSSARY OF KEY TERMS***

**Sectoral regulation:** The U.S. approach to data privacy, which governs personal data through separate laws tied to specific industries or populations — health data, children's data, one state's residents — rather than a single law covering all personal data. This structure leaves gaps wherever data falls outside any one sector's scope.

**GDPR (General Data Protection Regulation):** The European Union's data protection law, which treats control over personal data as a fundamental right belonging to the individual, enforceable against both government and private companies.

**Adequacy decision:** A formal determination by the European Commission that a non-EU country's data protections meet the EU's legal standard, allowing personal data to be transferred there without additional safeguards.

**Schrems I and Schrems II:** Two rulings by the Court of Justice of the European Union, in 2015 and 2020, that struck down the two prior U.S.-EU data transfer agreements for failing to guarantee EU-level privacy protections once data left European jurisdiction.

**Data Privacy Framework (DPF):** The current U.S.-EU data transfer agreement, adopted in 2023 as the third attempt at an adequacy arrangement after Schrems I and Schrems II invalidated its predecessors.

**Privacy self-management:** Solove's term for the U.S. privacy model, which places responsibility for protecting personal data on the individual through notice and consent, rather than through binding rules that govern how companies handle data regardless of what a user agrees to.

**Contextual integrity:** Nissenbaum's framework for understanding privacy violations — not as any disclosure of information, but as information moving outside the context in which it was originally shared. Sharing health data with a doctor is expected; that same data reaching an employer is not, even though no new disclosure occurred.

**Redress:** The ability to formally contest, correct, or seek remedy when personal data has been misused, beyond simply being notified that misuse occurred.

**FTC consent order:** A negotiated settlement in which a company agrees to specific data practices following an FTC enforcement action, used in place of upfront regulatory requirements set before harm occurs.

**Purposive sampling:** A qualitative sampling method that deliberately selects participants for relevant expertise or experience, rather than drawing from the population at random.

**Composite variable:** A single measure built by averaging two or more related survey items, used to capture a broader concept than any one item could measure alone. This study builds two: Personal\_Agency and Concern\_Misuse.

**OLS regression:** A statistical method used to test whether one or more factors predict an outcome, while holding other variables constant.

**IRB exempt status:** A determination by a university's ethics review board that a study involving human participants carries minimal risk and does not require full committee review before proceeding.

## ***V. INTRODUCTION***

Despite the exponential growth of data-driven technologies, users in the United States lack enforceable rights over how their personal data is collected, processed, and shared. U.S. frameworks emphasize procedural mechanisms — transparency, notice, and accountability — but it remains unclear whether these translate into genuine user knowledge, perceived control, or accessible redress in practice. This gap is thrown into relief by the European Union's General Data Protection Regulation, which frames data protection as a fundamental right and embeds transparency, access, correction, and redress into enforceable legal obligations. That contrast reframes U.S. data privacy failures as failures of democratic and procedural rights, with direct implications for how domestic reform is debated and how EU–U.S. adequacy disputes are understood.

This study addresses the gap between formal governance commitments and lived user experience by examining whether current frameworks substantively operationalize user rights, rather than merely articulate them.

### **Research Question**

To what extent does the U.S. sectoral data privacy system provide users with meaningful knowledge, transparency, and redress over personal data practices, and how are these procedural protections interpreted and experienced in practice?

### ***Sub-Questions***

1. How do U.S. privacy laws and enforcement mechanisms conceptualize user rights to transparency, access, correction, and redress?
2. How do users interpret transparency and control over personal data in practice?
3. What factors shape user trust in companies that manage personal data?
4. How do users perceive their ability to respond to or challenge data misuse?

### **Hypotheses**

This study tests the following hypotheses:

- H1: Lower perceived understanding of corporate data practices is associated with lower trust in companies that manage personal data.

- H2: Lower perceived control over personal data is associated with lower trust in institutions responsible for data governance.

These hypotheses assess whether procedural elements of privacy governance — particularly transparency and control — are directly associated with institutional trust.

## ***VI. STATEMENT OF PROBLEM***

In the United States, data privacy functions more as a privilege than a right. It is accessible to those with the resources, knowledge, and capacity to navigate a fragmented system, but it is not guaranteed to anyone as a matter of entitlement (Schwartz, 2013; Pew Research Center, 2023). Where the European Union grounds data protection in constitutional guarantees enforceable against both government and private actors, the U.S. system has historically emphasized notice, consent, and sector-specific accountability mechanisms — formal obligations that do not amount to guaranteed individual rights (Schwartz, 2013). That contrast is not merely jurisdictional; it reframes U.S. data privacy failures as failures of democratic and procedural rights, with direct implications for how domestic reform is debated and how EU–U.S. adequacy disputes are understood.

The practical consequence is a governance architecture in which transparency is required but not designed to produce understanding (Solove, 2013), consent is obtained but not designed to be authentic (Solove, 2013; Nissenbaum, 2009), and redress is formally available but structurally difficult to access (Kuner, 2015; Qing, 2022). That is the problem this study investigates: not whether these protections exist on paper, but whether they function for the people they are meant to protect.

## ***VII. PURPOSE OF STUDY***

This distinction is a predictable consequence of a system built around institutional compliance rather than individual entitlement (Kempeneer, 2021). Unlike the European Union, which enforces data protection commitments through independent regulatory bodies with sanctioning authority, the U.S. system distributes regulatory responsibility across sector-specific statutes, state-level frameworks, and Federal Trade Commission enforcement actions that respond to documented harm rather than to preventing harm (Qing, 2022). The Court of Justice of the European Union has repeatedly invalidated U.S.-EU data transfer frameworks — striking down Safe Harbor in 2015 and Privacy Shield in 2020 — with the current Data Privacy Framework facing similar legal scrutiny (European Commission, 2023; Schrems I, 2015; Schrems II, 2020). Each ruling reflects the same judicial finding: procedural infrastructure without independent, binding enforcement does not constitute adequate protection. That pattern speaks directly to how individuals in the United States experience their privacy rights: formal protections exist, but the mechanisms for exercising them are institutional rather than individual, leaving most people with no clear path to enforcement (Kuner, 2015; Qing, 2022).

When a governance system does not treat data as fundamentally belonging to the person it concerns, consent becomes procedural rather than authentic (Solove, 2013). Transparency becomes a compliance exercise rather than a tool that individuals can actually use (Kempeneer, 2021). Redress exists on paper but remains structurally inaccessible to those who need it most (Kuner, 2015; Qing, 2022). These are predictable outcomes of a system designed around the wrong unit of analysis — one that centers institutions and data flows rather than the individuals those institutions are supposed to serve.

Existing scholarship has mapped the legal architecture of these governance failures (Schwartz, 2013; Bignami & Resta, 2015), traced enforcement gaps (Kuner, 2015), and analyzed regulatory design (Qing, 2022), but has largely left unexamined how individuals interpret and experience procedural privacy rights in practice. Where user experience appears in the literature, it is often examined at the platform or behavioral level rather than at the governance level (Hargittai & Marwick, 2016; Pew Research Center, 2023). National survey data suggest that public understanding of corporate data practices is declining — 67% of U.S. adults reported understanding little to nothing about what companies do with their personal data in 2023, up from 59% in 2019 (Pew Research Center, 2023) — yet that data alone cannot explain why this

decline persists or what it means for how individuals experience their privacy rights in practice. Hargittai and Marwick (2016) find that young adults understand privacy risks and engage in protective behaviors, yet feel that once data are shared, it is effectively beyond their control — attributing this to unclear institutional practices and platform design. That finding is suggestive but limited in scope: it does not examine whether governance frameworks themselves are structured in ways that produce that loss of control, nor does it extend to the broader population or to those with professional experience inside data governance systems.

This project examines whether transparency disclosures produce genuine understanding, whether perceived control over personal data corresponds with trust in companies that manage it, and whether redress feels accessible or effectively out of reach for the individuals it is designed to protect. To examine these questions, this project uses a mixed-methods convergent design combining secondary quantitative analysis of nationally representative survey data with semi-structured qualitative interviews with professionals in technology, data governance, and privacy policy, following Creswell and Plano Clark's (2018) convergent framework. This approach contributes empirical, direct evidence to a literature that has approached these dynamics primarily through institutional and legal analysis.

## ***VIII. REVIEW OF LITERATURE***

The European Union enshrines data privacy as a fundamental right (Charter of Fundamental Rights of the European Union, 2000/C 364/01, Art. 8), meaning that personal data belongs to the person it concerns, not to the market or the state. In the United States, data privacy functions more as a privilege. It is accessible to those with the resources, knowledge, and capacity to navigate a fragmented system, but it is not guaranteed to anyone as a matter of right. That distinction is not a technicality. It is the foundation of a three-decade-long transatlantic data governance conflict.

That divergence has generated three decades of scholarship on legal architecture (Schwartz, 2013; Bignami & Resta, 2015), regulatory design (Qing, 2022), and enforcement gaps (Kuner, 2015) — but has left largely unexamined how individuals actually experience those protections in practice. Where user experience appears, it is often inferred from governance outcomes rather than examined directly. How individuals actually understand their privacy rights, whether they perceive meaningful control over their data, and whether redress feels accessible or abstract across federal, municipal, and transnational contexts remains largely unexamined in the existing literature. That is the gap this study addresses.

### **The Structural Foundation: U.S. and EU Privacy Frameworks in Conflict**

Any examination of data privacy governance must begin with the foundational divergence between the American and European approaches to privacy as a legal and political concept. This divergence is not a matter of degree but of kind — rooted in different constitutional traditions, different relationships between the state and the market, and different understandings of what kinds of power privacy is meant to constrain.

Schwartz (2013) provides the most influential account of this divergence, distinguishing between European "dignity-based" privacy and the American tradition of privacy as protection from state intrusion. In the European model, privacy is a fundamental right secured against both government and private actors, embedded in constitutional documents and enforceable through independent judicial and regulatory bodies. In the American model, privacy has historically meant freedom from government surveillance, with the private sector granted broad latitude to collect, process, and share personal data subject only to sector-specific statutory limits. Schwartz argues that this difference is not merely philosophical but structural — it shapes the design of

regulatory institutions, the scope of individual rights, and the conditions under which cross-border data governance is possible. He demonstrates that transparency and accountability are often formalized in U.S. frameworks, but without the procedural infrastructure needed to make them protective in practice. This finding anchors several of the analyses reviewed later in this chapter.

Bignami and Resta (2015) extend this structural argument by situating EU-U.S. privacy disputes within a broader pattern of regulatory conflict between incompatible constitutional and institutional systems. Their analysis shows that transatlantic data transfer frameworks have repeatedly attempted to manage this conflict through administrative accommodation — creating mechanisms that allow data flows to continue without resolving the underlying constitutional incompatibility between the two systems. The result, they argue, is a cycle of provisional frameworks that satisfy neither system's core commitments and therefore remain perpetually vulnerable to legal challenge. Their contribution is significant because it reframes the transatlantic privacy conflict not as a coordination problem, receptive to negotiation and compromise, but as a constitutional incompatibility that is far more difficult to resolve through policy instruments alone. For the present study, this reframing is significant. If the gap between formal protection and practical accessibility is structural rather than incidental, its effects should be visible in how users experience those protections on the ground.

This structural incompatibility has produced concrete and recurring legal ruptures that illustrate the limits of administrative accommodation in practice. In *Schrems I* (CJEU, 2015), the Court of Justice of the European Union invalidated the U.S.-EU Safe Harbor framework, holding that U.S. surveillance practices and the absence of effective judicial redress failed to provide the "essentially equivalent protection" required under EU law. The decision was explicit: adequacy cannot rest on political assurances or administrative oversight alone (*Schrems I*, 2015). In *Schrems II* (CJEU, 2020), the Court reached the same conclusion regarding the Privacy Shield framework, reaffirming that oversight mechanisms lacking genuine independence and binding authority do not satisfy the EU's constitutional standard for data protection. Across both rulings, the Court's reasoning is consistent. The Court treats redress as essential to adequate protection, yet it is persistently addressed as secondary in U.S. frameworks (*Schrems I*, 2015; *Schrems II*, 2020). A framework that offers transparency without the procedural infrastructure to support it is not just incomplete. It is structurally compromised at its core (Schwartz, 2013).

The current EU-U.S. Data Privacy Framework (DPF), adopted in 2023 following Executive Order 14086, represents the third iteration of this cycle. The European Commission concluded that new safeguards — including proportionality standards for intelligence collection and the establishment of a Data Protection Review Court — satisfied the "essentially equivalent protection" standard (Commission Implementing Decision 2023/1795). However, early assessments from the European Data Protection Board and civil society organizations have argued that the DPF reproduces the same structural vulnerability as its predecessors: it rests on executive-branch commitments rather than statutory reform, and leaves intact the underlying surveillance authorities — particularly Section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333 — that the CJEU has repeatedly scrutinized (European Data Protection Board, 2023; NOYB – European Center for Digital Rights, 2023). NOYB already announced its intention to challenge the DPF before the CJEU, raising the prospect of what observers informally termed "Schrems III." Schwartz (2013) and Bignami and Resta (2015) identify structural tensions that successive frameworks have deferred rather than resolved.

This history is what makes the present study necessary. If the foundational divergence between U.S. and EU privacy frameworks means that procedural protections are repeatedly formalized without being made reliably enforceable, then the question of how individual users experience those protections becomes both more urgent and more difficult to answer from the existing legal literature alone. The structural scholarship reviewed here explains the governance conditions that shape user experience; it does not examine what that experience looks like in practice.

### **When Rights Exist on Paper: Enforcement Gaps in U.S. and Transnational Privacy Governance**

A second body of scholarship shifts attention from constitutional architecture to enforcement, examining how procedural privacy rights perform in practice, independent of how they are articulated in law. This literature consistently finds that the gap between formal protection and practical accessibility is wide, and that the mechanisms designed to close it are frequently insufficient.

Kuner (2015) examines this problem in the transnational context. His work demonstrates that even where substantive data protection rights exist on paper, jurisdictional fragmentation —

the difficulty of applying any single regulatory authority across multiple legal systems — systematically undermines individuals' ability to exercise those rights. Weak extraterritorial enforcement means that data transferred across borders enters a legal environment where the protections nominally attached to it may be unenforceable in practice. Kuner's central contribution is to reframe the adequacy debate: the question is not only whether formal protections exist, but whether the institutional infrastructure needed to activate them is realistically available to individuals who need to use them. His analysis shifts attention from legal design to legal access, revealing a consistent gap between the protections frameworks promise and those they can realistically deliver to individuals.

Qing (2022) applies a parallel critique to the U.S. domestic context, examining the Federal Trade Commission's (FTC) role as a *de facto* privacy regulator in a system lacking a federal omnibus privacy statute. Because the FTC operates primarily through post hoc enforcement actions and negotiated consent orders rather than through proactively defined user-facing rights, the protection it offers is reactive and institutional rather than anticipatory and individual. Users are nominally protected by FTC oversight, but the mechanism of that protection operates at the institutional level — enforcement actions follow documented harm rather than providing structural guarantees that prevent it. Qing argues that this design is not incidental but structural: it reflects the sectoral, market-oriented nature of U.S. privacy governance, in which regulatory legitimacy is maintained through institutional activity while user-facing remedies remain largely theoretical. His analysis helps explain why individuals may have difficulty identifying concrete mechanisms for challenging data practices, even within a system that formally maintains oversight functions.

Both Kuner (2015) and Qing (2022) point toward the same underlying problem: the institutional distance between the bodies that hold privacy authority and the individuals whose data that authority is meant to protect. Kuner (2015) and Qing (2022) suggest this distance extends beyond procedural inconvenience; it is a governance design feature that determines whether privacy rights function as genuine entitlements or nominal commitments. For this capstone, this scholarship raises a foundational empirical question: if enforcement gaps and institutional distance are as significant as these scholars suggest, what does that mean for public trust in the institutions responsible for data governance?

## **The Limits of Notice and Consent: When Transparency Stops Working**

The failure of transparency in data governance is not simply a design problem. It is a predictable consequence of building privacy protection around individual consent. In the United States, the dominant regulatory approach places the burden of privacy protection on the individual. Daniel Solove (2013) calls this "privacy self-management": the law provides notice, access, and consent rights, and once a user clicks agree, those choices legally legitimize almost any downstream data practice. The problem, as Solove documents, is that this model is being asked to do far more than it can. A complex data ecosystem with lengthy privacy policies and unpredictable downstream uses leaves users unable to evaluate the consequences of their consent decisions. Solove (2013) argues that consent serves as the mechanism by which companies seek legal protection rather than as the means by which users exercise real control. Tim Wu's (2016) account of the "attention economy" extends this critique from consent design to business incentive: platforms are structurally motivated to maximize engagement and data extraction precisely because user attention, not the product itself, is what generates revenue — a dynamic that helps explain why consent mechanisms remain thin even as they proliferate.

Helen Nissenbaum's (2009) framework of contextual integrity helps explain why this failure runs deeper than information overload. Nissenbaum argues that privacy is not fundamentally about secrecy — it is about information flowing in ways that match the norms of the context in which it was originally shared. When you share health information with a doctor, you expect it to flow to other treating physicians, not to insurers or employers. The violation is not that information moved, but that it moved in ways that broke the contextual expectations under which it was given. Applied to data governance, this framework reveals a structural problem with consent-based systems: consent is obtained in one context — a sign-up screen, a cookie banner, a terms-of-service agreement — while data flows into entirely different contexts. The contextual norms users assume when sharing their data do not align with the legal protections and transparency the governance system actually provides (Nissenbaum, 2009).

Together, Solove (2013) and Nissenbaum (2009) establish that the consent architecture underlying U.S. data governance does not fail due to user inattentiveness. It fails because the framework itself does not produce genuine user understanding or control.

Kempeneer (2021) makes this structural failure visible at the institutional level. Her analysis of transparency initiatives in public-sector data governance finds that these initiatives

routinely assume that making information visible is sufficient to produce accountability. The same logic makes notice-and-consent seem like a privacy solution when it is not sufficient, and instead functions more as a liability shield (Kempeneer, 2021). Effective accountability requires not just disclosure but the procedural conditions that allow individuals to interpret, challenge, and act on what they are told. Without accessible redress mechanisms (Kuner, 2015) and genuine institutional responsiveness, transparency becomes a governance performance rather than a governance function. Individuals can observe that governance is occurring, but cannot participate substantively in shaping it.

König (2021) finds the same pattern in smart city governance. Municipalities adopt data ethics frameworks and participatory language, while the governance structures underneath remain managerial and technocratic, limiting genuine public oversight. Accountability gets framed as an internal administrative commitment rather than an acknowledgment and protection of a right belonging to the people whose data is being used. What König adds to Kempeneer's analysis is a warning about scale: as cities become significant data collectors across housing, transportation, and public safety, the gap between ethical language and enforceable rights has real consequences for people who interact with public services and lack viable alternatives.

Wu (2023) applies this critique directly to U.S. municipalities. Across a range of local governments, Wu documents wide variation in how cities define transparency and accountability in data use — but a consistent pattern: those commitments reside within institutional governance structures rather than in mechanisms that residents can actually access. The same pattern appears across federal regulatory frameworks and transnational adequacy debates wherever data governance prioritizes institutional management without accounting for individual rights (Schwartz, 2013; Qing, 2022).

The sectoral character of U.S. privacy law identified by Schwartz (2013) and Qing (2022) is embodied in three federal and state statutes central to this fragmentation: the Health Insurance Portability and Accountability Act (HIPAA, 1996), which governs health data disclosure but leaves most non-medical personal data untouched; the Children's Online Privacy Protection Act (COPPA, 1998), which imposes parental-consent requirements on data collection from children under 13 but does not extend meaningfully to adolescents; and the California Consumer Privacy Act (CCPA, 2018), a state-level statute often cited as the closest U.S. analogue to the GDPR, but one whose protections do not extend automatically to residents outside California. Together,

these statutes illustrate the sectoral, jurisdiction-bound structure that Qing (2022) identifies as characteristic of U.S. privacy governance — protection exists, but only within narrow, non-overlapping domains, leaving significant gaps for data that falls outside any single statute's scope.

### **Municipal Data Governance and the One Seattle Data Strategy**

The dynamics identified by Kempeneer (2021), König (2021), and Wu (2023) at the conceptual and comparative levels are evident in Seattle's One Seattle Data Strategy, which this capstone engages as a local policy case that aligns with those broader patterns. Published in 2023, the One Seattle Data Strategy outlines how the City of Seattle intends to coordinate data collection, management, and use across city departments to improve decision-making, equity, and public service delivery. The strategy identifies commitments to data quality and governance, data literacy and culture, equity analysis, and increased accountability and transparency (City of Seattle, 2023).

Reviewed as a governance document, however, the One Seattle Data Strategy reflects the pattern Wu (2023) identifies across U.S. municipalities. Its transparency and accountability commitments are articulated as internal governance standards rather than enforceable individual rights. The strategy does not define concrete mechanisms through which Seattle residents can access information about how their data is used, correct inaccuracies, or seek redress for harms arising from data practices. In this respect, it functions less as a user-rights framework and more as an institutional accountability plan. This approach aligns with the broader finding in the municipal governance literature that local data strategies tend to prioritize internal coordination over external accountability to residents (Wu, 2023; König, 2021).

The One Seattle Data Strategy is included to provide local context. The individuals interviewed for this study reside in the Seattle area, and the strategy offers a concrete illustration of how the federal patterns identified in this literature — transparency commitments without enforceable individual rights, and accountability framed institutionally rather than individually — also appear at the local level. The gap between stated transparency goals and the practical availability of procedural rights is not unique to federal or transnational governance. It is visible in Seattle, too. Most recently, the City of Seattle's 2025–2026 AI Plan extends this framework into AI governance, articulating commitments to transparency, bias mitigation, and explainability

while continuing to frame accountability as an internal governance function rather than a set of enforceable rights available to residents (City of Seattle, 2025).

### **The Missing Perspective: User Experience in Privacy Governance Research**

Across federal, transnational, and municipal contexts, the literature reviewed in this chapter consistently finds that governance frameworks articulate commitments to transparency, accountability, and redress (Schwartz, 2013; Kuner, 2015; Qing, 2022; Wu, 2023). What they do not consistently provide is the procedural infrastructure that would make those commitments accessible to the individuals they are supposed to protect (Kempeneer, 2021; König, 2021).

The literature reviewed here is primarily concerned with formal institutional design — what frameworks say, what courts have ruled, and what regulatory agencies have done (Schwartz, 2013; Bignami & Resta, 2015; Kuner, 2015). How ordinary users understand their privacy rights, whether they perceive genuine control over their personal data, and whether redress feels accessible or abstract remains largely outside its scope (Solove, 2013; Nissenbaum, 2009; Pew Research Center, 2023). Pew Research Center (2023) data suggest that the gap is already visible in public perception—67% of U.S. adults reported understanding little to nothing about what companies do with their personal data.

The existing literature has also largely left unaddressed a distributional dimension to this gap. Structural critiques of privacy governance tend to focus on aggregate institutional failures without examining how the consequences of those failures are distributed across different populations (Solove, 2013; Pew Research Center, 2023). The distance between formal privacy rights and practical user experience is not evenly distributed — individuals with fewer resources, lower digital literacy, or greater exposure to data-intensive public systems are likely to experience this gap most acutely (Pew Research Center, 2023). This study does not directly address that distributional dimension. The qualitative sample is limited to professionals with experience in technology, data governance, and privacy policy. It does not include representation from the vulnerable or marginalized populations most likely to bear the costs of governance gaps — a recognized limitation discussed further in the methodology section. This project addresses the experiential gap more broadly: whether users who regularly interact with data systems perceive transparency, control, and redress as accessible in practice. The Pew Research Center's

(2023) American Trends Panel provides a nationally representative baseline for those patterns, and in-depth expert interviews provide interpretive depth that survey data alone cannot capture.

## ***IX. METHODOLOGY***

This project uses a mixed-methods research design combining secondary quantitative analysis with semi-structured qualitative interviews to examine whether procedural data privacy rights—transparency, knowledge, and access to redress—are accessible in practice. This approach is grounded in Creswell and Plano Clark's (2018) convergent mixed methods framework, in which quantitative and qualitative strands are collected and analyzed in parallel, then integrated to produce a more complete account than either method could provide alone.

### **Quantitative Component**

#### *Data Source*

This study drew on publicly available data from the Pew Research Center's 2023 American Trends Panel (Wave 127), a nationally representative survey of 5,101 U.S. adults conducted May 15–21, 2023. The American Trends Panel is a probability-based online panel; Wave 127 focused on public perceptions of data privacy, including how Americans understand corporate data practices, their sense of control over personal information, their trust in companies and institutions managing data, and their attitudes toward AI and data regulation. Respondents were recruited through address-based sampling and completed the survey online. The unit of analysis is the individual survey respondent. Five variables were selected from the dataset for analysis.

#### *Variables*

Two variables were drawn directly from the dataset as individual measures. Perceived\_Control (CONTROLCO\_W127) operationalized respondents' felt sense of control over the data companies collect about them, measured on a four-point scale ranging from 1 (not at all) to 4 (a great deal). Perceived\_Understanding (UNDERSTANDCO\_W127) operationalized respondents' self-reported understanding of what companies do with the data they collect and was measured on the same four-point scale. These two variables served as the primary operationalizations of the transparency and control dimensions central to H1 and H2.

Two composite variables were then constructed by averaging pairs of theoretically related items. Personal\_Agency was constructed as the mean of Perceived\_Control (CONTROLCO\_W127) and Perceived\_Understanding (UNDERSTANDCO\_W127). These two

items were combined because perceived control and perceived understanding together capture whether respondents felt genuine agency over their personal data, rather than either dimension in isolation. Concern\_Misuse was constructed as the mean of two items: CONCERNCO\_W127 ("How concerned are you about how companies are using the data they collect about you?") and PRIVWRY\_b\_W127 ("How worried are you about companies selling your information to others without you knowing?"). These items were combined because both reflect concern about corporate misuse or unauthorized use of personal data; together, they produced a more reliable measure of that construct than either item alone. Both composites were calculated as simple means, reflecting the assumption that the two contributing items carry equal theoretical weight within each construct. All component items were direction-coded so that higher values consistently indicate more of the construct being measured — greater agency in the case of Personal\_Agency, and greater concern in the case of Concern\_Misuse. Given the exploratory nature of this study and the two-item composition of each composite, formal reliability statistics (e.g., Cronbach's alpha) were not calculated; however, both composites were constructed based on conceptual alignment between items, consistent with common practice in exploratory survey research.

Trust\_in\_Companies (AIPRIV3\_W127) — "How much do you trust companies to make responsible decisions about how they use AI in their products?" — served as the dependent variable for both H1 and H2. It was measured on a four-point scale ranging from 1 (not at all) to 4 (a great deal), with higher values indicating greater trust.

### *Analytic Strategy*

All variables were measured on four-point scales. Trust\_in\_Companies ranged from 1 (not at all) to 4 (a great deal), with higher values indicating greater trust. The composite measures — Personal\_Agency and Concern\_Misuse — were each constructed as the mean of two four-point items, with all component items direction-coded so that higher values consistently indicate more of the construct being measured. Political ideology and education were included as covariates to account for their potential correlation with the primary predictors and the dependent variable. Statistical analysis proceeded in three stages. First, univariate descriptive statistics summarized the distributions of all study variables. Second, bivariate correlations were used to examine whether Personal\_Agency and Concern\_Misuse were associated with

Trust\_in\_Companies. Third, a multivariate OLS regression model predicted Trust\_in\_Companies using Concern\_Misuse and Personal\_Agency as primary predictors, with political ideology and education included as covariates. Trust\_in\_Companies served as the dependent variable for both H1 and H2. The dataset does not include a direct measure of trust in government's use of AI comparable to AIPRIV3; the company trust measure therefore functioned as the closest available proxy for examining how perceived control relates to institutional confidence more broadly. The dataset does include parallel government-focused items on perceived control and understanding (CONTROLGOV, UNDERSTANDGOV), though these were not incorporated into the present analysis. All analyses were conducted in SPSS using its graphical menu interface; full procedural documentation, including variable construction, menu paths, and output, is provided in the Appendix.

## **Qualitative Component**

### *Sample and Recruitment*

To complement the survey analysis, this study included semi-structured interviews with five adult participants (numbered 2 through 6) recruited from the Seattle metropolitan area. Participants were selected through purposive sampling (Patton, 2002, pp. 230–246) for their professional experience in fields directly engaged with data governance, privacy policy, or technology systems — including AI and data governance, private privacy consulting, corporate technology strategy, venture capital technology investment, and technology sourcing. Participants were selected to balance professional expertise in the technology and data governance industry with lived, personal experience navigating data privacy in their own lives. Each participant was chosen not simply for their sector, but because their role gave them direct insight into the cost-benefit calculations companies make around data privacy — while also being personally invested in understanding and protecting their own data as private individuals. This dual positioning — professional proximity to how the industry operates, combined with individual experience as data subjects themselves — was intended to surface perspectives that neither a purely institutional analysis nor a general population survey could capture on its own.

Participants are identified throughout this study by ID numbers 2 through 6; the number 1 was reserved for header/tracking information in the recruitment spreadsheet and does not correspond to a participant. Participant #2 was selected for his cross-sector vantage point as a

Senior Emeritus Fellow with the International Association of Privacy Professionals (IAPP), whose consulting and legal work gives him a broad, historically informed view of data governance across industries. Participant #3 was selected for her direct, hands-on experience designing consent and cookie systems during her time on Microsoft's privacy team, offering an insider's perspective on the gap between technical compliance and genuine user protection. Participant #4 was selected for her dual perspective as a venture capital professional who evaluates data governance risk in portfolio companies professionally, and as a parent making active, personal decisions about her family's data exposure. Participant #5 was selected for his enterprise technology background, which provided direct comparative insight into how major companies — Google, Apple, and Meta — differ in their actual data practices versus their public messaging. Participant #6 was selected for his procurement and vendor-compliance experience with GDPR and CCPA at Microsoft, combined with firsthand experience navigating both financial fraud and a healthcare data breach as an individual.

This sample was not designed to represent the general public's experience. While the Pew data captured nationally representative patterns in how U.S. adults perceive corporate data practices, the qualitative component drew on participants whose professional roles provide direct, substantive engagement with the systems this study examines. The two strands addressed the same research questions from different vantage points: one distributional and population-level, the other interpretive and expert-informed.

### *Ethics and Procedures*

The University of Washington Human Subjects Division reviewed the study protocol and determined it qualified for exempt status under Category 2 (IRB ID: STUDY00025193). All participants were provided with sufficient context about the study's purpose and how their responses would be used before their interview. Participants are described in general terms by professional role only; no identifying information appeared in the final research project.

Recruitment drew on the researcher's professional network, consistent with the study's Seattle municipal policy context and its engagement with the City of Seattle's One Seattle Data Strategy (2023) and 2025–2026 AI Plan, which serve as local illustrations of federal governance patterns. Participants were contacted by email and invited to complete a 30–45-minute interview conducted via Zoom or phone. Participation was voluntary, and participants were informed they

could decline any question or stop the interview at any time. With participants' consent, interviews were audio-recorded for transcription accuracy. Recordings were stored on a password-protected device, and audio files were deleted after transcription and verification were complete, consistent with the study's IRB-approved protocol. Interviews were recorded using Apple iPhone Voice Memo, automatically transcribed, and then manually reviewed against the original audio to clarify and finalize each transcript prior to analysis.

### *Interview Structure*

Interviews were organized around three core areas aligned directly with the variables analyzed in the Pew dataset: perceived control over personal data, trust in companies, and perceptions of data misuse. Each interview opened with a broad question about participants' general feelings regarding personal data privacy when using digital services, allowing concerns to surface organically before moving into more focused areas. Core questions then addressed what contributed to participants' sense of control — or lack thereof — over their personal data; how much they trusted companies to protect their data and what shaped that trust; and whether they had ever suspected their data was being misused and what indicated that to them. A closing question invited participants to reflect on what changes would make data privacy protections feel more meaningful or effective for individuals. Follow-up probes were used throughout to explore specific tools, policies, or practices affecting participants' experiences. Rather than asking participants directly about abstract concepts such as transparency or redress, the interview guide was designed to allow those themes to emerge from participants' responses, which were then used as an analytical lens for interpreting how procedural privacy rights are experienced in practice.

### *Analytic Strategy*

Interview transcripts were analyzed using thematic analysis (Braun & Clarke, 2006). Following data collection, transcripts were reviewed to identify recurring patterns related to the three core interview areas. Initial codes were developed inductively from the transcripts and then organized into broader themes mapping onto the study's conceptual framework. Given the small, expert sample, the goal of qualitative analysis was interpretive depth rather than saturation or

generalizability, and findings were integrated with the quantitative results during the discussion phase.

## ***X. LIMITATIONS***

The study does not include representation from minority, low-income, or otherwise vulnerable populations who may experience data governance gaps most acutely, and this is a recognized limitation of the study's scope. The qualitative findings are intended to provide interpretive depth rather than generalizable conclusions and should be read accordingly.

The quantitative component draws on the Pew Research Center's 2023 American Trends Panel, which provides a nationally representative baseline for public perception patterns. However, the dataset was not designed specifically to test the hypotheses in this study, and the variables used here provide imperfect operationalizations of the underlying theoretical constructs. The composite measures — *Personal\_Agency* and *Concern\_Misuse* — rely on respondent self-report and were constructed from items not originally intended to be combined. These choices are theoretically justified and documented in the methodology, but they introduce measurement limitations that should be considered when interpreting the findings. Additionally, the Pew dataset does not include a direct measure of redress — the ability to contest, correct, or seek recourse for data misuse. As a result, this study's quantitative strand speaks to the transparency and control dimensions of procedural privacy rights but cannot directly assess redress; qualitative interview data offer some interpretive insight into this dimension, though it was not a targeted measure in either strand.

Additionally, H1 and H2 are both scoped specifically to trust in companies, not trust in government or public institutions. This was a deliberate design choice, not a weakness — the study set out to examine corporate data governance specifically, given the sectoral, market-driven structure of U.S. privacy law described in the literature review. As noted in the methodology, *Trust\_in\_Companies* served as a proxy for institutional confidence more broadly. While the Pew dataset includes parallel government-focused items (e.g., perceived control and understanding of government data use), it does not include a direct government-trust item comparable to AIPRIV3; this study's dependent variable therefore has no true institutional parallel, though related constructs exist in the dataset and were not used here. However, qualitative findings (see Sub-theme 5.1 and Sub-theme 6.3) suggest this proxy may understate a real distinction: several participants described corporate trust and trust in government's handling of personal data — particularly in the context of AI — as separate concerns that do not necessarily move together. This indicates a direction for future quantitative work: testing whether

corporate and institutional trust are in fact distinct constructs, rather than assuming one can stand in for the other.

Together, these limitations mean the study is best understood as exploratory. The goal is not to produce definitive causal claims but to examine whether procedural privacy rights feel functional in practice, drawing on patterns in national survey data alongside interpretive depth from expert interviews. These constraints do not undermine the study's central contribution; they mark the boundaries within which its findings should be read.

## ***XI. FINDINGS***

### **Quantitative Findings: Pew American Trends Panel Analysis**

To test H1 and H2, this study analyzed data from the Pew Research Center's 2023 American Trends Panel (Wave 127), examining whether perceived understanding and control over personal data (Personal\_Agency) and concern about corporate data misuse (Concern\_Misuse) predict trust in companies (Trust\_in\_Companies). Because the trust measure (AIPRIV3\_W127) asks specifically about companies' responsible use of AI rather than data governance broadly, it functions here as a proxy for general corporate data trust — a limitation addressed further in the Discussion.

*Table 1. Descriptive Statistics for Study Variables*

| Variable             | N    | Mean | SD   | Min | Max |
|----------------------|------|------|------|-----|-----|
| Trust in Companies   | 4335 | 1.98 | 0.81 | 1   | 4   |
| Personal Agency      | 5019 | 2.15 | 0.66 | 1   | 4   |
| Concern About Misuse | 5010 | 3.15 | 0.75 | 1   | 4   |
| Ideology             | 4971 | 2.94 | 1.06 | 1   | 5   |
| Education            | 5083 | 3.85 | 1.57 | 1   | 6   |

Trust in companies is generally low among respondents ( $M = 1.98$ ,  $SD = 0.81$ , on a four-point scale). Nearly three-quarters of respondents reported either "not at all" (31.0%) or "not too much" trust (43.0%), while only 2.7% reported trusting companies "a great deal." Perceived personal agency was moderate to low ( $M = 2.15$ ,  $SD = 0.66$ ), while concern about corporate misuse was comparatively high ( $M = 3.15$ ,  $SD = 0.75$ ).

*Table 2. Correlations Among Key Variables*

| Variable              | 1       | 2 | 3 | 4 | 5 |
|-----------------------|---------|---|---|---|---|
| 1. Trust in Companies | —       |   |   |   |   |
| 2. Personal Agency    | .224*** | — |   |   |   |

|                   |          |          |                 |
|-------------------|----------|----------|-----------------|
| 3. Concern Misuse | -.225*** | -.077*** | —               |
| 4. Ideology       | .046**   | .041**   | -.025 —         |
| 5. Education      | .013     | .011     | -.026 .145*** — |

Note. Pearson correlations reported.

\*  $p < .05$ , \*\*  $p < .01$ , \*\*\*  $p < .001$ .

Bivariate correlations indicate that both predictors are significantly associated with trust. Personal\_Agency is positively correlated with Trust\_in\_Companies ( $r = .224$ ,  $p < .001$ ), while Concern\_Misuse is negatively correlated ( $r = -.225$ ,  $p < .001$ ). Political ideology shows a weak positive correlation ( $r = .046$ ,  $p < .01$ ); education is not significantly correlated with trust ( $r = .013$ ,  $p = .398$ ).

*Table 3. OLS Regression Predicting Trust in Companies*

| Predictor            | B      | SE   | p     |
|----------------------|--------|------|-------|
| Concern about misuse | -0.249 | .018 | <.001 |
| Personal agency      | .251   | .019 | <.001 |
| Political ideology   | .025   | .011 | .026  |
| Education            | .000   | .008 | .961  |
| Constant             | 2.169  | .087 | <.001 |

Model statistics:  $R^2 = .091$ ,  $N = 4,257$ .

To test H1 and H2, an OLS regression model was estimated predicting Trust\_in\_Companies using Concern\_Misuse and Personal\_Agency as primary predictors, with political ideology and education included as covariates. The model was statistically significant ( $F = 213.79$ ,  $p < .001$ ,  $R^2 = .091$ ,  $N = 4,257$ ). Consistent with H1, Personal\_Agency was positively associated with trust ( $B = 0.251$ ,  $p < .001$ ); respondents who reported greater understanding of and control over their personal data also reported higher trust in companies. Consistent with H2, Concern\_Misuse was negatively associated with trust ( $B = -0.249$ ,  $p < .001$ ). Political ideology showed a small positive association ( $B = 0.025$ ,  $p = .026$ ); education was not significant ( $B = 0.000$ ,  $p = .961$ ).

These quantitative patterns establish that perceived agency and concern about misuse are measurably associated with institutional trust at the population level. The qualitative interviews, discussed next, provide interpretive depth into how these dynamics are experienced directly.

### **Qualitative Findings: Semi-Structured Expert Interviews**

Thematic analysis of the five interviews identified six core themes, three of which contain further sub-themes, integrated here with the quantitative findings above. The most consistent theme across all five participants was the experience of consent as performative rather than functional — directly aligned with the low Personal\_Agency mean (2.15/4) in the Pew data.

#### **Theme 1: Consent as Performative**

All five participants independently described consent mechanisms — privacy policies, cookie banners, terms-of-service agreements — as performative rather than functional, using language strikingly consistent across interviews despite no shared vocabulary being introduced in the interview protocol. Participant #2 (AI/Data Governance Expert) stated plainly, "consent is useless," and characterized standard consent forms as "intended for compliance. They are not intended for a result other than compliance." Participant #6 (Principal Sourcing Engineer) reached a similar conclusion from direct professional experience, noting that privacy notices offer no real protection: "they are going to get in, and they are gonna get your data, regardless of what their privacy policy states." Participant #3 (Private Privacy Consultant) — whose professional role involved designing these systems — described a "Goldilocks problem" in consent design, where complexity is either overwhelming or ineffective, and noted that even privacy professionals routinely click "accept all" out of frustration rather than genuine agreement.

This convergence is notable given participants' professional distance from one another and their varied vantage points — legal/consulting, corporate engineering, and privacy design. Their independent use of terms like "performative," "noise," and "useless" suggests the experience of non-functional consent is not confined to any one professional context, but reflects a structural feature of how consent mechanisms are currently designed. This finding directly supports H1: participants' low perceived understanding of what consent actually accomplishes

corresponds with the broader population-level pattern of low personal agency documented in the Pew data.

### *Sub-theme 1.1: Work Persona vs. Personal Persona Split*

Both Participant #2 and Participant #4 described an identical bifurcation using nearly the same language: within employer-controlled systems, data feels bounded and owned ("good tools that generally say the data is mine... working inside the sandbox"), while in personal life, participants "work from the assumption that the information is already out there and available to everyone." This split suggests perceived control is not a fixed trait but is contingent on institutional context — a nuance the Pew Personal\_Agency composite, as a single population-level measure, cannot capture.

## **Theme 2: Business Model as the Primary Trust Signal**

Across all five interviews, participants converged on one shared benchmark for evaluating corporate trustworthiness: whether a company's revenue depends on user data or on direct payment for a product or service. This logic consistently overrode stated privacy policies as the operative basis for trust. Participant #2 articulated the underlying calculation directly: "Follow the money — is the money in the data or is the money in my subscription? If the money is in the subscription, I do not worry as much. If the money is in the data, I have to assume they are going to play very aggressive roles in trying to use that data to turn it into some form of revenue stream." Participant #5 (Corporate Technology Executive) and Participant #4 (VC Professional) independently invoked nearly identical language — "if you are not paying for the service or product, then you are the product" — treating this as the clearest available signal of whether a company's incentives align with user protection or work against it.

Participants extended this logic to direct company-by-company comparisons, evaluating firms not by stated policy but by where their business models placed user interests relative to company benefits. Participant #5 drew a three-way contrast: Google was described as "more sensitive to protecting consumers' information," Meta was characterized as more upfront that data would be used for advertising — "honest about not caring" — while Apple was singled out as the most concerning case precisely because its public image diverges from this logic: "this squeaky clean, pro-consumer image... and in reality, they are some of the worst offenders for

data privacy and selling your data." This suggests participants distrust misalignment between stated values and business model more than they distrust an openly data-driven model — Meta's transparency about its incentives was treated as more trustworthy than Apple's perceived discrepancy between image and practice.

Participant #6 offered a contrasting data point suggesting business model logic can be overridden by verified behavior. He reported trusting his employer, Microsoft, specifically because it complies with GDPR and CCPA standards "even where not legally required," treating voluntary compliance beyond legal minimums as evidence that a company's practices exceed what its business model alone would predict. He described the underlying comparison directly: "I know what I have to do to bring software in and protect my customers and my own personal IP address... I know we're protected, but I got to tell you, I don't feel the same without any other corporation." Together, these accounts indicate that participants are not simply weighing whether a company profits from data, but actively assessing whether that incentive structure benefits the company at the user's expense or has been counterbalanced by verifiable protective practice — a distinction with direct implications for Concern\_Misuse: participants' concern appears calibrated less to disclosed practices than to inferred incentive alignment.

This incentive-driven logic extends to the scale of collection itself: Participant #3 characterized data-monetization-driven companies as prone to a "hoarding mentality," collecting far more than is ever operationally used — a pattern consistent with the broader finding that incentive structure, not stated policy, drives corporate data behavior.

### **Theme 3: Privilege Gap — Privacy as a Purchasable Good**

Participants consistently identified financial resources as a precondition for meaningful privacy protection, describing specific tools and practices that are unavailable to those without the means. Participant #2 acknowledged directly that his own privacy practices — credit locks, paid anonymity services — constitute "a privilege." Participant #4 described the same dynamic in reverse, both structurally and through her own behavior. Reflecting on a health-tracking app decision, she said: "I had a choice about whether to use an app for some health tracking — I looked at the US-based one and a European-based one, and I chose the European-based one specifically because they have more data protections." On the broader trade-off of convenience versus privacy, she added: "There's this trade-off that you have to wrestle with, and it's really

frustrating. I finally just gave in — the privilege was I could see my lab data right away." She named the underlying pattern directly: "If you have more money and more accessibility and can invest in things to protect your data, you are almost more secure than the average American." Participant #6 extended this to consequences, not just access: after a fraudulent charge of roughly \$18,963 on his credit card, the issue was resolved within three days because of proactive credit protections already in place—a resolution he explicitly attributed to having resources most people lack. He contrasted this with a separate healthcare data breach in which no equivalent recourse existed. He noted that those living paycheck to paycheck lack the financial literacy and standing protections to respond to fraud at all. Together, these accounts suggest privilege operates on two levels: access to preventive tools and speed of recovery when protection fails.

#### **Theme 4: EU vs. U.S. Framing — Fundamental Right vs. Fragmented System**

Participants repeatedly contrasted European data protection as constitutionally grounded against the U.S.'s sectoral approach, and several translated this contrast into direct personal choices. Participant #2 traced the divergence to differing historical foundations: Europe's WWII- and Stasi-informed grounding of privacy as a fundamental right, versus the U.S.'s "frontier heritage" and reliance on the Fourth Amendment as its primary constitutional anchor. He invoked the historical framing of privacy as "the right to be let alone" — a phrase originating in Warren and Brandeis's (1890) influential Harvard Law Review article, and later revived in Brandeis's dissent in *Olmstead v. United States* (1928) — alongside early fears surrounding the camera as one of the earliest U.S. privacy concerns, framing both as never having developed into the kind of coherent foundational framework Europe possesses. Participant #4 made the same contrast concrete through repeated personal choices rather than abstract preferences: she selected a Europe-based health-tracking app over its U.S. equivalent specifically for stronger protections, explaining, "I had a choice about whether to use an app for some health tracking — I looked at the US-based one and a European-based one, and I chose the European-based one specifically because they have more data protections." She was separately in the process of switching to a European email provider for the same reason — two independent decisions pointing to the same underlying judgment about which jurisdiction takes data rights seriously. This theme reinforces the literature review's account of the Schwartz (2013) divergence at the level of lived experience:

participants independently reconstruct the dignity-based/procedural distinction Schwartz identifies without prompting and, in some cases, act on it as consumers.

### **Theme 5: Perceived Threats and Structural Vulnerability**

Across the interviews, participants described a shifting and expanding sense of who or what threatens their data privacy — from algorithmic prediction, to routine breaches, to the specific populations left most exposed by current gaps in protection. The three sub-themes below trace this progression: from individual discomfort, to systemic fatigue, to disproportionate impact on specific groups.

#### *Sub-theme 5.1: Algorithmic Discomfort and Shifting Threat Models*

Participants described unease at the accuracy of behavioral prediction, and for at least one participant, this unease extended into a broader shift in whom they perceive as the primary threat to their privacy. Participant #2 recounted discussing a trip to Portugal and subsequently "seeing a bunch of Portugal ads." Participant #3 complicated this pattern by naming confirmation bias directly as a competing explanation: "Like, I rented a Bronco Sport, and I really liked this car. Now I look around, and they're everywhere. I just wasn't paying attention before." Participant #3 also described a more significant shift in threat perception over time, tying it directly to a change in political context: "Honestly, when Trump came into power, and they started opening people's laptops and looking at their social media — now I'm worried about the government. Whereas before I wasn't." This suggests government surveillance may be an emerging dimension of data-privacy concern worth examining in future research, separate from the corporate-trust focus of this study.

#### *Sub-theme 5.2: Breach Fatigue and the Limits of Remediation*

Several participants described data breaches as routine rather than exceptional, and offered specific details on why remediation feels inadequate, rather than simply stating fatigue in the abstract. Participant #4 described this directly: "Not good. Very bad. I get notifications, probably at least every other week, of my data being part of a hack. Or my child's data being part of the hack." She separately described MyChart — the healthcare data platform she is required to use — as holding "pretty much a monopoly in the industry" while facing an active lawsuit over

its data handling, with little competitive pressure to improve. Participant #6 stated the underlying belief plainly: "There is no data that is private," and described a live example unfolding during the interview itself — a nationwide university platform breach occurring during finals week, which she suspected was a deliberate, possibly nation-state action, and which produced a degree of personal stress and panic beyond what she had anticipated. She also raised a specific structural gap: healthcare records are retained for six to seven years, with no clear notice of destruction or verification process, meaning the risk of a breach persists long after the original data-sharing interaction. Concern about misuse (Concern\_Misuse,  $M = 3.15/4$ ) registers as high in the Pew data, yet these accounts suggest that this concern coexists with resignation and structurally limited remediation options, rather than active, effective vigilance — a distinction that the quantitative measure alone cannot separate.

### *Sub-theme 5.3: Vulnerable Populations*

Participants repeatedly named specific populations as disproportionately exposed, often citing specific mechanisms of exposure rather than general concern. Participant #2 raised concern for LGBTQ+ individuals specifically, pointing to the risk of sensitive information — including medical records — becoming newly exposed or restricted as political and legal contexts shift: "You can even imagine some out of the LGBTQ community... suddenly seeing at least some quarters start to close in on that. You can see folks very concerned about what they have hosted... what they have between them and their physician." Participant #4 identified a bidirectional age vulnerability: elderly individuals are heavily targeted and under-supported, while adolescents aged 11–14 are, in her assessment, now equally vulnerable due to inexperience rather than age-related decline. She noted that the Children's Online Privacy Protection Act (COPPA) provides some baseline protection for minors but described its coverage as limited. This theme also exposes an imbalance of understanding: those with the professional expertise to navigate data privacy are positioned very differently than the general population, and that asymmetry does not resolve itself — one group's understanding does not protect the other. Consistent with the broader pattern across this study's findings, participants' accounts suggest that data protection functions less as a benefit designed for consumers and more as a compliance obligation designed for companies, leaving those without professional or financial resources most exposed to the gap between the two.

## **Theme 6: Calls for Structural Reform**

Participants converged on the need for reform, though they proposed different mechanisms — legislative, oversight-based, and forward-looking — for closing the gap between formal privacy protections and their practical accessibility. The three sub-themes below present these proposals in turn.

### *Sub-theme 6.1: Call for Federal Legislation*

A GDPR-equivalent federal privacy law was the single most consistent policy recommendation among participants, and several grounded this in specific regulatory gaps rather than in general appeals for reform. Participant #4 named this as her top priority: "I would like us to have stronger privacy protections at the federal level — something equivalent to the GDPR law beneath the EU." Participant #5 argued a federal standard would benefit businesses and consumers alike, describing the current patchwork of state-level rules — including inconsistent CCPA compliance outside California — as costly and difficult for companies to navigate: "It's this soup of different regulations, and you are trying to manage a business across multiple privacy requirements. It's very hard, very expensive, very time-consuming." Participant #3 extended the argument to enforcement specifically, arguing that consent without enforcement is meaningless and calling for a comprehensive statutory floor below which no data use should be permitted without explicit opt-in, in contrast to the U.S.'s current sectoral approach (HIPAA, COPPA, and state-level rules). This theme connects directly to the structural policy problem outlined in Chapter 1 — participants are independently arriving at the same diagnosis of fragmented, non-enforceable protections that anchors the literature review.

### *Sub-theme 6.2: Journalism and Civil Society as an Oversight Mechanism*

Participant #2 proposed a specific alternative to consumer-driven oversight: mandated transparency about data lifecycle practices, evaluated by journalists, academics, and civil society rather than individual consumers, arguing directly that "no consumer should ever be expected to review that stuff." This reframes the redress gap identified in the study's limitations — the proposal shifts responsibility for enforcement away from individual users entirely, toward institutional and civic oversight. Consistent with Sub-theme 5.3, this reflects a broader pattern in

the interviews: even from a professionally privileged vantage point, participants consistently recognized that the burden of understanding complex data systems should not fall on ordinary users.

### *Sub-theme 6.3: AI Governance Gap*

Participant #4 raised this concern directly: "It's very unclear if there's any enshrinement of constitutional rights and protections having any sort of impact on what is being done by the government with AI. Anthropic is fighting with the government right now to preserve some rights and protections, and the government has said no." Participant #6 echoed this concern from a different angle, questioning how long existing government-mandated privacy protections will remain stable given current AI investment priorities. Read alongside Sub-theme 5.1, this concern points to a broader pattern: participants' sense of who holds power over their data is expanding beyond corporations to include government use of AI. This falls outside what this study's hypotheses were designed to measure — H1 and H2 focus specifically on corporate trust — but it points to something this study's scope cannot fully address. Data privacy already spans business models, ethical practice, technological infrastructure, and user understanding; as AI development increasingly intersects with all of these, the stakes of ensuring users understand their data rights only grow. This is a limitation of the current study's scope, and a clear direction for future research.

## ***XII. CONCLUSION***

This study set out to examine the extent to which the U.S. sectoral data privacy system provides users with actionable knowledge, transparency, and redress over personal data practices, and how these procedural protections are interpreted and experienced in practice. This research question was answered. Quantitative analysis confirmed that perceived agency and concern about misuse are measurably associated with institutional trust. Qualitative interviews showed that consent functions as compliance theater rather than genuine control, directly reinforcing H1 and H2. The interviews also revealed something the quantitative data alone could not capture: data privacy is not a single, contained issue but a complex web spanning corporate incentive structures, government surveillance, sector-specific statutes, and unevenly distributed vulnerability. Redress remains the least resolved dimension of this study. Rather than describing existing mechanisms as accessible, participants proposed structural alternatives, including federal legislation and institutional oversight, suggesting individual redress is not currently perceived as realistic. Together, these findings show that procedural protections exist on paper but remain difficult to interpret, exercise, or enforce in practice.

The four sub-questions guiding this study point toward the same conclusion from different angles. On the first sub-question, how U.S. law conceptualizes user rights, this study confirms that enforcement remains institutional rather than individual (Kuner, 2015; Qing, 2022). Participants found no realistic mechanism to contest or correct misuse of their own data. On the second sub-question, how users interpret transparency and control, all five participants described consent as performative rather than functional. This directly reinforces H1 and echoes Solove's (2013) account of consent as a legal shield rather than genuine agreement. On the third sub-question, what shapes trust, participants relied not on stated privacy policies but on inferred business incentives. Apple's divergence between image and practice was seen as more concerning than Meta's transparency about its data-driven model, adding interpretive depth to H2. On the fourth sub-question, users' ability to respond to misuse, no participant described existing redress mechanisms as adequate. Instead, they called for structural alternatives, including federal legislation and civic oversight, rather than individual recourse. Rather than describing existing mechanisms as accessible, participants proposed structural alternatives,

including federal legislation and institutional oversight, suggesting individual redress is not currently perceived as realistic.

Future research should extend this study's sample beyond data-governance professionals to populations more likely to experience these governance gaps directly. It should also examine how AI governance is reshaping corporate and government data practices alike, a concern participants raised but this study's scope did not address. A related question, whether trust in companies and trust in government are separate constructs, is addressed in Recommendation #5.

### ***XIII. RECOMMENDATIONS***

#### **Recommendation #1: Federal Privacy Legislation**

Congress should enact comprehensive, GDPR-equivalent federal privacy legislation, replacing the current sectoral patchwork of HIPAA, COPPA, and state-level laws (e.g., CCPA), within the next legislative session. This recommendation is directly supported by this study's qualitative findings: three of five participants independently called for federal legislation modeled on the GDPR, citing the current patchwork of state and sector-specific rules as costly, difficult to navigate, and insufficiently protective (Sub-theme 6.1).

#### **Recommendation #2: Business-Model Disclosure Requirement**

The Federal Trade Commission should require all consumer-facing platforms to display a standardized, plain-language revenue-model disclosure — indicating whether the service is subscription-funded, data-monetized, or a hybrid — within 18 months of the federal legislation proposed above. This recommendation responds directly to this study's second-strongest qualitative finding: participants consistently used a company's business model, not its stated privacy policy, as the primary basis for trust, often distrusting companies whose public image diverged from their actual revenue structure (Theme 2). Participant #5's comparison of Apple's "squeaky clean, pro-consumer image" against its actual data practices exemplifies this pattern directly.

#### **Recommendation #3: Data Minimization Independent of Consent**

Congress should establish federal data-minimization and purpose-limitation requirements that apply regardless of user consent, as a core provision of the federal legislation proposed above. These requirements would restrict companies from collecting or using personal data beyond what is strictly necessary for the requested service, independent of whether a user clicked "agree." This recommendation responds directly to this study's strongest qualitative finding: all five participants described consent as performative rather than functional, with even privacy professionals routinely clicking "accept all" out of frustration rather than genuine agreement (Theme 1). Because consent does not function as a meaningful check on data practices in participants' own accounts, a regulatory floor that does not depend on consent is necessary to

close this gap. This protection could be enforced through the same federal legislation proposed above.

#### **Recommendation #4: Mandatory Data Retention Limits and Verifiable Deletion**

Congress should require, within the same federal legislation proposed above, that companies establish defined data retention limits by data category, disclose those limits and any third-party data transfers in plain language, and provide users with verifiable confirmation once data has been deleted. This requirement should not rely on companies' self-reported compliance alone. This recommendation responds directly to a structural gap identified in this study's qualitative findings: Participant #6 noted that healthcare records are retained for six to seven years with no clear notice of destruction or verification process, meaning the risk of a breach persists long after the original data-sharing interaction (Sub-theme 5.2). More broadly, participants across the interviews described a recurring pattern in which companies are nominally responsible for communicating how long data is stored, who can access it, and whether it is transferred to third parties — while the burden of verifying any of this falls entirely on the user, who typically has no practical means to do so. Shifting from a disclosure-only model to one that includes independently verifiable deletion would address this imbalance directly.

#### **Recommendation #5: Future Research — Testing Whether Corporate and Government Trust Are Separate Attitudes**

As noted in the Conclusion, future research should test whether trust in companies and trust in government to responsibly handle personal data are two separate attitudes, rather than a single underlying sense of "institutional trust" that applies to both, using Pew's parallel government-focused items (CONTROLGOV, UNDERSTANDGOV) alongside the company-focused items used here. ***Specifically: H3 — Trust in companies and trust in government are only weakly correlated, indicating that a person's trust in one does not predict their trust in the other.*** This responds directly to a limitation of this study: Trust\_in\_Companies was used as a proxy for institutional confidence more broadly, since no direct government-trust item paralleling AIPRIV3 exists in the dataset. Qualitative findings support the need for this distinction: participants described corporate data misuse and government surveillance as separate, evolving concerns rather than a single unified threat (Sub-theme 5.1; Sub-theme 6.3).

#### ***XIV. APPENDIX***

##### **Data Preparation and Variable Construction**

Prior to analysis, all five component items (CONTROLCO\_W127, UNDERSTANDCO\_W127, CONCERNCO\_W127, PRIVWRY\_b\_W127, AIPRIV3\_W127) were reverse-coded via Transform → Recode into Different Variables, so that higher values consistently indicate more of the construct being measured across all items. Missing and non-substantive responses (e.g., "no answer," "not sure") were coded as 99 and excluded from analysis.

Personal\_Agency was computed via Transform → Compute Variable as the mean of the recoded CONTROLCO\_W127 and UNDERSTANDCO\_W127 variables. Higher values indicate greater perceived agency (control and understanding combined).

Concern\_Misuse was computed via Transform → Compute Variable as the mean of the recoded CONCERNCO\_W127 and PRIVWRY\_b\_W127 variables. Higher values indicate greater concern about corporate data misuse.

Trust\_in\_Companies used the recoded AIPRIV3\_W127 variable directly as the dependent variable, with an additional missing-value code (5.00) applied to exclude "not sure" responses from analysis.

##### **Step 1: Descriptive Statistics**

Univariate descriptive statistics were generated for all five study variables to establish sample composition and identify data quality issues prior to hypothesis testing.

In SPSS: Analyze → Descriptive Statistics → Frequencies, with Descriptives run in parallel for mean, standard deviation, minimum, and maximum. Valid sample sizes ranged from N = 4,335 (Trust\_in\_Companies) to N = 5,083 (Education), reflecting item-level nonresponse—full results reported in Table 1.

##### **Step 2: Bivariate Correlations**

This step examined whether Personal\_Agency and Concern\_Misuse were significantly associated with Trust\_in\_Companies, and whether the covariates (Ideology, Education) warranted inclusion in the regression model.

In SPSS: Analyze → Correlate → Bivariate, with Pearson correlation coefficients selected across all five variables. Personal\_Agency correlated positively with Trust\_in\_Companies ( $r = .224$ ,  $p < .001$ ); Concern\_Misuse correlated negatively ( $r = -.225$ ,  $p < .001$ ); Ideology showed a weak positive correlation ( $r = .046$ ,  $p < .01$ ); Education was not significantly correlated ( $r = .013$ ,  $p = .398$ ). Full results reported in Table 2.

### **Step 3: Multivariate Regression**

This step tested H1 and H2 directly, estimating the independent contribution of Personal\_Agency and Concern\_Misuse to Trust\_in\_Companies while controlling for Ideology and Education.

In SPSS: Analyze → Regression → Linear. Dependent variable: Trust\_in\_Companies. Independent variables (entered in a single block): Personal\_Agency, Concern\_Misuse, Ideology, Education. Model was statistically significant,  $F(4, 4252) = 213.79$ ,  $p < .001$ ,  $R^2 = .091$ ,  $N = 4,257$ . Full results reported in Table 3.

## **Interview Recruitment Email**

Subject: Invitation to participate in UW research interview on data privacy governance

Dear [Name],

My name is Anna Templeton, and I am a graduate student in the Master of Arts in Policy Studies program at the University of Washington Bothell. I am currently conducting research for my capstone project on how individuals understand transparency, control, and accountability in the U.S. data privacy system.

Earlier in the project, I analyzed publicly available survey data from the Pew Research Center on Americans' views of data privacy. The purpose of the interview portion of the study is to better understand how people interpret those issues in their own experiences with digital services.

I am inviting a small number of participants to share their perspectives. Participation would involve a 30–45-minute semi-structured interview conducted via Zoom or phone. The conversation will focus on general experiences with data privacy, perceptions of personal control over data, and trust in companies that manage personal information.

A few additional details:

- Participation is voluntary. You may decline to answer any question or stop the interview at any time.
- Confidentiality: Your name will not appear in the final research project. Participants will be described only in general terms (for example, "digital services user" or "technology policy professional").
- Recording: With your permission, the interview may be audio recorded for note-taking accuracy.
- Use of information: Interview responses will be used for a graduate research project examining how individuals interpret data privacy protections in practice.

There are no anticipated risks beyond those associated with a normal conversation about professional or personal perspectives on digital services. While there is no compensation, your input will help provide a better understanding of how data privacy protections are experienced in

practice. If you would like, I would also be happy to share a short summary of the research findings once the project is completed.

If you are interested in participating, please let me know your availability over the next few weeks. Thank you for considering the request, and please feel free to reach out if you have any questions.

## **Interview Opening Script**

Thank you for agreeing to participate in this interview. Before we begin, I want to briefly explain the purpose of the study.

This project examines how individuals understand transparency, knowledge of data practices, and accountability mechanisms within the U.S. data privacy system. Earlier in the research, I analyzed survey data from the Pew Research Center on Americans' views of data privacy, including attitudes about data misuse, personal control over information, and trust in companies that manage personal data. The purpose of this conversation is to better understand how people interpret these issues in their everyday experiences with digital services. Your perspective helps provide context for how individuals think about personal data agency, trust in companies, and perceptions of data misuse.

Your participation is voluntary. You may decline to answer any question or stop the interview at any time. With your permission, I would like to audio-record the interview for note-taking accuracy. The recording will be stored securely and deleted after the project is completed. If you would like, I would also be happy to share a short summary of the research findings once the project is finished. Do you consent to participate in this interview?

## **Opening Question**

1. Overall, how do you feel about your personal data privacy today when using digital services or online platforms?
  - a. Possible follow-ups:
    - i. What kinds of concerns, if any, come to mind when you think about data privacy?
    - ii. Are there particular situations where you feel more or less comfortable sharing data?

## **Core Question 1 — Personal Data Agency**

2. What contributes to your sense of control—or lack of control—over your personal data online?
  - a. Possible follow-ups:

- i. Are there tools, settings, or policies that affect how much control you feel you have?
- ii. What makes it easier or harder for people to manage their personal data?

### **Core Question 2 — Trust in Companies**

- 3. How much do you trust companies to protect your personal data, and what shapes that level of trust?
  - a. Possible follow-ups:
    - i. Are there particular practices that increase or decrease your trust?
    - ii. Do privacy policies or consent notices affect how much you trust a company?

### **Core Question 3 — Perceptions of Data Misuse**

- 4. Have you ever had a moment where you suspected your data was being misused — and if so, what tipped you off?
  - a. Possible follow-ups:
    - i. Are there signs that make people think their data has been mishandled?
    - ii. What options do individuals have if they believe their data has been misused?

### **Closing Question**

- 5. What changes would make data privacy protections feel more meaningful or effective for individuals?

### **Closing Script**

Thank you for sharing your perspective. Your input helps provide context for understanding how people interpret transparency, control, and accountability in data governance systems.

## **XV. BIBLIOGRAPHY**

- Bignami, F., & Resta, G. (2015). Transatlantic privacy regulation: Conflict and cooperation. *Law and Contemporary Problems*, 78(4), 231–266.  
[https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2431&context=faculty\\_publications](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2431&context=faculty_publications)
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (2018).  
[https://leginfo.ca.gov/faces/codes\\_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5](https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5)
- Charter of Fundamental Rights of the European Union, 2000/C 364/01, art. 8 (2000).  
[https://www.europarl.europa.eu/charter/pdf/text\\_en.pdf](https://www.europarl.europa.eu/charter/pdf/text_en.pdf)
- Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (1998).  
<https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>
- City of Seattle. (2023). *One Seattle Data Strategy*. City of Seattle.  
<https://www.seattle.gov/documents/Departments/MayorHarrell/OneSeattleInitiatives/OneSeattleDataStrategy.pdf>
- City of Seattle. (2025). *City of Seattle 2025–2026 AI plan*. Seattle Information Technology.  
<https://seattle.gov/documents/Departments/Tech/Privacy/AI/City%20of%20Seattle%202025-2026%20AI%20Plan.pdf>
- Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE.
- Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems, Case C-311/18, ECLI:EU:C:2020:559 (Court of Justice of the European Union, July 16, 2020).  
<https://www.statewatch.org/media/1317/eu-cjeu-schrems-ii-judgement-16-7-20.pdf>
- European Commission. (2023, July 10). *Commission implementing decision (EU) 2023/1795 on the adequate level of protection of personal data under the EU-U.S. Data Privacy Framework*.  
[https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-07/adequacy\\_decision\\_eu-us\\_data\\_privacy\\_framework\\_en.pdf](https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-07/adequacy_decision_eu-us_data_privacy_framework_en.pdf)

- European Data Protection Board. (2023, February 28). *Opinion 5/2023 on the European Commission draft implementing decision on the adequate protection of personal data under the EU–US Data Privacy Framework*.  
[https://www.edpb.europa.eu/system/files/2023-02/edpb\\_opinion52023\\_eu-us\\_dpf\\_en.pdf](https://www.edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf)
- Hargittai, E., & Marwick, A. (2016). "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication (19328036)*, 10, 3737–3757.
- Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).  
<https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf>
- Kempeneer, S. (2021). A big data state of mind: Epistemological challenges to accountability and transparency in data-driven regulation. *Government Information Quarterly*, 38(3), Article 101578. <https://doi.org/10.1016/j.giq.2021.101578>
- König, P. D. (2021). Citizen-centered data governance in the smart city: From ethics to accountability. *Sustainable Cities and Society*, 75, Article 103308.  
<https://doi.org/10.1016/j.scs.2021.103308>
- Kuner, C. (2015). *Extraterritoriality and international data transfers in EU data protection law* (University of Cambridge Faculty of Law Research Paper No. 49/2015). SSRN.  
<https://ssrn.com/abstract=2644237>
- Maximilian Schrems v. Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650 (Court of Justice of the European Union, Oct. 6, 2015).  
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362>
- Nissenbaum, H. (2009). Capacity to spread and find everything, everywhere. In *Privacy in context: Technology, policy, and the integrity of social life* (pp. 51–64). Stanford University Press.  
<https://doi-org.offcampus.lib.washington.edu/10.1515/9780804772891-006>
- NOYB – European Center for Digital Rights. (2023, July 10). *European Commission gives EU–US data transfers a third round before the CJEU*. NOYB.  
<https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>
- Patton, M. Q. (2002). *Qualitative research & evaluation methods* (3rd ed.). Sage Publications.

- Pew Research Center. (2023, October). *How Americans view data privacy*  
<https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>
- Qing, Q. (2022). *Governing information privacy: Understanding how the Federal Trade Commission regulates privacy* [Doctoral dissertation, University of Washington]. ProQuest Dissertations & Theses Global  
<https://www.proquest.com/dissertations-theses/governing-information-privacy-understanding-how/docview/2655880184/se-2>
- Schwartz, P. M. (2013). The EU–U.S. privacy collision: A turn to institutions and procedures. *Harvard Law Review*, 126(7), 1966-2009.
- Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880-1903.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220. <https://doi.org/10.2307/1321160>
- Wu, T. (2016). *The attention merchants: The epic scramble to get inside our heads*. Knopf.
- Wu, Y. (2023). *Data governance in public sector: A study of U.S. municipal open data platforms* [Doctoral dissertation]. ProQuest Dissertations & Theses Global.  
<https://www.proquest.com/dissertations-theses/data-governance-public-sector-study-u-s-municipal/docview/2829678873/se-2>