NetNubby: A Context-Bound Web Annotation System for Decoupled Social Signaling

Abstract

NetNubby is a web-based annotation and communication system that enables users to attach short textual notes to arbitrary URLs. Unlike conventional social media platforms, NetNubby intentionally decouples expressive activity from visible social feedback mechanisms such as likes, follower counts, and algorithmic ranking. Instead, it introduces a constrained, context-bound interaction model in which communication is organized around web resources rather than centralized feeds or identity-centric social graphs.

This paper presents the design rationale, system architecture, and interaction model of NetNubby, with particular emphasis on its separation of communication modalities, suppression of social metric visibility, and introduction of asymmetric interaction signals. We argue that these design choices produce a non-normative socio-technical environment in which expression, attention, and identity formation are structurally decoupled from conventional engagement economies.

1. Introduction

Modern social computing systems typically rely on engagement-driven architectures in which user interaction is transformed into measurable signals (e.g., likes, shares, follower counts) that are subsequently used to rank, recommend, and amplify content. While effective for scaling attention, these mechanisms conflate expression with measurable popularity and embed social comparison into the core user experience.

NetNubby explores an alternative design space: a context-bound annotation layer for the web in which communication is anchored to URLs rather than feeds, and where interaction signals are intentionally prevented from becoming public social metrics. At a structural level, this approach is compatible with established web annotation models such as the W3C Web Annotation Data Model, which defines how annotations attach to web resources. However, NetNubby's primary contribution lies in redefining the social and interactional semantics of such annotations, rather than their representation.

The system is motivated by the hypothesis that decoupling expression from visible engagement metrics can reduce social performance pressure while preserving localized communicative utility.

NetNubby should not be understood as a conventional social platform optimized for engagement, discoverability, or communicative efficiency. Instead, it explores a constrained interaction model that prioritizes contextuality, boundedness, autonomy, and reduced social performativity.

2. System Overview

NetNubby is implemented as a web annotation overlay system in which users create constrained textual artifacts ("Notes") associated with specific URL contexts. Notes are bounded in size, non-scrollable, and rendered directly within the spatial context of the target webpage.

Importantly, the system is not limited to the conventional centralized web (clearnet). NetNubby extends its context-binding model to alternative addressing schemes, including:

- **Content Identifiers (CIDs) over IPFS:** enabling annotation of content-addressed, decentralized web resources
- **Onion services (Tor hidden services):** enabling annotation within privacy-preserving, network-layer-anonymized environments (e.g., via Tor-compatible browsers such as Brave)
- **Local machine resources (file:/// protocol):** enabling annotation of locally stored documents rendered in the browser environment

This extension preserves NetNubby's core invariant—annotation bound to resource identity—while broadening the addressable space beyond DNS-based web infrastructure.

The system defines five mutually exclusive communication modalities:

- Public Notes: Contextual annotations visible to all users of a URL instance.
- Personal Notes: Self-addressed notes stored server-side.
- Exclusive Notes: Direct one-to-one communication between users.
- Group Notes: Broadcast messages to user-defined contact sets ("tribes").
- Local Notes: Device-resident notes not transmitted to the server.

Mode exclusivity ensures that a given interaction context exposes only one communication layer at a time, preventing cross-modal contamination of audience interpretation.

3. Design Principles

3.1 Contextual Anchoring

All Notes are bound to URL contexts, treating web pages as persistent conversational surfaces rather than passive content endpoints.

3.2 Suppression of Social Metric Visibility

The system explicitly avoids exposing engagement metrics such as likes, follower counts, or ranking signals. Interaction data may be stored internally but is not rendered as user-facing social information.

3.3 Pseudonymous Identity Model

Users operate under pseudonymous monikers. Identity is stable for coordination but is not elevated into a system-visible social object (e.g., profiles, reputation scores).

3.4 Asymmetric Interaction Visibility
Certain interaction signals (e.g., cohort membership or engagement events) may exist at the system level without corresponding user-facing representations. This ensures that behavioral data does not function as social feedback.

3.5 Modal Separation of Communication
The system enforces strict separation between communication types (public, personal, exclusive, group, local), preventing their co-occurrence within a single rendering context.

4. Tribes: User-Defined Communication Sets
Tribes are bounded (maximum cardinality constraint of 20 members) user-defined contact sets used for Group Note distribution.

Key properties include:

- Explicit user curation of membership
- Absence of system-generated expansion or recommendation
- Lack of public visibility or enumeration
- Non-guaranteed message reception due to recipient-side silent discard functionality and intentionally reduced delivery transparency

Tribes function as intent-based coordination structures rather than persistent social identity graphs. They support directed communication without enforcing reciprocity or visibility of engagement.

5. Cohorts: Implicit Interaction Records
Cohorts represent system-level records of user interaction events, such as approval or engagement with Notes. While these records are not exposed to users or rendered as social objects, they occupy a dual-role design space: simultaneously functioning as system instrumentation and as latent user preference signals.

5.1 Dual-Role Interpretation: System Utility and User Value
Unlike conventional engagement logs in social platforms, cohorts are intentionally excluded from public visibility, ranking systems, and social graph construction. However, this design choice does not eliminate their user-facing value; instead, it relocates it away from social competition and toward private preference expression.

From a user perspective, cohorts enable:

- **Non-performative preference signaling:** Users can express approval of Notes without contributing to visible social metrics or identity performance.
- **Private curation of content exposure:** Engagement implicitly shapes future content relevance without exposing preferences to other users or authors.
- **Low-friction subscription-like behavior:** Users can repeatedly signal interest in content sources without being required to commit to explicit follow relationships or social acknowledgment.

These properties position cohorts as a mechanism for *latent personalization without social legibility*, distinguishing them from explicit social graph edges.

5.2 System-Level Function

From a system perspective, cohorts remain useful for:

- Abuse detection and anomaly analysis
- Sybil attack mitigation via behavioral clustering
- Integrity monitoring of interaction patterns

Crucially, system-level utility is explicitly decoupled from user-facing representation; cohort-derived insights do not propagate into ranking, recommendation, or visibility mechanisms that would otherwise transform latent interaction patterns into socially performative feedback structures.

5.3 Design Tension

The dual nature of cohorts introduces a structural tension between:

- **User interpretation:** cohorts as private preference expression
- **System interpretation:** cohorts as behavioral telemetry

NetNubby resolves this tension by ensuring that only the user-facing interpretation influences experience design, while system interpretation remains non-exposed and non-operationalized in social feedback loops.

5.4 Distinction from Hidden Follow Systems

A key design question is how cohorts differ from traditional or hidden follow mechanisms commonly found in social platforms.

In conventional systems, even when follow relationships are partially obscured, they typically function as:

- persistent subscription edges between users
- inputs to ranking or recommendation algorithms
- signals that contribute to identity formation or audience definition

In contrast, NetNubby cohorts differ along three critical dimensions:

- **Non-reciprocity:** Cohorts are not exposed as mutual or even unilateral social relationships; neither party is aware of the specific linkage.
- **Non-operationalization in ranking:** Cohort data is explicitly excluded from content ranking, feed construction, or visibility amplification mechanisms.
- **Event-based rather than structural persistence:** Cohorts reflect discrete interaction events rather than durable, user-navigable relationship graphs.

As a result, while cohorts may superficially resemble hidden follow systems, they do not function as latent social graphs. Instead, they operate as *ephemeral preference traces that never crystallize into user-facing relational structures*.

This distinction is central to maintaining NetNubby's separation between interaction history and social identity formation.

For example, a user may repeatedly express appreciation for Notes authored in a particular stylistic or thematic manner without either party perceiving a persistent relational linkage. Unlike conventional social systems, this interaction does not produce visible follower counts, mutual acknowledgment, or publicly legible affiliation structures. The resulting ambiguity reduces interactional interpretability, but also suppresses audience management behaviors and performative reciprocity expectations commonly associated with explicit social graphs.

6. Interaction Model

6.1 Posting Semantics

Users generate Notes within a selected communication mode. Notes are constrained textual objects with fixed spatial rendering rules and do not support scrolling or expansion.

Public Notes are additionally subject to bounded contextual occupancy constraints. Each URL instance permits only a fixed maximum number of simultaneously visible Public Notes, limiting conversational density and preserving contextual legibility and visual clarity within the annotated space. In the current implementation, this limit is fixed at 20 Public Notes per URL instance.

Notes support full Unicode text rendering, enabling multilingual and cross-script expression within constrained annotation spaces. This includes support for non-Latin writing systems, symbols, and emoji-based communication. Importantly, expressive flexibility is preserved despite the bounded spatial constraints of the Note model, allowing stylistic and linguistic variation without privileging specific languages or scripts.

6.2 Engagement Semantics

Engagement events are recorded but not surfaced as comparative or competitive signals. There is no mechanism for users to observe relative performance of Notes or authors.

6.3 Recipient Control and Silent Discard

Recipients of Exclusive Notes and Group Notes may silently discard messages without notifying senders. This introduces unilateral reception control and decouples distribution intent from guaranteed delivery.

7. Social Structure and Identity

NetNubby maintains a pseudonymous identity model in which monikers function as stable but non-authoritative identifiers. The system does not expose global social graphs, follower structures, or reputation metrics.

Social structure exists only through user-defined tribes and localized interaction patterns. Importantly, the system does not operationalize these structures into visibility or ranking mechanisms, nor does it elevate them into persistent public reputation systems or algorithmically amplified identity constructs.

8. System Distinction from Conventional Social Media

NetNubby diverges from conventional social platforms along several axes:

8.1 Absence of Engagement Economies

Unlike platforms such as Reddit or Tumblr, NetNubby does not expose engagement metrics or use them for ranking or amplification.

8.2 Context-First Communication

Communication is anchored to URLs rather than centralized feeds or algorithmically curated timelines. Unlike services such as Hypothes.is, content is not bound to fragments of page content.

8.3 Non-Operational Social Graphs

While interaction data and relational structures may exist internally, they are not exposed or operationalized as user-facing social graphs.

8.4 Decoupled Identity and Feedback

Identity is maintained for coordination purposes but is not coupled to public feedback systems or reputation mechanisms.

9. Discussion

The NetNubby architecture occupies a design space characterized by intentional decoupling of expression, identity, and engagement visibility. By suppressing social metric exposure and enforcing modal separation, the system seeks to reduce performative behavior driven by attention optimization while preserving localized communicative functionality within its sphere.

However, the system introduces asymmetric visibility between user interaction and system-level observation, raising questions regarding interpretability, transparency, and

long-term behavioral adaptation. Additionally, the presence of external coordination channels for tribe formation suggests that relational structure may partially externalize beyond system boundaries.

10. Conclusion

NetNubby represents a context-bound annotation system that intentionally avoids conventional social media feedback architectures. Its defining characteristic is not the absence of social interaction, but rather the refusal to transform interaction into visible, comparable, or rankable social structure. This design positions NetNubby as a non-normative alternative within the landscape of social computing systems, emphasizing contextual expression over engagement-driven visibility.

11. Threat Model and Abuse Analysis

11.1 Overview

Although NetNubby suppresses many conventional social media dynamics (e.g., public engagement metrics and follower-based amplification), its design introduces a distinct set of interactional tensions and misuse possibilities shaped by contextual posting, pseudonymous identity, and asymmetric visibility of interaction signals.

This section outlines potential misuse scenarios and interactional tensions introduced by the system's design choices, and evaluates how NetNubby constrains, tolerates, or redistributes these behaviors within its broader interaction philosophy.

11.2 Spam and Contextual Pollution

Threat: Adversaries may inject irrelevant or repetitive Notes into high-visibility URL contexts, effectively polluting the contextual annotation layer.

Mitigations:

- Per-URL Note caps (bounded density constraint)
- Time-to-expiry defaults for Public Notes
- Mode isolation preventing cross-contamination of communication types

Residual Risk: High-traffic URLs remain attractive targets for low-effort spam bursts due to contextual concentration of attention.

11.3 Coordinated Harassment in Group Channels

Threat: Tribes may be used to repeatedly target individuals with unwanted Group Notes, constituting low-grade harassment.

Mitigations:

- Maximum tribe size constraint limits blast radius
- Recipient-side silent discard reduces feedback reinforcement
- Lack of sender-side delivery confirmation reduces adversarial optimization loops

Residual Risk: Absence of explicit reporting feedback to sender may reduce deterrence while also limiting escalation visibility.

11.4 Impersonation and False Authority Claims

Threat: Pseudonymous Notes may assert false authority (e.g., pretending to be official communication on a website context).

Mitigations:

- Moniker-based pseudonymity reduces real-world identity spoofing
- Skeuomorphic design and clearly branded Note layer reduces UI confusion risk
- Absence of privileged verification channels prevents escalation to “verified authority” status within system

Residual Risk: Users must rely on external trust heuristics; the system does not resolve authenticity disputes at the identity layer.

11.5 Sybil Attacks and Account Proliferation

Threat: Adversaries may create multiple pseudonymous accounts to amplify Notes, simulate consensus, or bypass moderation constraints.

Mitigations:

- Email-based account anchoring introduces minimal friction cost
- Cohort-based interaction logging enables backend anomaly detection
- Lack of visible engagement metrics reduces payoff of manufactured consensus

Residual Risk: Internal detection systems become the primary defense layer, increasing reliance on opaque enforcement mechanisms.

11.6 Abuse of Silent Discard Semantics

Threat: Recipients may systematically discard messages without engagement, enabling invisible suppression of communication.

Mitigations:

- Tribe size caps reduce large-scale targeting incentives
- No sender-side visibility prevents retaliatory optimization

Residual Risk: Silent discard intentionally preserves recipient autonomy by withholding delivery and engagement visibility from senders. While this reduces interpretability of message reception, it also suppresses obligation signaling and reactive optimization behaviors common in conventional messaging systems.

From the perspective of NetNubby's interaction philosophy, this ambiguity is considered a net gain rather than a systemic deficiency.

11.7 Context Hijacking of URL Spaces

Threat: High-traffic URLs may become contested spaces where Notes attempt to reframe or dominate contextual interpretation of the underlying page.

Mitigations:

- Strict Note density caps per URL instance
- Mode separation ensures only one communication layer is visible at a time
- Temporal decay of Public Notes limits long-term occupation

Additionally, NetNubby introduces a voluntary cooperative mechanism through the **X-DIGITAL-NOTE-OPTIONS** HTTP response header, allowing site operators to request suppression of Public Notes on specific resources. While the annotation layer remains client-side and user-mediated, this mechanism provides a protocol-level means for websites to express contextual annotation preferences without requiring centralized platform negotiation, content modification, or the issuance or adjustment of Content Security Policy (CSP) directives intended to mitigate annotation behavior.

To the authors' knowledge, this represents an uncommon example of a web annotation system exposing a standardized, site-operator-readable preference mechanism at the HTTP protocol layer.

Residual Risk: Popular contexts remain inherently adversarial due to shared attention concentration, particularly where high-traffic resources attract competing attempts to shape or influence contextual interpretation.

11.8 System-Level Asymmetry and Opaqueness

Threat: Internal use of cohorts for system integrity introduces asymmetric observability between system and users.

Mitigations:

- Cohorts are explicitly non-exposed and non-representational
- No user-facing social inference is derived from cohort data

Residual Risk: This asymmetry reflects a deliberate prioritization of user-facing simplicity and reduced social visibility over fully symmetric observability.

11.9 Summary

NetNubby's threat model is characterized not by engagement amplification risks typical of social media systems, but by contextual concentration risks, pseudonymous abuse vectors, and asymmetric system visibility. The system mitigates many conventional social computing vulnerabilities while introducing a new class of risks centered on contextual integrity, interpretability, and invisible interaction governance.

12. Related Work

NetNubby occupies an intersection of web annotation systems, decentralized communication tools, and anti-engagement social architectures. Several prior systems inform its design space.

12.1 Web Annotation Systems

Systems such as Hypothes.is and earlier web annotation projects (e.g., Third Voice) introduced the concept of persistent, user-generated overlays on web content. These systems typically emphasize collaborative annotation and knowledge layering but differ from NetNubby in their openness of social signaling and lack of strict mode separation.

12.2 W3C Web Annotation Standard

The W3C Web Annotation Data Model defines a standardized framework for associating annotations with web resources (e.g., targets, bodies, selectors, and motivations). NetNubby is compatible at a conceptual level with this model insofar as Notes are bound to URL contexts and represent user-authored annotation bodies.

However, NetNubby's primary contribution lies above the data model layer. While the W3C standard focuses on representation and interoperability, NetNubby introduces a constrained socio-technical layer that governs how annotations are created, viewed, interpreted, and behaviorally contextualized within bounded interaction environments.

In particular, it:

- Enforces strict modality separation (Public, Personal, Exclusive, Group, Local)
- Suppresses public aggregation of interaction signals
- Avoids ranking, recommendation, and visibility amplification based on engagement
- Introduces asymmetric interaction semantics (e.g., silent discard; non-exposed cohort signals)

Accordingly, NetNubby should be understood not as an implementation of the W3C standard, but as a system that leverages annotation primitives while redefining their social meaning and interaction dynamics.

12.3 Social Media Platforms and Engagement Economies

Platforms such as Reddit and Tumblr operationalize engagement through visible metrics (upvotes, likes, reblogs) that contribute directly to content ranking and social visibility. NetNubby explicitly decouples these signals from user-facing interfaces to avoid engagement-based amplification loops.

12.4 Federated and Decentralized Social Systems

ActivityPub-based systems (e.g., Mastodon) distribute social graphs across servers but retain explicit follower/following relationships. NetNubby diverges by limiting explicit social graph visibility and constraining group size and message delivery semantics.

12.5 Ephemeral and Contextual Communication Tools

Temporary messaging systems (e.g., disappearing message platforms) share NetNubby's interest in temporal decay, though they typically operate in private messaging contexts rather than URL-bound public annotation spaces.

13. Privacy and Security Model

13.0 Account Authentication Model

NetNubby employs a pseudonymous account model with a security-oriented authentication design. Accounts are protected using Argon2-based password hashing, and authentication requires two user-defined, non-public identifiers: a username and a passphrase. Neither identifier is exposed within the system's public interface.

Importantly, email addresses are not used as login identifiers. While an email may be associated with an account for recovery or optional discovery, it is not treated as a primary credential. This contrasts with common platform practices in which email functions as a partial or primary authentication factor.

This design reduces reliance on externally discoverable identifiers and reinforces the system's broader goals of minimizing identity exposure, limiting account enumeration risk, and decoupling authentication from public-facing identity constructs. Resistance to account discovery is treated as a first-class design objective within the authentication

model, reducing reliance on externally identifiable credentials and limiting opportunities for unsolicited account targeting, enumeration, or identity correlation across contexts.

13.1 Definitions

NetNubby distinguishes three overlapping but non-equivalent concepts:

- **Privacy:** The degree to which user activity or behavior is hidden from other users or external observers (including the platform itself).
- **Security:** The degree to which user data is protected from unauthorized access or modification at the system level.
- **Anonymity:** The degree to which user identity cannot be inferred from either a lack of privacy or a breakdown of security.

13.2 System Positioning

NetNubby provides partial privacy, strong pseudonymity, and controlled security guarantees:

- The system is **not fully private from the service operator**, as Notes and interactions are stored server-side.
- The system is **pseudonymous rather than fully anonymous**, as monikers provide persistent but non-real-world identity anchors.
- The system is **externally non-indexed by design**, limiting global discoverability of Notes without explicit URL context.

13.3 Observability and Internal Access

While user-facing interfaces suppress aggregation and social inference, the backend system retains the ability to inspect Notes and interaction events for moderation, abuse detection, and system integrity.

This creates an intentional asymmetry between user observability and system observability, in which the platform retains limited operational visibility while deliberately restricting the exposure of interactional and relational signals to participants themselves.

13.4 Threat Surface Implications

The privacy model implies several security-relevant properties:

- Reduced public discoverability limits mass surveillance of content aggregation.
- Pseudonymity reduces direct identity linkage but does not eliminate behavioral inference risk.
- Internal system visibility introduces a trusted operator model rather than a fully decentralized trustless model.

13.5 Summary

NetNubby's privacy and security model prioritizes pseudonymous expression and reduced social visibility over strict end-to-end opacity. It trades full user-to-system symmetry for structural suppression of social metric exposure and identity-driven amplification

mechanisms, prioritizing reduced performative pressure and constrained visibility over comprehensive interaction transparency.

14. Design Space

14.0 Network Substrate Axis

An additional distinguishing dimension is the underlying network substrate on which annotated resources reside:

- **Clearnet systems:** DNS-based, centralized hosting
- **Decentralized systems:** content-addressed networks (e.g., IPFS)
- **Anonymity networks:** onion services over Tor
- **Local resources:** file-based documents accessed via browser (file:///)

NetNubby spans all four, maintaining consistent interaction semantics across heterogeneous network layers. This contrasts with most social and annotation systems, which are tightly coupled to the clearnet.

This property reinforces NetNubby's abstraction of "resource as context," independent of how that resource is addressed or retrieved.

14.1 Engagement Visibility Axis

NetNubby can be situated within a multi-dimensional design space for socio-technical systems. This section identifies key axes along which it differentiates itself from conventional social media and annotation platforms.

14.1 Engagement Visibility Axis

- **High visibility systems:** Explicit likes, follower counts, public metrics (e.g., Reddit, Tumblr, Facebook)
- **NetNubby position:** Engagement exists only as non-exposed system signals (cohorts), with no user-facing metrics

14.2 Social Graph Explicitness Axis

- **Explicit graphs:** Followers, friends, subscriptions
- **Implicit graphs:** Behavioral inference, recommendation networks
- **NetNubby position:** Minimal explicit graphs (tribes capped, non-public) and suppressed inference surfaces

14.3 Context Anchoring Axis

- **Feed-based systems:** Content detached from origin context
- **Hybrid systems:** Mix of feed and contextual content
- **NetNubby position:** Strong URL-bound anchoring; context is the primary organizational unit

14.4 Reciprocity Symmetry Axis

- **Symmetric systems:** Mutual visibility of interactions (likes, follows, read receipts)
- **Asymmetric systems:** Hidden or partial feedback loops
- **NetNubby position:** Strong asymmetry via silent discard and non-exposed cohort signals that intentionally limit reciprocal social visibility

14.5 Temporal Persistence Axis

- **Persistent systems:** Content remains indefinitely and accumulates engagement
- **Ephemeral systems:** Content decays or disappears
- **NetNubby position:** Hybrid temporal model with default expiry for Public Notes and bounded per-URL density constraints

15. Limitations and Ethical Considerations

15.1 Systemic Opacity

NetNubby intentionally limits the visibility of many interactional and relational signals that are commonly surfaced in conventional social platforms. Structures such as cohorts, delivery outcomes, and engagement patterns remain partially or fully non-exposed to platform users.

This opacity is not primarily intended to obscure system behavior, but rather to reduce performative social optimization, obligation signaling, and engagement-driven interaction dynamics. By constraining social visibility, the system attempts to preserve contextual communication while minimizing pressure toward audience management and behavioral self-monitoring.

However, these design choices also reduce the interpretability of certain interaction states and may complicate user understanding of message reception, relational structure, or broader participation patterns.

In conventional social systems, increased transparency is often associated with improved coordination and engagement optimization. NetNubby intentionally questions this assumption by treating partial opacity as a mechanism for reducing performative social behavior and preserving user autonomy.

15.2 Silent Discard Ambiguity

Recipient-side silent discard in Exclusive and Group Notes removes delivery feedback, which preserves autonomy but eliminates sender-side awareness of communication efficacy. This may complicate social coordination and reduce communicative accountability within interactions that would otherwise rely on explicit reciprocal visibility or delivery confirmation mechanisms.

15.3 External Coordination Dependence

The system anticipates and does not discourage off-platform coordination for tribe formation. While this preserves user autonomy, it may reduce the platform's completeness as a standalone social system and shift relational structure outside its governance boundary.

15.4 Potential for Informal Social Structures

Despite suppression of explicit social graphs, users may still form informal or emergent social hierarchies based on stylistic recognition, repeated interaction patterns, or off-platform coordination. This suggests that social structure may be considered to be displaced rather than fully eliminated or squelched.

15.5 Abuse and Misrepresentation Risks

Pseudonymous Notes may be used for impersonation or false authority signaling on contextual pages. Although system design reduces amplification mechanics, it does not eliminate the potential for localized deception.

15.6 Ethical Tradeoffs in Asymmetric Visibility

The system's reliance on internal-only interaction data (cohorts) creates ethical tension between abuse mitigation and user transparency. This tradeoff reflects a design choice prioritizing behavioral safety over full observability.

NetNubby intentionally sacrifices communicative transparency in order to preserve autonomy and reduce social pressure dynamics.

From the perspective of conventional platform design, this may appear to reduce interactional efficiency. However, NetNubby treats reduced visibility and interpretability as protective constraints that limit obligation signaling, behavioral optimization, and engagement-driven social pressure.

15.7 Summary

NetNubby's design introduces a set of ethical and structural tradeoffs centered on opacity, autonomy, and contextual communication. While it reduces engagement-driven harms common in social media systems, it intentionally declines to internalize many forms of social coordination and relationship management common to conventional platforms.