ISSN: 3143-8458

Wissen PUBLICATION GROUP

Journal of
Artificial Intelligence and Data Analytics

Research Article

Volume: 1 | Isssue: 1 | April 2026 | Pages 01 –11

Deep Personal Privacy as Network Impedance: A Diffusion-Based Model of Knowledge Flow

Yair Oppenheim

The Lester and Sally Antin Faculty of Humanities, Tel Aviv University, Tel Aviv, Israel

***Corresponding Author:** Yair Oppenheim, The Lester and Sally Antin Faculty of Humanities, Tel Aviv University, Tel Aviv, Israel.

Submitted: 01 April 2026 **Accepted:** 06 April 2026 **Published:** 15 April 2026

Citation: Oppenheim, Y. (2026). Deep Personal Privacy as Network Impedance: A Diffusion-Based Model of Knowledge Flow. Journal of Artificial Intelligence and Data Analytics, 1(1), 1-11. DOI: doi.org/10.67927/JAIDataAnalytics/2026(1)103.

Abstract

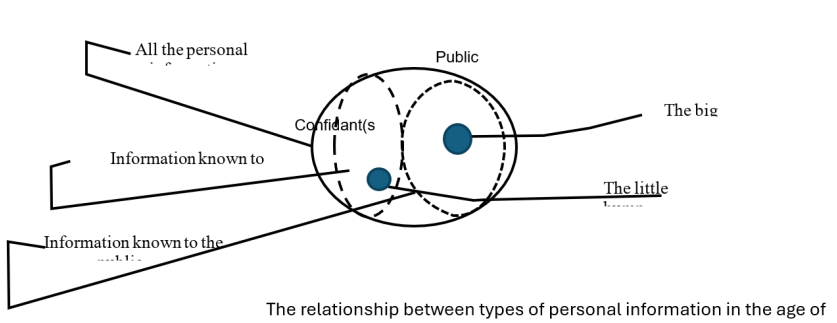
This paper introduces a novel theoretical and mathematical framework for Deep Personal Privacy (DPP), conceptualized as a network-level impedance to the diffusion of knowledge about individuals. Moving beyond traditional binary notions of privacy as secrecy versus disclosure, the model reframes privacy as a dynamic, system-wide resistance governing the propagation of novel information across interconnected data ecosystems. By integrating graph-theoretic structures with a novelty-driven, non-conservative diffusion process, the framework captures the non-rival and accumulative nature of knowledge. A central innovation is the identification of the directed novelty gradient as the unifying driver of both knowledge diffusion and privacy erosion. The analysis further shows that AI systems act as high-connectivity inference hubs that structurally reduce privacy impedance and accelerate adversarial knowledge acquisition. The proposed DPP framework establishes a rigorous link between network topology, diffusion dynamics, and privacy loss, positioning privacy as a measurable, system-level property and offering a new foundation for ethical and regulatory analysis in AI-driven environments.

Keywords: Deep Personal Privacy (DPP), Information Diffusion, Network Impedance, Knowledge Propagation, Privacy Risk, Artificial Intelligence, Network Science, AI Ethics.

Introduction

Personal Privacy as Information

Many attempts have been made to redefine personal privacy[1], none of them adequate [1-6]. In this article, I replace the discussion about personal privacy with discussion of personal privacy information. The central argument is that replacing the discourse on personal privacy with one on personal privacy information is justifiable, supported by several points: personal privacy information can be digitized and detached from the individual; personal privacy is fundamentally viewed as personal privacy information; and any discussion about personal privacy is, in essence, a discussion about this information [7,8]. The relationship between deep privacy, general privacy and personal information in general in the age of ICTs can be represented by the following graph. The outermost oval represents all the personal information about an individual, the dashed oval represents the personal information known to confidants, and the dotted oval represents the personal information that is known to the public[2] [8].



The relationship between types of personal information in the age of

[1]Personal privacy is the type of privacy that applies to individual humans, unlike general privacy, which also applies to organizations, corporations and agencies

[2]"humps" – information about the individual that is known to others (one or more confidants or the general public) but not known to, possessed by or controlled by the individual who is the information subject

Deep personal privacy information (information known only to the person in question) is all the area outside the dashed and dotted ovals.

General personal privacy information is the entire area of the outermost oval minus the area of the dotted oval.

Digital technologies have transformed the structure of personal information ecosystems. Modern individuals interact with numerous information systems including social networks, databases, sensors, and AI-based analytics platforms. Information about a person rarely resides in a single location; rather, it is distributed across multiple interconnected sources.

Traditional privacy frameworks focus on protecting specific datasets or attributes. However, privacy loss often occurs through **inference across multiple sources,** where partial information fragments are combined to produce knowledge about an individual.

Diffusion Information Process

Diffusion is commonly understood as the process by which information, behaviors, or states spread across a network over time, typically driven by interactions among agents and structural properties of the network [9-11]. Classical models of diffusion rely on graph-theoretic formulations, particularly Laplacian-based dynamics, which assume conservative flow and have been widely applied to model physical, social, and informational processes.

Recent advances extend these classical approaches by incorporating temporal dynamics, probabilistic mechanisms, and machine learning techniques. Studies have shown that both network topology and time-dependent interactions critically influence diffusion patterns in complex systems [12]. Graph Neural Networks (GNNs) have further enabled the prediction and analysis of information diffusion by capturing structural dependencies between nodes and learning propagation patterns from data [13].

Moreover, diffusion has emerged as a central paradigm in modern artificial intelligence. Diffusion models, widely used in generative AI, describe stochastic processes that gradually transform noise into structured data, offering a probabilistic interpretation of information propagation and reconstruction [14].

Importantly, work highlights that diffusion processes themselves may introduce significant privacy risks [15]. In graph-based systems, diffusion can expose sensitive relational information, motivating the integration of differential privacy mechanisms to mitigate leakage [15]. Furthermore, diffusion-based models have been shown to enable inference attacks capable of reconstructing hidden structures and extracting sensitive data, particularly in AI-driven environments [16].

Despite these advances, existing frameworks largely treat diffusion as either a predictive or generative process, without explicitly linking it to privacy degradation. This paper builds on these foundations and proposes a novel perspective in which diffusion is directly connected to privacy loss through a novelty-driven propagation mechanism.

This Paper Makes Four Main Contributions

- **A Novel Conceptualization of Privacy**
  It reconceptualizes personal privacy as a network-level impedance to knowledge diffusion, moving beyond traditional data-centric and binary frameworks.
- **A New Mathematical Model of Knowledge Propagation**
  It introduces a novelty-driven, non-conservative diffusion model grounded in set-theoretic and scalar formulations, capturing the non-rival and accumulative nature of information.
- **A Unified Quantitative Framework Linking Diffusion and Privacy**
  It identifies the directed novelty gradient as the fundamental quantity governing both knowledge propagation and privacy erosion, thereby establishing a formal connection between network dynamics and privacy loss.
- **A Structural Analysis of AI-Driven Privacy Risk**
  It demonstrates that AI systems act as high-connectivity inference hubs that reduce privacy impedance, accelerate knowledge aggregation, and structurally amplify privacy risks across heterogeneous data sources.

These contributions are developed in Sections 2–4.

Deep Personal Privacy (DPP) as Network Impedance

In this model: personal information flows through a network, Privacy mechanisms act as resistance, AI systems reduce resistance by integrating information sources.

The proposed framework interprets personal privacy as a structural property of information networks. Personal information flows through a network of interconnected nodes, while privacy mechanisms act as resistance. AI systems reduce this resistance by integrating information across sources. Thus, privacy is not a binary condition but a dynamic property determined by network topology and information flow. This allows privacy to be analyzed quantitatively using network theory.

Related Work

Research on privacy has traditionally focused on data protection mechanisms such as differential privacy, privacy-preserving machine learning, and statistical disclosure limitation [17]. These approaches aim to control access to sensitive data or limit the information that can be inferred from datasets. More recent work has highlighted the risks of inference attacks, including membership inference and data extraction attacks, demonstrating that privacy leakage can occur even without direct access to raw data [18,19].

In parallel, the study of information diffusion in networks has been extensively developed using graph-theoretic frameworks. Classical models rely on Laplacian dynamics [9,10], which assume conservative flow. These models have been applied to social contagion, epidemic spreading, and information cascades. However, such formulations do not capture the non-rival nature of knowledge, where information is replicated rather than transferred.

Recent research on complex systems and network science has emphasized the importance of topology, connectivity, and dynamic processes in shaping system behavior. In particular, non-equilibrium systems provide a useful lens for understanding continuously evolving environments in which new information is constantly generated.

Despite these advances, existing frameworks do not provide a unified model that connects knowledge diffusion, inference processes, and privacy degradation. The present work addresses

this gap by introducing a novelty-driven diffusion model and defining privacy as a network-level impedance to knowledge flow. This approach bridges privacy theory, network dynamics, and AI-driven inference, offering a new structural perspective on privacy risk.

Information Networks

We model the information ecosystem surrounding an individual as a weighted graph [10,11].$G=(V,E)$. Were

- Vi {I =1,2, 3,…,n} the set of information nodes
- Ej {j =1,2, 3,…,m} the set of information channels

Examples of nodes include:

- social media platforms
- public databases
- data brokers
- Machine Learning Systems
- sensor infrastructures, Internet application [13,17].

Each edge (i,j) is assigned a **conductivity weight** $w_{ij}\geq 0$ representing the strength of information flow or inferential capability between nodes [9,10].

Knowledge Diffusion

Knowledge Propagation as Novelty-Driven Non-Conservative Diffusion

In classical network diffusion models, the evolution of a quantity over a graph is typically governed by the Laplacian operator [9, 10]: $K(t+1)=K(t)-\alpha LK(t)$,

where L=D-W is the graph Laplacian. This formulation assumes **conservative flow**, meaning that the quantity transferred from one node is subtracted from the source and added to the destination. Such models are appropriate for physical processes such as heat diffusion, mass transport, or electrical flow [19].

However, **knowledge propagation in informational networks fundamentally differs from physical diffusion [7,9]**. Information is **non-rival**: when a node transmits knowledge, it does not lose it. Moreover, a receiving node should only increase its knowledge through **novel information**, i.e., information that it does not already possess.

Limitation of Laplacian-Based Models

The Laplacian formulation implicitly enforces conservation:

- Knowledge flowing from node i to node j reduces the state at node i.
- The total quantity across the network is preserved.
- These assumptions are incompatible with informational processes, where:
- Knowledge is **replicable** rather than conserved [9,18].
- Sources retain their knowledge after transmission.
- Repeated exposure to the same information does not increase knowledge indefinitely.
- Thus, a different mathematical formulation is required.

Novelty-Driven Knowledge Propagation Model

Let K_i (t)denote the amount of knowledge about an individual available at node i at time t, and define the state vector: $K(t)=(K_1(t),K_2(t),\ldots,K_n(t))^T$.

Let $W=[w_{ji}]$ be a weighted adjacency (influence) matrix, where $w_{ji}\geq 0$ quantifies the strength of information transfer from node i to node j.

To ensure that only **novel knowledge** contributes to the receiving node, we define the **Set-Theoretic Model of Knowledge (Fundamental Formulation).**

A faithful representation of knowledge treats it as a **set of informational elements [7,8].** Let: $S_i(t)$denote the set of knowledge items available at node i at time t. The **novel knowledge** that can flow from node ito node j is given by the set difference: $Si(t)\backslash Sj(t)$. Let $Tji(t)\subseteq S_i(t)\backslash S_j(t)$ denote the subset of knowledge actually transmitted from i to j.The update rule is:$S_j(t+1)=S_j(t)\cup\bigcup_{i=1}^{n}T_{ji}(t)$.

Interpretation of the Set Model

This formulation captures the true epistemic structure of knowledge propagation:

- Knowledge is **accumulated via union**, not transferred via subtraction [7].
- Only **previously unknown information** contributes to growth.
- Once an item is known, it **cannot increase knowledge again** through repetition.

Thus, propagation is inherently **non-conservative and novelty based.**

- **Novelty-Driven Knowledge Propagation with a Single Information Source**
  We consider a network of three nodes, where node 1 represents the unique source of information and corresponds to the individual. Nodes 2 and 3 represent external entities that possess partial knowledge about the individual.
- **Model Assumptions**
  The model is defined under the following assumptions.
- **Single-Source Information Generation**
  All information about the individual originates at node 1. Formally, there exists a finite set of information items: $U=\{a,b,c,d\}$, such that:$S_1(0)=U$.
- **No External Information ("No Hump" Condition)**
  Nodes 2and 3cannot possess any information that is not already contained in U. That is: $S_i(t)\subseteq$U"for all " $i\in\{2,3\}$," " $t\geq 0$.
- **Epistemically One-Directional Information Flow**
  Although nodes 2 and 3 may exchange information between themselves, all information ultimately originates from node 1. Thus, there is no independent information creation outside the source node.
- **Partial Initial Knowledge**
  At time t=0, nodes 2 and 3 possess strict subsets of U: $S_2(0)=\{a\}$,$S_3(0)=\{b\}$.
- **Stochastic Single-Item Broadcasting**
  At each discrete time step t, every node irandomly selects a single item:$x_i(t)\in S_i(t)$, and broadcasts it to all neighboring nodes [12].
- **Novelty-Based Update Rule**
  Each receiving node updates its knowledge set by incorporating only novel items. Formally:S_j (t+1)=S_j (t)∪{x_i (t):w_{ji}=1}, where $w_{ji}\in\{0,1\}$denotes the network adjacency.

Network Structure
We consider the following influence (adjacency) matrix:

$$W = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

where w_{ji}=1 indicates that node i can transmit information to node j. In particular: Node 1 transmits to nodes 2 and 3. Nodes 2 and 3 can exchange information. Node 1 does not receive information from other nodes.

System Evolution
We illustrate one possible realization of the stochastic process over time.
Time t=0 $S_1(0)=\{a,b,c,d\}$, $S_2(0)=\{a\}$, $S_3(0)=\{b\}$.
Time t=1 Assume the following random selections: Node 1 broadcasts c, Node 2 broadcasts a, Node 3 broadcasts b. Then: Node 2 receives c(from node 1) and b (from node 3): $S_2(1)=\{a,b,c\}$ Node 3receives c (from node 1) and a (from node 2) :$S_3(1)=\{a,b,c\}$, Node 1nremains unchanged: $S_1(1)=\{a,b,c,d\}$
Time t=2
Assume: Node 1 broadcasts d, Node 2 broadcasts c, Node 3 broadcasts a
Then: Node 2 receives d(new): $S_2(2)=\{a,b,c,d\}$. Node 3 receives d(new):$S_3(2)=\{a,b,c,d\}$, Node 1 remains unchanged:$S_1(2)=\{a,b,c,d\}$
Time t=3All nodes already possess the full set U. Any further transmissions produce no change: $S_1(3)=S_2(3)=S_3(3)=\{a,b,c,d\}$.

Discussion
This example illustrates several key properties of novelty-driven knowledge propagation:

- **Monotonicity:** Knowledge sets grow monotonically via union operations.
- **Non-Depletive Dynamics:** The source node retains all information throughout the process.
- **Novelty Constraint:** Only previously unknown items contribute to knowledge growth.
- **Convergence to Closure:** The system converges to the global knowledge set:

$$\lim_{t\to\infty} S_i(t) = \bigcup_{k=1}^{3} S_k(0) = U.$$

Thus, knowledge propagation can be understood as a **distributed process of set completion,** driven by the gradual elimination of informational asymmetries across the network.

According to Oppenheim y., Personal privacy information is a form of order, reflecting the legal, social, and institutional structures that define ownership and control over personal data [1].

These determine the degree of order in personal privacy. An increase in entropy means a decrease in the degree of that order. The process of personal information leaking out of the private sphere into the public sphere may be compared to Heat Diffusion from one container to another until they reach equal heat, in accordance with the second law of thermodynamics [19].

Theorem: Convergence to Union Closure under Novelty-Driven Propagation
Setting: Let $G=(V,E)$ be a directed graph with $V=\{1,\ldots,n\}$ and adjacent matrix $W=[wji]\in\{0,1\}^{(n\times n)}$.Let $S_i(t)\subseteq$Udenote the knowledge set at node i at time t, where U is a finite universe of information items. Assume:

- **Finite Universe:** |U|<∞.
- **Single-Source Containment:** $S_i(0)\subseteq$Ufor all i.
- **Novelty-Driven Update:** $S_j(t+1)=S_j(t)\cup\{x_i(t):w_{ji}=1\}, x_i(t)\in S_i(t)$.
- **Fairness (Weak Persistence):** For every directed edge i→jand every item u∈$S_i(0)$, the event "u is eventually broadcast by i" occurs infinitely often (or at least once along some path to j).

Define the global union: $U^\star = \bigcup_{k=1}^{n} S_k(0) \subseteq U.$

Statement
Under the above assumptions, for every node $i \in V$, $\lim_{t\to\infty} S_i(t) = U^\star$.

Moreover, the process converges in finite time (almost surely under i..d. random broadcasting), and the limit is the union closure of the initial knowledge sets.
Proof:

(Monotonicity) By construction, $S_j(t+1) = S_j(t)\cup(\cdot)$, hence $S_j(t)\subseteq S_j(t+1)\forall j,t$. Thus, each sequence $\{S_j(t)\}$is monotone non-decreasing.

(Boundedness)
All sets are subsets of $U^\star$, hence the sequences are bounded above: $S_j(t)\subseteq U(^\star)\forall j,t$.
Since U*is finite, each $S_j(t)$ can increase only finitely many times. Therefore, each sequence stabilizes in finite time: $\exists T_j < \infty$ such that $S_j(t) = S_j(T_j)\ \forall t \geq T_j$
Let T=$\max_j T_j$. Then for all t≥T, the system is at a fixed point.

(Attainment of the Union)
Fix any item u∈U*. Then u∈$S_k(0)$for some node k. By the fairness assumption and graph connectivity (reachability), there exists a sequence of transmissions along a directed path from k to any node i, such that u is eventually broadcast along that path and included in S_i (t). Thus, for all i, u∈$S_i(t)$ for sufficiently large t. Since uwas arbitrary, $Si(t)\to U^\star$.

Remark (Interpretation)
The dynamics implement a distributed set-union computation [7]: nodes iteratively eliminate informational asymmetries until all possess the same knowledge—the union of all initial knowledge sets.

Definition: Knowledge Gradient and DPP
We now connect the propagation mechanism to a quantitative notion of privacy risk.

Let $K_i(t) = \mu(S_i(t))$, where μ is a monotone set measure (e.g., cardinality, weighted measure, or entropy) [7].

Directed Knowledge Gradient
Define the novelty (directed) gradient from node i to node j as:Δ_(i→j) (t)=μ($S_i(t)\setminus S_j(t)$). In the scalar approximation: $\Delta_{(i\to j)}(t)\approx(K_i(t)-K_j(t))_+$. Network-Wide Knowledge Gradient (Flow Functional).

Define the total novelty-driven flow: $\Phi(t) = \sum_{i,j} w_{ji}\ \Delta_{i\to j}(t)$.

In scalar form: $\Phi(t) \approx \sum_{i,j} w_{ji}\ (K_i(t) - K_j(t))_+$.Deep Personal Privacy (DPP) as Impedance to Knowledge FlowWe define Deep Personal Privacy (DPP) as an inverse functional of the network's ability to propagate novel knowledge: $\mathrm{DPP}(t) = \frac{1}{1+\Phi(t)}$.Properties.

- **Non-Negativity:** Φ(t)≥0, hence 0<DPP(t)≤1.
- **Monotonicity of Exposure:** As knowledge spreads, Φ(t) decreases (gradients vanish), and the system approaches equilibrium.
- **Maximal Privacy (No Gradients):**
- If $S_i(t)=S_j(t)\ \ \forall i,j$, then $\Phi(t)=0$ and DPP(t)=1.
- Maximal Exposure Phase: Large gradients (high asymmetry) imply large Φ(t) and lower DPP.
- Interpretation
- Φ(t)measures the total actionable novelty in the network—the amount of information that can still propagate.
- DPP quantifies the resistance (impedance) to that propagation.
- As the system converges to union closure, novelty vanishes, gradients collapse, and the propagation process saturates.

Link to the Scalar Dynamics

The scalar update: $K_j(t+1) = K_j(t) + \alpha \sum_i w_{ji}\,(K_i(t) - K_j(t))_+$

is a gradient-driven accumulation rule, where each node integrates incoming novelty proportional to the local gradient.

Thus, the same quantity $(K_i\text{-}K_j)_+$ simultaneously:
- drives the dynamics, and
- defines the privacy-relevant flow functional Φ(t).

Key Insight for the Paper

Knowledge propagation and privacy loss are governed by the same underlying object: the directed novelty gradient across the network [18,19].

Example: Scalar Novelty-Driven Propagation with Partial Information Transfer

Model Setting: We consider a three-node network in which node 1is the unique source of information representing the individual. Nodes 2 and 3 possess partial knowledge about node 1. Let the universe of information be:$U=\{a,b,c,d\}$,and define the scalar knowledge level: $K_i(t) = \mu(S_i(t)) = |S_i(t)|$.Initial conditions:$K_1(0)=4, K_2(0)=1, K_3(0)=1$.

Partial Information Transfer

Unlike the binary case, we now assume fractional transmission capacity: $0\le w_{ji}\le 1$.
where w_{ji} represents the fraction of available novel information that is effectively transmitted from node i to node j.

Propagation Model: The scalar update rule becomes:

$K_j(t+1) = K_j(t) + \alpha \sum_{i=1}^{n} w_{ji}\ (K_i(t) - K_j(t))_+$, where:

- $(x)_+$=max (x,0)
- $\alpha\in(0,1)$ is a propagation rate

Network Structure - We define: $W = \begin{pmatrix} 0 & 0 & 0 \\ 0.8 & 0 & 0.3 \\ 0.6 & 0.5 & 0 \end{pmatrix}$

Interpretation: Node 1 → Node 2: strong influence (0.8), Node 1 → Node 3: moderate influence, (0.6), Node 2 → Node 3: medium (0.5), Node 3 → Node 2: weak (0.3). Let:α=0.5. Time Evolution $\mathbf{Time\ t = 0} - K(0) = \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix}$Gradients:$(K_1 - K_2)_+ = 3, (K_1 - K_3)_+ = 3, (K_2 - K_3)_+ = 0, (K_3 - K_2)_+ = 0$

Flow: Φ(0)=(0.8·3+0.6·3+0.5·0+0.3·0)=(2.4+1.8)=4.2DPP:

$$DPP(0) = \frac{1}{1+4.2} \approx 0.192$$

Timet=1-Update[3]:$K_2(1)=1+0.5\cdot(0.8\cdot 3)=1+1.2=2.2$, $K_3(1)=1+0.5\cdot(0.6\cdot 3)=1+0.9=1.9$, $K_1(1) = 4. K(1) = \begin{pmatrix} 4 \\ 2.2 \\ 1.9 \end{pmatrix}$,

Gradients: $(K_1\text{-}K_2)_+=1.8, (K_1\text{-}K_3)_+=2.1, (K_2\text{-}K_3)_+=0.3, (K_3\text{-}K_2)_+=0$.

Flow: Φ(1)=0.8·1.8+0.6·2.1+0.5·0.3=1.44+1.26+0.15=2.85

$$\text{DPP: } DPP(1) = \frac{1}{1+2.85} \approx 0.26$$

Time t=2 - Update : $K_2(2)=2.2+0.5\cdot(0.8\cdot 1.8+0.3\cdot 0)=2.2+0.72=2.92$, $K_3(2)=1.9+0.5\cdot(0.6\cdot 2.1+0.5\cdot 0.3)=1.9+0.705=2.605$ $K(2) = \begin{pmatrix} 4 \\ 2.92 \\ 2.605 \end{pmatrix}$

Flow: $(K_1\text{-}K_2)=1.08, (K_1\text{-}K_3)=1.395, (K_2\text{-}K_3)=0.315$
Φ(2)=0.8·1.08+0.6·1.395+0.5·0.315=0.864+0.837+0.1575=1.8585

DPP: $DPP(2) = \frac{1}{1+1.8585} \approx 0.35$

Time t=3 - Update:$K_2(3)=2.92+0.5\cdot(0.8\cdot 1.08)=2.92+0.432=3.352$
$K_3(3)=2.605+0.5\cdot(0.6\cdot 1.395+0.5\cdot 0.315)=2.605+0.497=3.102$,

$K(3) = \begin{pmatrix} 4 \\ 3.352 \\ 3.102 \end{pmatrix}$

Flow: $(K_1\text{-}K_2)=0.648, (K_1\text{-}K_3)=0.898, (K_2\text{-}K_3) = 0.25$Φ(3)= 0.8·0.648+0.6·0.898+0.5·0.25=0.518+0.539+0.125=1.182

DPP: $DPP(3) = \frac{1}{1+1.8585} \approx 0.458$

Summary Table-1

t	K_1	K_2	K_3	Φ(t)	$DPP(t)$
0	4	1	1	4.2	0.192
1	4	2.2	1.9	2.85	0.26
2	4	2.92	2.605	1.86	0.35
3	4	3.352	3.102	1.20	0.455

Partial transmission weights $w_{ji}\in[0,1]$ induce a gradual dissipation of knowledge gradients, leading to smoother convergence dynamics and a continuous increase in DPP.

Temporal Dynamics of DPP and the Role of Regulation In the illustrative example presented above, the Deep Personal Privacy (DPP) metric increases monotonically over time, reflecting a continuous reduction in knowledge gradients across the network. The system converges toward a state of informational equilibrium, in which the knowledge about the individual—initially concentrated at the source node is progressively disseminated to all other nodes. The rate at which this

[3]Here we use α=0.5
[4]Here we use α=0.5

convergence occurs is governed by the propagation parameter α. Increasing α accelerates the diffusion of knowledge and leads to faster convergence toward equilibrium, whereas decreasing α slows down the propagation process and delays the system's approach to full informational symmetry. Thus, α controls the temporal dynamics of privacy erosion, rather than its ultimate outcome.

Key Properties

Monotonicity: $K_j(t+1) \geq K_j(t)$

Bounded Growth (In Practice): limited by network structure or external constraints

The model is related to **max consensus dynamics**, but evolves gradually rather than instantaneously.

However, real-world informational systems fundamentally differ from this closed-model behavior. In practice, the source node—the individual—continuously generates new information through actions, interactions, and behavioral traces, both voluntarily and involuntarily. This ongoing production of information implies that the underlying knowledge set is **non-stationary:**

$$U = U(t), \frac{d}{dt} \mid U(t) \mid > 0.$$

Moreover, newly generated information is neither instantaneously nor completely propagated across the network. As a result, a persistent **informational gap** exists between the individual and the surrounding nodes. This gap represents a residual layer of privacy, sustained by the continuous renewal of knowledge at the source and the finite speed and incompleteness of propagation. privacy gap, preventing the system from collapsing into full informational equilibrium.

Within the DPP Framework, this Model Provides a Precise Interpretation of Privacy Loss:

- Privacy degradation is driven by the **propagation of novel knowledge**, not raw data transfer.
- Nodes with higher knowledge act as **sources of informational gradients.**
- Nodes with similar knowledge contribute **negligible additional privacy risk.**
- Thus, privacy risk is governed by:
- knowledge differentials network topology
- propagation intensity rather than total information volume.

From this perspective, privacy is not a static property but a **dynamic imbalance** between information generation and information diffusion. The role of regulation and social norms is therefore to maintain this imbalance within acceptable bounds [17]. By constraining propagation mechanisms (e.g., limiting α, restricting connectivity W, or introducing friction in information transfer), regulatory frameworks aim to preserve a **reasonable privacy gap**, preventing the system from collapsing into full informational equilibrium.

Summary

We replace classical Laplacian diffusion with a **novelty-driven, non-conservative propagation model,** grounded in a set-theoretic formulation and approximated by the nonlinear equation:

$$K_j(t+1) = K_j(t) + \alpha \sum_{i=1}^{n} w_{ji} \, (K_i(t) - K_j(t))_+.$$

This Framework:

- Aligns with the non-rival nature of information
- Ensures growth only through novel knowledge
- Avoids redundant accumulation
- Provides a rigorous foundation for modeling knowledge spread and privacy risk

Open-System Extension: Dynamic Knowledge Generation

The closed-network model is analytically useful but does not fully capture real-world privacy dynamics. In the closed setting, the knowledge universe is fixed, and diffusion gradually eliminates all informational asymmetries, leading to full equilibrium and, ultimately, the exhaustion of privacy. In contrast, real-world privacy systems are inherently open[5][21,22]. Individuals continuously generate new information through ongoing activities such as communication, movement, transactions, and digital interactions [22]. As a result, the knowledge universe evolves over time, and cannot be treated as fixed.

To model this, let the knowledge universe be time-dependent:

$$U = U(t), \frac{d}{dt} \mid U(t) \mid > 0,$$

indicating continuous information generation. Let node 1represent the individual, who acts as the source of new information. The source evolves according to:$S_1(t+1)=S_1(t)\cup G(t)$,

where G(t)denotes newly generated information. Other nodes update via novelty-driven propagation:$S_j(t+1) = S_j(t)\cup\cup i\ T_{ji}(t), j\neq 1$, with $T_{ji}(t)\subseteq S_i(t)\setminus S_j(t)$. In scalar form: $K_1(t+1)=K_1(t)+g(t), K_j(t+1)=K_j(t)+\alpha \sum_i w_{ji}\,(K_i(t)-K_j(t))_+,\ j\neq 1.$

Thus, the System is Governed by Two Coupled Processes:

(i) Continuous knowledge generation at the source, and

(ii) Diffusion across the network.

A key implication is that the system generally does not converge to full equilibrium [20]. Even under efficient diffusion, ongoing information generation recreates knowledge gradients. Consequently, a persistent gap remains between the individual's knowledge and that of the network.

Open vs. Closed Systems (Condensed)

In a Closed System: U is fixed

- No new knowledge is generated
- Diffusion eliminates asymmetries
- The system converges to: $S_i(t)\rightarrow \cup_{k=1}^{n} S_k(0)$leading to full exposure and minimal privacy. In an Open System:
- U(t)evolves
- the source continuously generates information
- diffusion is delayed and incomplete
- asymmetries are continuously recreated

[5]Diffusion (or spreading processes) in networks describes the propagation of information, behaviors, or states through links conecting nodes [21].

Open vs. Closed Systems (Condensed)
In a Closed System: U is fixed
- No new knowledge is generated
- Diffusion eliminates asymmetries
- The system converges to: $S_i(t) \rightarrow \bigcup_{k=1}^{n} S_k(0)$leading to full exposure and minimal privacy.

In an Open System:
- $U(t)$evolves
- The source continuously generates information
- Diffusion is delayed and incomplete
- Asymmetries are continuously recreated

Thus, the system approaches a dynamic nonequilibrium rather than full convergence [20]. Privacy is therefore not a static condition, but the persistence of a nonzero knowledge gradient: $K_1(t) - K_j(t) > 0$ over sustained intervals.

Key Insight
Privacy is not the absence of information flow, but the persistence of an informational advantage maintained by continuous knowledge generation that outpaces diffusion [7].

Regulatory Interpretation
This distinction has important normative consequences. In a closed system, regulation can only slow down the rate of convergence to exposure. In an open system, by contrast, regulation and social norms can help preserve a stable privacy margin by limiting the speed, scope, and completeness of information propagation [6,17].

Such Mechanisms Include:
- Reducing the effective propagation rate α,
- Limiting network connectivity W,
- Introducing delays, frictions, or access constraints,
- Restricting secondary dissemination of received information,
- Establishing norms against intrusive observation, inference, or redistribution.

The function of regulation is therefore not to eliminate information flow altogether, but to maintain a reasonable privacy gap between the individual and the surrounding network. This gap is what prevents the system from collapsing into complete informational symmetry.

Conclusion
The closed-system model clarifies the intrinsic logic of novelty-driven propagation: once information exists in a fixed universe and is allowed to spread, the network tends toward informational equilibrium. Real privacy, however, exists not in such equilibrium states, but in open systems characterized by continuous information production and incomplete diffusion. From this perspective, the role of regulation and social norms is to preserve a sustainable level of informational asymmetry, thereby ensuring that privacy remains a live and renewable condition rather than a transient delay before total exposure.

In real-world informational environments, privacy survives not because information does not spread, but because the generation of new personal information continuously outpaces its complete diffusion across the network.

Privacy as Network Impedance
We interpret privacy mechanisms as **increasing resistance within the information network flow** [7]. $w_{ij} = b_{ij} + x_{ij}$. Where: b_{ij} = privacy resistance (static barriers), x_{ij} = dynamic impedance (contextual and temporal barriers). If wijrepresents information conductivity, then privacy resistance is $r_{ij}=1/w_{ij}$. High resistance implies limited data access, encryption, anonymization, differential privacy [17]. Low resistance implies open data access, cross-platform integration, AI inference. Thus, privacy functions as a **network-level impedance** to knowledge diffusion.

Spectral Measure of Deep Personal Privacy
The structural capacity of the network to propagate knowledge is determined by the eigenvalues of the Laplacian matrix [11]. Let $0=\lambda_1 \leq \lambda_2 \leq ... \leq \lambda_n$ be the eigenvalues of L.The value λ_2 is known as the **algebraic connectivity** of the graph. High connectivity implies rapid information diffusion.We therefore define a global measure of Deep Personal Privacy as$DPP=1/(\lambda_2+\varepsilon)$ where $\varepsilon>0$. Interpretation: High $\lambda_2 \rightarrow$ strong connectivity $\rightarrow$ low privacy, Low $\lambda_2 \rightarrow$ weak connectivity $\rightarrow$ high privacy impedance [21].

Diffusion Model Equations
$K(t+1) = K(t) - \alpha LK(t)$, $L=D-W$, $D=\text{diag}(d_1,\ldots,d_n)$, $d_i=\sum_j wij$, Where $\Phi(t) \approx \sum_{ij} w_{ij} * (K_i(t)-K_j(t))+$, $DPP(t)=1/(1+\Phi(t))$, and $(x)+= \max(x,0)$

Numerical Example
To illustrate the implications of the proposed diffusion model, we consider an information network with the following nodes:
- P— Person
- S— Social Network
- D— Public Database
- A— Adversarial Agent
- M— AI Inference System [18,19]

We Study Two Scenarios:
- **Scenario 1:** without the AI node
- **Scenario 2:** with the AI node

In both cases, the initial knowledge is concentrated entirely at the source node P.

The dynamics are governed by the discrete-time diffusion equation: $K(t+1)=K(t)-\alpha LK(t)$,
where $L=D-W$ is the graph Laplacian, Wis the weighted adjacency matrix, D is the corresponding degree matrix, and $\alpha=0.1$ is the diffusion parameter.

Scenario 1: Without AI Node
Network Structures and Diffusion are as below

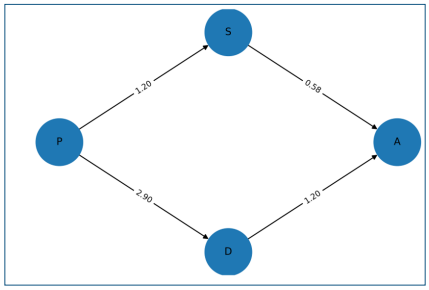


Figure 1: Baseline network without AI.

In the first scenario, the network consists of the four nodes $\{P,S,D,A\}$.

The state vector is $K(t)=\begin{pmatrix}K_P(t)\\K_S(t)\\K_D(t)\\K_A(t)\end{pmatrix}, K(0)=\begin{pmatrix}10\\0\\0\\0\end{pmatrix}$. The weighted adjacent matrix is taken as $W=\begin{pmatrix}0&1.2&2.9&0\\1.2&0&0&0.58\\2.9&0&0&1.2\\0&0.58&1.2&0\end{pmatrix}$.

The corresponding degree matrix is D=$\begin{pmatrix}4.1&0&0&0\\0&1.68&0&0\\0&0&4.1&0\\0&0&0&1.68\end{pmatrix}$,

hence the graph Laplacian is $L=D-W=\begin{pmatrix}4.1&-1.2&-2.9&0\\-1.2&1.68&0&-0.58\\-2.9&0&4.1&-1.2\\0&-0.58&-1.2&1.68\end{pmatrix}$.

$\Phi(0)\approx\sum_{ij}w_{ij}*(K_i(0)-K_j(0))+$,and the nonzero contributions are:K_P=10,K_S=0,K_D=0,K_A=0

$\Phi(0)$ calculation: $P\rightarrow S$: K_P-KS=10-0=10,then 1.2·10=12, P→D:K_P-KD=10-0=10,then2.9·10=29,**S→A**:,K_S-K_A=0-0=0, then 0.58·0=0, **D→A**: K_D-K_A=0-0=0,then 1.2·0=0

Overall $\Phi(0)$=12+29+0+0=41,**then** DPP(0)= $\frac{1}{1+41}=\frac{1}{42}\approx 0.0238$

Step 1: Computing K(1)

We first compute $LK(0)$: $LK(0)=\begin{pmatrix}4.1&-1.2&-2.9&0\\-1.2&1.68&0&-0.58\\-2.9&0&4.1&-1.2\\0&-0.58&-1.2&1.68\end{pmatrix}\begin{pmatrix}10\\0\\0\\0\end{pmatrix}=\begin{pmatrix}41.0\\-12\\-29\\0\end{pmatrix}$.

Therefore, $K(1)=K(0)-0.1\,LK(0)=\begin{pmatrix}10\\0\\0\\0\end{pmatrix}-0.1\begin{pmatrix}41.0\\-12\\-29\\0\end{pmatrix}=\begin{pmatrix}5.9\\1.2\\2.9\\0\end{pmatrix}$.

$\Phi(1)\approx\sum_{ij}w_{ij}*(K_i(1)-K_j(1))+$, and the nonzero contributions are: Then: K_P=5.9,K_S=1.2,K_D=2.9,K_A=0

Φ(1) calculation: P→S: K_P-K_S=5.9-1.2=4.7,then 1.2·4.7=5.64, **P→D**:K_P-K_D=5.9-2.9=3, then 2.9·3=8.7, **S→A**: ,KS-KA=1.2-0=1.2, then 0.58·1.2=0.696,**D→A**: KD-KA=2.9-0=2.9,then 1.2·2.9=0.696
OverallΦ(1)=5.64+8.7+0.696+0.696=18.516,

then DPP(1)= $\frac{1}{1+18.516}=\frac{1}{19.516}\approx 0.0512$

Step 2: Computing $K(2)$

Next, we compute $LK(1)$: $LK(1)=\begin{pmatrix}4.1&-1.2&-2.9&0\\-1.2&1.68&0&-0.58\\-2.9&0&4.1&-1.2\\0&-0.58&-1.2&1.68\end{pmatrix}\begin{pmatrix}5.9\\1.2\\2.9\\0\end{pmatrix}=\begin{pmatrix}14.34\\-5.064\\-5.22\\-4.176\end{pmatrix}$.

Hence, $K(2)=K(1)-0.1\,LK(1)=\begin{pmatrix}5.9\\1.2\\2.9\\0\end{pmatrix}-0.1\begin{pmatrix}14.34\\-5.064\\-5.22\\-4.176\end{pmatrix}=\begin{pmatrix}4.47\\1.71\\3.42\\0.4176\end{pmatrix}$.

$\Phi(2)\approx\sum$ijwij * $(K_i(2)-K_j(2))+$,and the nonzero contributions are:Then:K_P=4.47,K_S=1.71,K_D=3.42,K_A=0.4176Φ(2)

Calculation:P→S:K_P-K_S=4.47-1.71=2.76, *then* 1.2·2.76=3.312, P→D: KP-KD=4.47-3.42=1.05, then 2.9·1.05=3.045, S→A: KS-KA=1.71-0.4176=1.2924, then 0.58·1.2924=0.749592,D→A: OverallΦ(2)=3.312+3.045+0.749592+3.60288=10.709472, then
DPP(2)=1/(1+10.709472)=1/11.709472≈0.0854

Step 3: Computing $K(3)$

Now compute $LK(2)$: $LK(2)=\begin{pmatrix}4.1&-1.2&-2.9&0\\-1.2&1.68&0&-0.58\\-2.9&0&4.1&-1.2\\0&-0.58&-1.2&1.68\end{pmatrix}\begin{pmatrix}4.47\\1.71\\3.42\\0.4176\end{pmatrix}=\begin{pmatrix}6.357\\-2.733\\0.558\\-4.394\end{pmatrix}$

Therefore, $K(3)=K(2)-0.1\,LK(2)=\begin{pmatrix}4.47\\1.71\\3.42\\0.4176\end{pmatrix}-0.1\begin{pmatrix}6.357\\-2.733\\0.558\\-4.394\end{pmatrix}=\begin{pmatrix}3.834\\1.973\\3.364\\0.857\end{pmatrix}$

$\Phi(3)\approx ijwij*(K_i(3)-K_j(3))+$,and nonzero contributions are: K_P=3.834,K_S=1.973,K_D=3.364, K_A=0.857

$\Phi(3)$ calculation: **P→S**: K_P-K_S=3.834-1.973=1.861, then 1.2·1.861=2.2332, **P→D:**K_P-K_D=3.834-3.364=0.47, then 2.9·0.47=1.363, **S→A**: , K_S-K_A=1.973-0.857=1.116, then 0.58·1.116=0.64728,**D→A**: K_D-K_A=3.364-0.857=2.507,then 1.2·2.507=3.0084
OverallΦ(3)=2.2332+1.363+0.64728+3.0084=7.25188 then

DPP(3)= $\frac{1}{1+7.25188}=\frac{1}{8.25188}\approx 0.1212$

Thus, after three time steps: Φ(0)=41,Φ(1)=18.516,Φ(2)=10.709 5,Φ(3)=7.2519. Φ(0)>Φ(1)>Φ(2)>Φ(3)

Accordingly:$DPP(0)<DPP(1)<DPP(2)<DPP(3)$.Thus, DPPincreases monotonically as knowledge gradients dissipate across the network. The potential for novel knowledge diffusion diminishes, knowledge disparities between nodes are progressively eroded, and consequently, DPP increases over time.5.2.2 Scenario 2: With AI Node

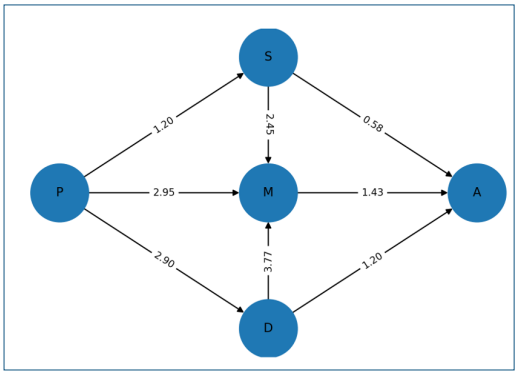


Figure 2: Network with AI Hub Node.

We now introduce an additional node M, representing an AI inference system.

The state vector becomes $K(t)=\begin{pmatrix}K_P(t)\\K_S(t)\\K_D(t)\\K_A(t)\\K_M(t)\end{pmatrix}, K(0)=\begin{pmatrix}10\\0\\0\\0\\0\end{pmatrix}$.

The weighted adjacent matrix is $W'=\begin{pmatrix}0&1.2&2.9&0&2.95\\1.2&0&0&0.58&2.45\\2.9&0&0&1.2&3.77\\0&0.58&1.2&0&1.43\\2.9&2.45&3.77&1.43&0\end{pmatrix}$

Interpretation of the Fifth Row/Column in the Weight Matrix. The fifth row (and, due to symmetry, the fifth column) corresponds to the AI inference node *M*. This implies the following edgeweights:$w_{M,P}$=2.95,$w_{M,S}$=2.45,$w_{M,D}$=3.77,$w_{M,A}$=1.43. By symmetry, the same values apply in the reverse direction. Reflecting the AI system's ability to aggregate and redistribute

information across multiple sources.

Degree Matrix and Laplacian

The corresponding degree matrix is $D' = \begin{pmatrix} 7.05 & 0 & 0 & 0 & 0 \\ 0 & 4.23 & 0 & 0 & 0 \\ 0 & 0 & 7.87 & 0 & 0 \\ 0 & 0 & 0 & 3.21 & 0 \\ 0 & 0 & 0 & 0 & 10.55 \end{pmatrix}$.

Hence, L'=D'-W'= $\begin{pmatrix} 7.075 & -1.12 & -2.9 & 0 & -2.95 \\ -1.2 & 4.23 & 0 & -0.58 & -2.45 \\ -2.9 & 0 & 7.87 & -1.2 & -3.77 \\ 0 & -0.58 & -1.27 & 3.21 & -1.43 \\ -2.9 & -2.45 & -3.77 & -1.43 & 10.55 \end{pmatrix}$.

Connection Interpretation

P↔M The AI system learns directly from the individual
S↔M The AI system extracts information from social networks
D↔M The AI system accesses and processes public databases
A↔M The AI system transfers inferred knowledge to the adversarial agent

Thus, the AI node acts as an information aggregator and distributor across heterogeneous data sources.

Generalized Modeling of the AI Node

While the specific weights assigned to the AI node in the numerical example are illustrative, the role of the AI node can be formalized in a general and systematic way.Let Mdenote an AI inference node introduced into a network with nodes i∈{1,…,n}. We define the weights connecting the AI node to the rest of the network as:$w_{M,i}=\gamma\cdot\beta_i$, where:γ>0 is a global scaling parameter representing the overall inference capacity of the AI system, $\beta_i\geq 0$represents the **information accessibility or relevance** of node *i*.

Degree-Proportional Connectivity

A natural and analytically convenient choice is to define: $\beta_i=d_i$,

where $d_i=\sum_j w_{ij}$ is the degree of node iin the original network. In this case, $w_{M,i}=\gamma_{di}$.

This formulation implies that the AI node connects more strongly to nodes that are already information-rich or highly connected. As a result, the AI node amplifies existing structural centralities in the network.

Interpretation

This construction reflects the empirical observation that AI systems:

- Preferentially access high-volume data sources (e.g., databases),
- Exploit high-connectivity platforms (e.g., social networks),
- Aggregate information from multiple channel simultaneously.

Thus, the AI node acts as a **centralized aggregator of heterogeneous information flows**, with connection strengths proportional to the informational importance of each node.

Impact on Network Dynamics

Introducing such an AI node modifies the diffusion operator in two key ways:

Increase in Node Degrees

The degree of each node becomes $d_i'=d_i+w_{iM}$,while the AI node itself has degree $d_M=\sum_i w_{M,i}$.

Acceleration of Diffusion

The augmented Laplacian *L'=D'-W'*has a larger spectral radius and typically a larger second-smallest eigenvalue (algebraic connectivity [11,22]), leading to faster convergence of the dynamics:$K(t+1)=K(t)-\alpha L' K(t)$.

Implications for Knowledge Propagation

Under this generalized model, the AI node introduces:

- **Additional high-weight edges,**
- **Shorter effective paths between nodes,**
- **Increased parallel channels for information flow**

Diffusion Dynamics

We apply the discrete-time diffusion model: $K(t+1)=K(t)-\alpha L' K(t),\alpha=0.1$.

Since the computations steps of **Scenario 2 are very similar to** calculations steps of **Scenario 1**, we'll only present the mains **computation** s.

Step-by-Step Computation

First compute *LK* (0): $\begin{pmatrix} 7.75 & -1.12 & -2.9 & 0 & -2.95 \\ -1.2 & 4.23 & 0 & -0.58 & -2.45 \\ -2.9 & 0 & 7.87 & -1.2 & -3.77 \\ 0 & -0.58 & -1.27 & 3.21 & -1.43 \\ -2.9 & -2.45 & -3.77 & -1.43 & 10.55 \end{pmatrix}\begin{pmatrix} 10 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 70.5 \\ -12 \\ -29 \\ 0 \\ -29 \end{pmatrix}$

Step 1: *K*(1) - Therefore, $K(1)=K(0)-0.1\ LK(0)=$

$$\begin{pmatrix} 10 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} - 0.1\begin{pmatrix} 70.5 \\ -12 \\ -29 \\ 0 \\ -29 \end{pmatrix} = \begin{pmatrix} 2.95 \\ 1.12 \\ 2.9 \\ 0 \\ 2.9 \end{pmatrix}.$$

Step 1: K(1)- $L' K(0)= \begin{pmatrix} 70.5 \\ -12 \\ -29 \\ 0 \\ -29 \end{pmatrix}$, $K(1) = K(0) - 0.1\ L'K(0) = \begin{pmatrix} 2.95 \\ 1.2 \\ 2.9 \\ 0 \\ 2.9 \end{pmatrix}$.

Step 2: $K(2)$ -$L' K(1)= \begin{pmatrix} 2.3925 \\ -5.5690 \\ 3.3350 \\ -8.3230 \\ 8.1670 \end{pmatrix}, K(2) = K(1) - 0.1\ L'K(1) = \begin{pmatrix} 2.7108 \\ 1.7569 \\ 2.5665 \\ 0.8323 \\ 2.0833 \end{pmatrix}$.

Step 3: $K(3)$-L' $K(2) = \begin{pmatrix} 3.4139 \\ -1.4080 \\ 3.4844 \\ -4.4062 \\ -1.0527 \end{pmatrix}$, $K(3) = K(2) - 0.1\ L'K(2) = \begin{pmatrix} 2.3694 \\ 1.8977 \\ 2.2181 \\ 1.2729 \\ 2.1886 \end{pmatrix}$.

Computation of DPP

We use the scalar approximation: $\Phi(t)\approx\sum_{i,j} w_{ji}' (K_i(t)-K_j(t))_+$,

and define: $DPP(t) = \frac{1}{1+\Phi(t)}$.

Results Φ(0)=70,DPP(0)≈0.0141,
Φ(1)≈14.878,DPP(1)≈0.0630,
Φ(2)≈10.4101,DPP(2)≈0.0876,
Φ(3)≈5.1588,DPP(3)≈0.1624.

Summary Table-2

t	K_P	K_S	K_D	K_A	K_M	Φ(t)	DPP(t)
0	10.0000	0.0000	0.0000	0.0000	0.0000	70.0000	0.0141
1	2.9500	1.2000	2.9000	0.0000	2.9000	14.8780	0.0630
2	2.7108	1.7569	2.5665	0.8323	2.0833	10.4101	0.0876
3	2.3694	1.8977	2.2181	1.2729	2.1886	5.1588	0.1624

Comparison Graph of DPP Evolution.

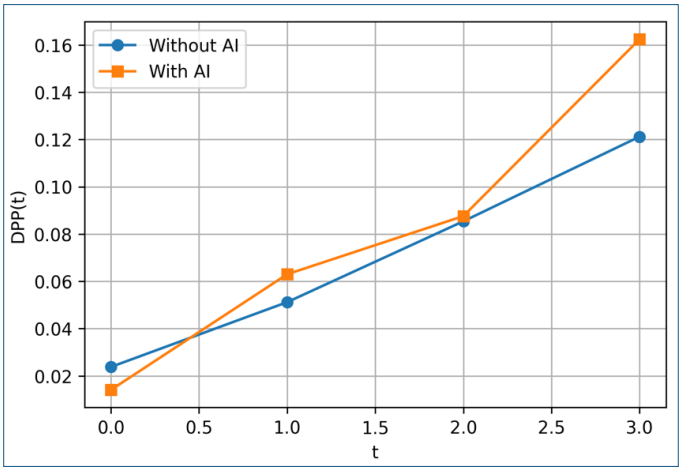


Figure 3: DPP Evolution.

Interpretation

The introduction of the AI node significantly accelerates the diffusion of knowledge across the network [21]. In particular, the adversarial node accumulates substantially more information within the same time horizon: $K_A(3) \approx 1.273$, which is considerably higher than in the non-AI scenario. At the same time, the novelty flow functional $\Phi(t)$decreases more rapidly, leading to a faster increase in DPP(t). This reflects an accelerated dissipation of knowledge gradients and a quicker transition toward informational equilibrium.

Key Insight

The AI node acts as a high-degree hub that aggregates and redistributes information across the network, thereby accelerating the collapse of informational asymmetries and significantly increasing adversarial knowledge within a short time horizon [7,18,22,23].

Conclusion

This work develops a fundamentally new paradigm for understanding personal privacy by modeling it as a network impedance to knowledge diffusion. By replacing classical conservative diffusion with a novelty-driven, non-conservative propagation model, the paper captures the epistemic structure of information flow in modern AI-driven environments. The identification of the novelty gradient as a unifying principle provides a rigorous bridge between network dynamics and privacy degradation, reframing privacy as resistance to inference rather than mere control of data.

The analysis demonstrates that network structure—particularly connectivity and the emergence of AI inference hubs—plays a decisive role in shaping privacy outcomes. AI systems function as structural accelerators that collapse informational asymmetries by integrating heterogeneous data sources, thereby reducing privacy impedance and amplifying inference capabilities. This reveals a fundamental limitation of traditional privacy frameworks, which focus on local protections while neglecting global network effects.

By extending the framework to open systems with continuous information generation, the paper establishes that privacy is inherently dynamic, emerging from the balance between information production and diffusion. Within this perspective, regulation and social norms acquire a precise operational meaning: they act as mechanisms for preserving a non-zero knowledge gradient by constraining propagation, limiting connectivity, and introducing friction into information flows.

Overall, the DPP framework offers a unified theoretical and mathematical foundation for analyzing privacy in the age of artificial intelligence. It connects diffusion theory, network science, and privacy research into a single coherent model, and provides a basis for designing systems and policies that maintain sustainable informational asymmetry. These contributions position Deep Personal Privacy as a measurable, system-level property and align directly with the core concerns of AI & Ethics: understanding and governing the structural conditions under which knowledge about individuals is produced, propagated, and controlled.

The analysis demonstrates that network structure—particularly connectivity and the presence of high-degree nodes such as AI systems—plays a decisive role in shaping privacy outcomes. AI inference systems are shown to function as epistemic accelerators that collapse informational asymmetries by integrating heterogeneous data sources, effectively reducing privacy impedance and shortening the path to adversarial knowledge. This insight highlights a critical limitation of traditional privacy frameworks, which focus on local data protection while neglecting global network effects.

By extending the model to open systems with continuous information generation, the paper further establishes that privacy is not a static condition but a dynamic equilibrium between information production and diffusion. Within this framework, regulation and social norms acquire a precise operational meaning: they act as mechanisms that preserve a non-zero knowledge gradient by constraining propagation rates, limiting connectivity, and introducing friction into information flows.

Overall, the proposed DPP framework offers both conceptual and mathematical advances. It provides a unified language for analyzing inference-based privacy risks, a formal link between graph topology and privacy dynamics, and a foundation for designing systems that maintain sustainable informational asymmetry. These contributions position Deep Personal Privacy as a measurable, system-level property and open new directions for research at the intersection of privacy, network science, and artificial intelligence.

References

1. Schoeman, F. (1984). "Privacy: philosophical dimensions", in: Philosophical Dimensions of Privacy: An Anthology, ed. Ferdinand D. Schoeman (Cambridge: Cambridge University Press), 3.
2. Laurie, G. (2002). Genetic privacy: a challenge to medico-legal norms. (Cambridge University Press), 6.
3. Hongladarom, S. (2016). A Buddhist theory of privacy. (Singapore: Springer Singapore), 16.
4. Ruth, G. (1980). “Privacy and the Limits of Law”. The Yale Law Journal, 89(3), 421.
5. Solove, D.J. (2010). Understanding Privacy. (London: Harvard University press), 1 2.
6. Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. (Stanford, Calif.: Stanford Law Books), 16.

7. Shannon, C.E. (1948). "A Mathematical Theory of Communication". reprinted with corrections from The Bell System Technical Journal, 27(3), 379 423.
8. Oppenheim, Y. (2024). Personal Privacy in the Age of the Internet. Spines, 136-139
9. Rogers, E. (2003). Diffusion of Innovations (5th ed.). The Free Press A Division of Macmillan. Publishing Co., Inc. 866 Third Avenue, New York, N. Y. 10022, 2003, 275-281
10. Jackson, M.O. (2008). Social and Economic Networks. Princeton University Press, 392-397
11. Chung, F.R. (1997). Spectral Graph Theory. published by the American Mathematical Society, Chapter 1.2
12. Bakenova, K., Kuznetsov, O., Artyshchuk, I., Shaikhanova, A., Shevchuk, R., et al. (2025). Information Diffusion Modeling in Social Networks: A Comparative Analysis of Delay Mechanisms Using Population Dynamics. Applied Sciences, 15(11), 6092.
13. Wang, D., Zhou, W., Hu, S. (2024). Diffusion Prediction with Graph Neural Networks. MM '24: Proceedings of the 32nd ACM International Conference on Multimedia, 9699-9708.
14. Yang, L., Zhang, Z., Song, Y., Hong, S., Xu, R., et al. (2023). Diffusion Models: A Comprehensive Survey of Methods and Applications. Survey of Methods and Applications, DOI: https://doi.org/10.1145/ 3626235.
15. Wei, R., Chien, E., Li, P. (2024). Differentially Private Graph Diffusion with Applications in Personalized PageRank's. 38th Conference on Neural Information Processing Systems (NeurIPS).
16. Chen, Y., Xue, H., Chen, Y. (2024). Diffusion Policy Attacker: Crafting Adversarial Attacks for Diffusion-based Policies. 38th Conference on Neural Information Processing Systems (NeurIPS).
17. Dwork, C. (2008). Differential Privacy: A Survey of Results. M. Agrawal et al. (Eds.): TAMC, LNCS 4978, c Springer-Verlag Berlin Heidelberg, 1-19.
18. Shokri, R., Stronati, M., Song, C., Shmatikov, V. (2017). Membership Inference Attacks Against Machine Learning Models. ARXiv, https://arxiv.org/abs/1610.05820.
19. Tivoni, R. (2014). "Entropiya neged evolutzia: Seder ba i-seder" [Entropy against evolution: Putting disorder in order] (in Hebrew). Davidson Institute of Science Education-The Educational Arm of The Weizmann Institute of Science.
20. Prigogine, I. (1977). Time, Structure and Fluctuations, Nobel Lecture.
21. Barabási, A.L. (2016). Network science, Cambridge University Press, section 10.2 Epidemic Modeling.
22. Kairouz, P., McMahan, H.B. (2021). Advances and open problems in federated learning. Foundations and Trends in ML, 14(1-2), 1-210.
23. Carlini, N., Tramer F., Wallace E., Jagielski, M., Voss, A. H., et al. (2021). Extracting training data from large language models. 30th USENIX Security Symposium, 11-13.