Privacy as Epistemic Impedance: Deep Personal Privacy and the Political Economy of Knowledge in Networked Societies

Yair Oppenheim[1]

[1] School of Philosophy, Linguistics and Science Studies, The Lester and Sally Antin Faculty of Humanities, Tel Aviv University, Israel

Correspondence: Dr. Yair Oppenheim, Ph. D., School of Philosophy, Linguistics and Science Studies, The Lester and Sally Antin Faculty of Humanities, Tel Aviv University, Israel. Tel: 972-53-285-6133.

Received: March 10, 2026 Accepted: April 2, 2026 Published: April 7,2026
doi:10.65343/tpss.v2i1.85 URL: https://doi.org/10.65343/tpss.v2i1.85

Abstract

This article reconceptualizes privacy as epistemic impedance within networked inference systems. Rather than treating privacy as control over data, I argue that privacy concerns the regulation of knowledge formation. Building on a structural analogy to electrical impedance, I formalize privacy current as I = V / Z, where V denotes knowledge pressure and Z denotes total privacy impedance. Deep Personal Privacy (DPP) is defined as the time-integrated inverse of effective knowledge flow. I demonstrate that privacy degrades nonlinearly under parallel integration, proves key monotonicity properties, and show how DPP yields enforceable regulatory thresholds. The framework integrates information theory, graph theory, and game-theoretical modeling (Shannon, 1948; Cover, & Thomas, 2006; Doyle, & Snell, 1984; Kong, Chen, Yang, Cheng, Zhang, & He, 2023) while remaining grounded in normative commitments to epistemic symmetry and autonomy.

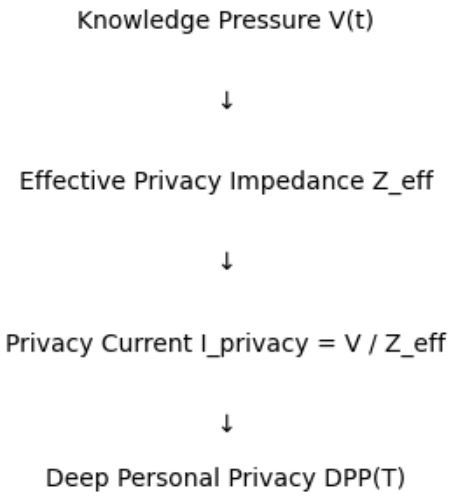

Figure 1. Core dynamics of the Deep Personal Privacy (DPP) framework

The conceptual structure of the model is illustrated in Figure 1.

Privacy Dynamics under Parallel Data Integration

This figure illustrates the theoretical relationship between effective privacy impedance Z_{eff}, privacy current I = V/ Z_{eff}, and Deep Personal Privacy DPP(T). The decrease in effective impedance (for example due to parallel integration of multiple information sources) increases the privacy current and accelerates the production of knowledge about the individual, thereby reducing DPP. individual, thereby reducing DPP.

Keywords: deep personal privacy, epistemic impedance, knowledge flow, inference governance, network privacy, philosophy of technology

1. Introduction

Many attempts have been made to redefine personal privacy, yet none has proven fully adequate to the structural conditions of contemporary technological society (Schoeman, 1984; Laurie, 2002; Hongladarom, 2016; Gavison, 1980; Solove, 2009; Nissenbaum, 2010). Classical philosophical accounts have described privacy in terms of intimacy, control, secrecy, autonomy, or contextual appropriateness. However, these approaches, while normatively rich, remain insufficiently responsive to the epistemic and technological transformation that characterizes the age of Information and Communication Technologies (ICT) (Zuboff; Acquisti, Taylor, & Wagman, 2016).

In this article, I propose a conceptual shift: instead of framing the debate around personal privacy as such, I replace the discourse with a more precise and analytically tractable notion—personal privacy information. This replacement reflects a structural transformation in the ontology of privacy itself. The central argument is that replacing the discourse on personal privacy with one on personal privacy information is philosophically and practically justified for at least three reasons (Shannon, 1948; Yair, 2024). First, personal privacy information can be digitized, stored, replicated, and detached from the embodied individual. Second, privacy is instantiated as information—debates about privacy concern the collection, aggregation, processing, inference, and dissemination of personal information. Third, public and legal discussions about privacy ultimately concern informational practices. If privacy is informational, its protection must be dynamic rather than static. It must model interactions among adversarial agents, defenders and attackers, regulators and platforms, individuals and algorithmic systems.

1.1 Basic Components of Personal Privacy

The basic components of personal privacy include private space (physical and virtual); the body (including biometric and genetic data); the mind (thoughts, emotions, inferred preferences); actions; property information; external entities; relationships; autonomy; identity; and anonymity in its various forms (Solove, 2009; Westin, 1984).

Each component may be conceptualized as a node in a dynamic network with states such as Safe, Attacked, or Isolated. Some nodes contain critical privacy information. Deep Personal Privacy refers to knowledge about oneself that remains exclusively known to the individual—formally, the difference between self-knowledge and societal knowledge.

General Personal Privacy refers to information shared with confidants but not with the public sphere. ICT infrastructures have dramatically increased the aggregation and correlation of information across all components.

1.2 Privacy as Information Flow in the ICT Age

In the ICT era, personal privacy information was continuously dispersed across physical and virtual platforms. It is aggregated without filtering and stored until activated by inference. Following Nissenbaum (1999), privacy may be understood as a form of information flow (Zuboff; Acquisti, Taylor, & Wagman, 2016). Privacy information flows from Deep Personal Privacy to General Personal Privacy and eventually into the Public Sphere.1.3 Structural Challenges of the Network Society. Personal information has become the primary resource of ICT culture. It is collected, analyzed, and monetized through IoT devices, AI systems, and digital platforms.

In the network society, individuals are both nodes and agents. Personal information is embedded in devices that continuously exchange and synchronize data. Economic and political actors have strong incentives to reduce barriers to information extraction. Network structures are flatter, reducing resistance and accelerating privacy erosion.

1.3 From Flow to Impedance

To address violations of Deep Personal Privacy, I propose a formal model based on Ohm's Law. Personal information corresponds to current; external actors are consumers; the individual is the source. High privacy corresponds to difficulty of flow, low privacy to free flow. Privacy thus functions as impedance within a network of inferences.

2. Translating Ohm's Law Into a Theory of Privacy

The structural dynamics of networked information systems suggest that privacy erosion is not merely a function of data accumulation, but of accelerated informational flow. To model this process formally, I introduce a structural analogy to Ohm's Law (Doyle, & Snell, 1984) and network flow analogy (Cover, & Thomas, 2006). The analogy is not metaphorical but relational: it captures how pressure, resistance, and flow interact in any system governed by constrained transmission.

Ohm's Law states:

$$I = V / R \tag{1}$$

where I denote current (rate of electrical flow), V denotes voltage (driving potential), and R denotes resistance

(constraint on flow). The general structural principle is that flow is driven by pressure but limited by resistance.

In informational systems, knowledge generation follows the same structural relation. I therefore define privacy current as: $I_p = V_k / Z_p$

where I_p represents the rate at which effective knowledge about an individual is generated (bits per unit time), V_k represents knowledge pressure (economic, political, and technological incentives to extract knowledge), and Z_p represents total privacy impedance.

2.1 Knowledge Pressure (V_k)

Knowledge pressure formalizes the incentive structure driving inference. It includes economic motivations (e.g., targeted advertising), political motivations (e.g., governance optimization), technological motivations (e.g., AI model training), and strategic motivations (e.g., competitive advantage). Formally, $V_k \geq 0$. When V_k increases while Z_p remains constant, privacy current increases proportionally.

2.2 Total Privacy Impedance (Z_p)

Unlike classical resistance, impedance includes both static and dynamic components:

$$Zp = R + X \quad (2)$$

Where:

R = privacy resistance (static barriers), X = dynamic impedance (contextual and temporal barriers). (3)

2.2.1 Privacy Resistance (R)

Privacy resistance includes Legislation (GDPR, HIPAA), Encryption, Access control mechanisms, Database separation, Economic costs of data collection, Basic anonymization mechanisms. High $R\Rightarrow$ direct information collection is difficult. Low $R\Rightarrow$ information is relatively accessible. When Resistors connected in series there will be (OpenStax) $R_{total}=R_1+R_2+R_3+\ldots$ When Resistors connected in parallel there will be (OpenStax) $\frac{1}{R_{\text{total}}} = \frac{1}{R_1} + \frac{1}{R_2} + \frac{1}{R_3} + \ldots$

This is the type of privacy barrier on which most public and regulatory discourse traditionally focuses.

2.2.2 Dynamic Impedance (X)

Dynamic impedance represents the difficulty of converting collected data into reliable knowledge. Examples include: Statistical noise (e.g., differential privacy (Dwork, & Roth, 2014)), Measurement error, Behavioral variability, Temporal delays, Context switching, Identity fragmentation, (pseudonymity), Integration difficulty across heterogeneous datasets. High $X\Rightarrow$ information remains unstable, noisy, or ambiguous, making inference difficult. Low $X\Rightarrow$ information converges rapidly into stable and reliable knowledge. While *R* limits *whether* information can be collected, *X* limits *how effectively* collected information can be transformed into knowledge.

The resulting privacy current becomes:

$$Ip = Vk / (R + X) \text{ then } Ip = Vk / Z \quad (4)$$

2.3 Series and Parallel Composition

$$Zseries = Z1 + Z2 + Z3 + ... \quad (5)$$

$$1 / Zparallel = 1/Z1 + 1/Z2 + 1/Z3 + ... \quad (6)$$

This implies that $Z_{parallel}$ is strictly less than the smallest individual impedance ($Z_{parallel} < \min(Z_i)$). Therefore, privacy degradation is nonlinear under channel aggregation. Adding even a seemingly minor information source reduces overall resistance. When privacy is defined in terms of information flow, **impedance (*Z*)** represents the **overall difficulty of transforming dispersed data into useful knowledge about an individual**.

Conclusion: *I* do not measure how much data has been collected, but rather how much effective knowledge is produced per unit of time.

3. Operationalizing Privacy Current in Information Systems

In information systems, privacy current ($I_{privacy}$) may be operationalized through measurable indicators reflecting the rate at which knowledge about an individual is generated. These indicators capture inferential outcomes rather than mere data accumulation.

• Rate of data collection

• Rate of data processing

• Rate of inference formation

• Rate of individualized decision-making

3.1 Practical Methods for Measuring $I_{privacy}$

Violation of Anonymity

If 1,000 anonymized profiles are observed and 120 are re-identified within one hour, the de-anonymization rate constitutes a measurable privacy information current (Narayanan, & Shmatikov, 2008).

Entropy-Based Measurement

$$\text{Iprivacy}(t) = - \, dH(t) / dt \quad (7)$$

H(t) denotes uncertainty about the individual. A rapid decrease implies high privacy current (Shannon, 1948; Yair, 2024; Rokach and Maimon).

Rate of Predictive Improvement

In machine learning / artificial intelligence (ML/AI), the privacy information current can be expressed as the rate at which predictive performance improves over time:

I ≈ Delta Accuracy / Delta t or I ≈ Delta Loss / Delta t

Rapid model convergence concerning an individual corresponds to high privacy current (Guan, Yu, Zhou, Li Chowdhury, Xie, Xiao, & Zou, 2025; Jegorova, Kaul, Mayor, O'Neil, Weir, Murray-Smith, & Tsaftaris).

Rate of Person-Specific Decisions

Another practical manifestation of the privacy current is the rate of decisions that are specifically tailored to an individual (Ullah, Boreli, & Kanhere, 2023), such as: price offers, targeted Advertising, risk scoring. Formally: $I_{privacy}$ = (Number of personalized decisions) / (Time)

Examples include personalized prices, targeted advertisements, and risk scoring (Ullah, Boreli, & Kanhere, 2023).

Why Data Volume Alone Is Insufficient

Gigabytes of stored data do not indicate utility; attribute counts do not indicate correlation; database counts do not indicate integration. Privacy current *I* measures outcomes rather than inputs.

3.2 Direct Structural Connection to Ohm's Law

If knowledge pressure (V_k) increases while impedance (Z) decreases, privacy current (e.g. $\boldsymbol{I_{privacy}}$) increases (Millikan, & Bishop, 1917). This pattern is observable in large technology platforms and data brokerage markets.

Privacy is not the sum of barriers, but the sum of their reciprocals (OpenStax; Doyle, & Snell, 1984).

and a sink combined to increase overall throughput, even when each individual path is constrained, highlighting that effective resistance to flow decreases as additional channels are introduced (Kleinberg, & Tardos, 2005). That is $\text{Privacy} \neq \sum_i Z_i$, but rather, $\text{Privacy} = \sum_i \frac{1}{Z_i}$. This result has a dramatic implication (Issa, Kamath, & Wagner, 2016). The addition of even a "small" information source can cause a significant degradation of privacy. There is no local fix without a network-level perspective. Therefore: **More data does not imply more knowledge; rather, it implies lower resistance.**

Numerical Illustration

Let assume: Channel A (Z=10), Channel B (Z=20), Channel C (Z=30)

$$1 / \text{Zprivacy} = 1/10 + 1/20 + 1/30 \text{ then the effective privacy resistance} \quad (8)$$

The parallel integration of channels significantly reduces effective privacy (Issa, Kamath, & Wagner, 2016; Sweeney, 2002).

3.3 Interpretation of Parallel Privacy Impedance

Although each individual information channel may appear reasonably protected when considered in isolation, the overall level of privacy may become significantly weaker once these channels operate simultaneously. When multiple information channels are combined in parallel, their collective effect substantially reduces the effective privacy impedance associated with the individual.

This observation illustrates the conceptual weakness underlying the common claim "I have nothing to hide." As

Calvin Gottlieb observed, many individuals tend to discount privacy concerns when other interests appear more pressing (Sweeney, 2002). However, even seemingly innocuous and well-protected sources of personal information may, when aggregated, dramatically reduce an individual's effective level of privacy.

If privacy barriers are modeled as impedances, two structural configurations must be distinguished.

Proposition (Parallel Collapse of Privacy Impedance)

Let $Z_1, \ldots, Z_n$ be positive privacy impedances corresponding to n independent information channels operating in parallel. Define the effective privacy impedance as: $1 / Z_{eff} = \sum_{i=1}^{n} \frac{1}{Z_i}$. Then Zeff is strictly decreasing in n. For any additional channel $Z_{\{n+1\}} > 0$: $Z_{eff}(Z_1,\ldots,Z_n,Z_{\{n+1\}}) < Z_{eff}(Z_1,\ldots,Z_n)$.

Moreover, $Z_{eff} \leq \min_i Z_i$, with strict inequality whenever $n \geq 2$.

Proof Sketch

Since each $Z_i > 0$, each reciprocal $1/ Z_i$ is positive. Adding a new channel adds a positive term to the reciprocal sum, so:

$$= + 1/Z\{n+1\} > \quad (9)$$

Taking reciprocals preserves strict inequality in the reverse direction because all quantities are positive, hence $\sum_{i=1}^{n} \frac{1}{Z_i}$ decreases. For the bound, observe that $\sum_{i=1}^{n} \frac{1}{Z_i} \geq 1/ \min_i Z_i$, hence $1/ Z_{eff} \geq 1/ \min_i Z_i$, so $Z_{eff} \leq / \min_i Z_i$ with strict inequality when at least two terms are present.

This proposition formalizes the non-linear collapse of privacy under aggregation: even channels that are individually well-protected reduce overall privacy when combined in parallel, explaining why network-level governance is necessary.

4. Personal Privacy Metrics

This section reviews several widely used privacy metrics and interprets them within the impedance framework introduced earlier. Rather than focusing on the quantity of data collected, these metrics emphasize the difficulty of identifying individuals or stabilizing knowledge about them.

Well-Known Privacy Metrics

(a) k-Anonymity

k-Anonymity ensures that each record in a dataset cannot be distinguished from at least k−1 other records (Sweeney, 2002; Yair, 2025). In the impedance interpretation:

• Small k → low resistance to identification.

• Large k → high resistance to identification.

However, when multiple information channels operate in parallel, effective resistance may drop sharply because auxiliary data sources can reduce the anonymity set.

(b) Differential Privacy

Differential privacy introduces controlled statistical noise into data queries to limit the influence of any single individual (Kobbi. 2020; Cover, & Thomas, 2006).

• Small ε (epsilon) → strong privacy guarantees large resistance.

• Large ε → weaker privacy guarantee → small resistance.

Accordingly, privacy resistance can be approximated as: $R \propto 1/\varepsilon$.

When multiple privacy mechanisms operate in parallel, total resistance satisfies the relation: $1 / R_{total} = \sum \varepsilon_i$.

This structure is formally analogous to the parallel composition of electrical resistors.

(c) Measures of Non-Knowledge / Non-Identification

A different family of privacy metrics focuses not on the amount of data collected, but on how difficult it is to infer an individual's identity, attributes, or decisions from the available information. These measures quantify effective non-knowledge.

Effective Number of Persons (ENP)

The Effective Number of Persons (ENP) measures how many plausible individuals remain from the system's

perspective after all available information has been considered. It therefore quantifies identity ambiguity.

Formal definition (entropy-based) (Shannon, 1948; Rokach and Maimon; Serjantov, & Danezis, 2002):

$$ENP = \exp(H), \tag{10}$$

where

$$H = - * \log (pi\ ). \tag{11}$$

Interpretation:

• High ENP → many plausible candidates → high privacy.

• Low ENP → sharp identification → low privacy.

Importantly, ENP is a post-inference measure rather than a post-collection measure.

DC – Degree of Confusion / Degree of Certainty

DC measures the degree to which an information system remains uncertain about the identity, attributes, or decisions of an individual after all available data and inferences have been incorporated.

Let $\{p_i\}$ represent the probability distribution over possible identities or states. A simple operational representation is: $DC \approx 1 / (\max_i p_i)$

Interpretation:

• If $(\max_i p_i)$ is large (a sharp probability peak), DC is small → high certainty.

• If $(\max_i p_i)$ is small (no dominant candidate), DC is large → high confusion.

A flat distribution indicates many plausible candidates and therefore strong privacy protection, whereas a sharply peaked distribution indicates near-certain identification.

DC is particularly sensitive to processes that sharpen probability distributions, including cross-dataset correlation, machine-learning inference, temporal integration, and contextual information.

DC within the Privacy Impedance Framework

In the impedance model, R represents static barriers (regulation, access control), while X represents dynamic barriers (noise, delay, ambiguity).

DC primarily reflects the dynamic component X:

• High DC → high X → knowledge remains difficult to stabilize.

• Low DC → low X → knowledge converges rapidly.

Thus: Z = R + X, A decrease in DC leads to:

$$Z \downarrow \Rightarrow \text{Iprivacy} \uparrow \tag{12}$$

In other words, reduced inferential uncertainty lowers privacy impedance and increases the privacy information current.

Illustrative Example

Before inference integration:

Let p = [0.25, 0.25, 0.25, 0.25] → DC ≈ 4 (high confusion)

After data fusion and inference (Narayanan, & Shmatikov, 2008; Gottlieb, 1996):

p = [0.7, 0.1, 0.1, 0.1] → DC ≈ 1.43 (high certainty)

No additional data has been collected; however, inference processes significantly reduce uncertainty and therefore decrease privacy.

Quantitative Summary: Effect of Integration

Before integration: DC high, ENP high, X high, Z high, $I_{privacy}$ low.

After integration: DC low, ENP low, X low, Z low, $I_{privacy}$ high.

Complementarity of ENP and DC

ENP measures the effective number of plausible candidates across the entire distribution (a global measure), whereas DC reflects the dominance of the most probable candidate (a local or extremal measure). It is therefore possible to observe high ENP together with low DC (a strong peak with a long tail), or moderate ENP with high DC (no clearly dominant candidate). Accordingly, ENP and DC should be viewed as complementary metrics rather than overlapping ones.

Summary

These metrics (e.g. ENP and DC**)** do not ask how much data has been collected. Instead, they address a deeper question: how difficult it is to infer an individual's identity, attributes, or decisions from the available information. In this sense they measure effective non-knowledge rather than data volume.

Proposition: Formal Link Between ENP/DC and Privacy Impedance

Let $\{p_i(t)\}$ be the posterior probability distribution maintained by an information system over candidate identities (or states) for an individual at time t. Define:

ENP(t) = exp(H(t)), where H(t) = - * log (pi(t)). Then DC(t) ≈ 1 / (maxi pi(t)). (13)

Assume privacy impedance decomposes as $Z(t) = R + X(t)$, where $R \geq 0$ is a static barrier (e.g., regulation, access control) and $X(t) \geq 0$ is a dynamic barrier capturing noise, delay, and ambiguity. Suppose the dynamic component is monotone increasing in uncertainty: there exists an increasing function g such that $X(t) = g(H(t))$. Then the following implications hold:

1) $ENP(t) \downarrow \Rightarrow H(t) \downarrow \Rightarrow X(t) \downarrow \Rightarrow Z(t) \downarrow$.

2) $DC(t) \downarrow \Rightarrow \max_i p_i(t) \uparrow \Rightarrow H(t) \downarrow \Rightarrow X(t) \downarrow \Rightarrow Z(t) \downarrow$.

3) Under fixed knowledge pressure

Vk > 0, Iprivacy(t) = Vk / Z(t) increases as ENP(t) and DC(t) decrease. (14)

Proof Sketch

$ENP(t) = \exp(H(t))$ is strictly increasing in H(t); therefore $ENP(t) \downarrow$ implies $H(t) \downarrow$. By monotonicity of g, $H(t) \downarrow$ implies $X(t) = g(H(t)) \downarrow$, and with R fixed, $Z(t) = R + X(t) \downarrow$.

For DC, note $DC(t) \approx 1/\max_i p_i(t)$, so $DC(t) \downarrow$ implies $\max_i p_i(t) \uparrow$, meaning the posterior distribution becomes more concentrated. Entropy decreases as probability mass concentrates, hence $H(t) \downarrow$. The same monotonicity argument yields $X(t) \downarrow$ and therefore $Z(t) \downarrow$.

Finally, with Vk fixed and $Z(t) > 0$, a decrease in Z(t) implies an increase in

Iprivacy(t) = Vk / Z(t). (15)

This proposition formalizes the claim that ENP and DC function as operational proxies for the dynamic impedance component X(t): as inference sharpens (ENP ↓, DC ↓), ambiguity falls, dynamic impedance declines, and privacy current increases.

5. Deep Personal Privacy (DPP)

This section introduces a new family of privacy metrics referred to as Deep Personal Privacy (DPP). Unlike traditional privacy metrics that focus primarily on the quantity of collected data, DPP emphasizes the difficulty, cost, and temporal dynamics involved in transforming dispersed data into actionable knowledge about an individual across the network.

The DPP framework measures privacy through two interacting quantities: (a) overall privacy impedance and (b) the resulting flow of knowledge about an individual. This formulation follows an analogy with Ohm's law, which relates potential, resistance, and current in electrical systems.

Basic Variables

V(t) - Knowledge pressure.

The economic, organizational, or technological value associated with extracting knowledge about an individual at time t.

Z(t) - Privacy impedance.

The total resistance to knowledge extraction, including legal, technological, behavioral, cognitive, and statistical barriers.

$I_{privacy}(t)$ - Privacy information current.

The rate at which useful knowledge about an individual is produced.

Relationship: $I_{privacy}(t) = V(t) / Z(t)$

Definition of Deep Personal Privacy

Deep Personal Privacy is defined as the cumulative resistance to knowledge (Yair, 2024, pp. 24-25, pp. 136-139, pp. 140-154) extraction over time. $DPP(T) = \int_0^T \frac{1}{I_{\text{privacy}}(t)}\, dt = \int_0^T \frac{Z(t)}{V(t)}\, dt$

Interpretation:

Small $I_{privacy}$ → large DPP → strong privacy.

Large $I_{privacy}$ → small DPP → rapid erosion of privacy.

Network Structure of Privacy Impedance

Privacy impedance arises from multiple information channels operating in parallel.

$$1 \ / \ Z(t) \ = \ : \frac{1}{Z(t)} = \sum_{i=1}^{N} \frac{1}{Z_i(t)} \tag{16}$$

Examples of channels include Social networks, Location data, Health information, Purchase records, Sensor data, Social relationships.

The addition of even a small information channel can significantly reduce overall privacy impedance.

Proposition 1: Network Aggregation Theorem

Let $Z_1(t)$, …, $Z_n(t)$ be privacy impedances associated with n independent information channels operating in parallel. The effective privacy impedance is:

$$1 \ / \ Zeff(t) \ = \frac{1}{Z(t)} = \sum_{i=1}^{N} \frac{1}{Z_i(t)} \tag{17}$$

If a new information channel $Z_{+1}(t)$ is introduced with $Z_{+1}(t) > 0$

then: $Z_{eff}(new) < Z_{eff}(old)$, Consequently: $DPP_{new}(T) < DPP_{old}(T)$

Proof Sketch

Adding a new channel introduces an additional positive term to the reciprocal sum $\sum(1/Z_i)$. Therefore, the reciprocal of the total impedance increases. Taking reciprocals implies that the effective impedance decreases.

Since $DPP(T) \ = \int_0^T \frac{Z(t)}{V(t)} \, dt$ and V(t) remains constant, a decrease in Z(t) implies a decrease in DPP(T).

Proposition 2: Learning Acceleration Effect

Let H(t) be the entropy of the posterior distribution maintained by an information system over candidate identities for an individual. Suppose machine learning inference processes reduce entropy over time such that: $dH(t) / dt < 0$

Assume the dynamic impedance component X(t) is an increasing function of entropy: $X(t) = g(H(t))$, $g'(H) > 0$ Then decreasing entropy implies:

$$X(t) \downarrow \Rightarrow Z(t) = R + X(t) \downarrow \Rightarrow I_{privacy}(t) \uparrow \tag{18}$$

Proof Sketch

As learning processes concentrate probability mass on fewer candidates, entropy decreases. Since X(t) increases with entropy, reduced entropy lowers dynamic impedance. With Z(t) decreasing and knowledge pressure V(t) fixed, the privacy current increases.

Theorem: DPP Collapse in Large Information Networks

Consider a network with N independent information channels, each with impedance $Z_i > 0$. Let the effective privacy impedance be defined by:

$$1 \ / \ Zeff(t) \ = \sum_{i=1}^{N} \frac{1}{Z_i(t)} \tag{19}$$

If the number of channels n grows while the individual impedances remain bounded ($Z_i \leq Z_{max}$), then: $\lim\{n\to\infty\} Z_{eff} = 0$

Consequently: lim_{N→∞} DPP(T) = 0

Proof Sketch

Each term $1/Z_i$ is positive and bounded below by $1/Z_{max}$. As n increases, the sum $\sum(1/Z_i)$ grows without bound. Therefore, the reciprocal Z_{eff} approaches zero. Since $DPP(T) = = \int_0^T \frac{Z(t)}{V(t)} \, dt$ and Z(t) approaches zero, the

cumulative deep privacy measure collapses.

This theorem formalizes the intuition that in sufficiently dense information ecosystems privacy degradation becomes structurally inevitable. Even if each channel individually appears well protected, the aggregation of many channels drives the effective privacy impedance toward zero.

6. DPP versus Classical Privacy Metrics

Table 1

Metric	What it Measures	Limitation
k-anonymity	Group size / anonymity set	Static and local
Differential Privacy	Noise added to queries	Algorithm-specific
ENP / DC	Degree of non-knowledge / identification uncertainty	Typically one-dimensional
Deep Personal Privacy (DPP)	Systemic difficulty of inferring knowledge	Dynamic, network-based, cumulative

Within the impedance framework, DPP subsumes these metrics as components of the total privacy impedance Z(t).

Theorem — DPP Subsumption Property

Let Z(t) denote the total privacy impedance governing knowledge extraction about an individual. Assume that Z(t) decomposes into components corresponding to different privacy protection mechanisms:

$$Z(t) = Zk + ZDP + ZENP + ZDC + Zothers \quad (20)$$

where Z_k represents resistance induced by k-anonymity mechanisms, Z_{DP} represents resistance induced by differential privacy noise, and Z_{ENP} and Z_{DC} represent uncertainty-based resistance arising from inference ambiguity.

Each classical privacy metric therefore contributes to the overall impedance governing knowledge extraction. The resulting privacy current satisfies:

$$I_{privacy}(t) = V(t) / Z(t)$$

Proof Sketch

k-anonymity increases uncertainty regarding identity, differential privacy introduces statistical noise that weakens inference reliability, and ENP/DC capture probabilistic ambiguity in identification. Each mechanism therefore increases resistance to knowledge extraction and contributes to the total impedance Z(t).

Conceptual Contribution of DPP

Deep Personal Privacy introduces a network-level metric that model's privacy as effective impedance to knowledge flow across distributed information systems.

Unlike traditional privacy measures, which focus on local protections or data collection limits, DPP captures the cumulative difficulty of transforming dispersed data into stable knowledge about an individual.

Illustrative Numerical Example (Medical Context)

Let knowledge pressure be

$$V = 0.8 \text{ bits/hour.} \quad (21)$$

Two parallel medical information channels exist:

$$Z_1 = 4,\ Z_2 = 4 \quad (22)$$

Parallel composition:

$$1 / Ztotal = 1/4 + 1/4 = 1/2 \Rightarrow Ztotal = 2 \quad (23)$$

Privacy current:

$$Iprivacy = 0.8 / 2 = 0.4 \text{ bits/hour} \quad (24)$$

For time horizon T = 5 hours:

$$DPP(5) = \quad dt = 12.5 \quad (25)$$

Interpretation: stable medical knowledge about the individual emerges rapidly, indicating relatively shallow privacy.

If barriers increase to

$$Ztotal = 8: Iprivacy = 0.8 / 8 = 0.1 \text{ bits/hour, } DPP(5) = 50 \quad (26)$$

Higher DPP indicates deeper privacy because useful knowledge is generated more slowly.

7. Regulatory Implications (CO Guidance, 2024) of the Deep Personal Privacy (DPP) Framework

Information and communication technologies (ICTs) have significantly expanded the capacity to collect, integrate, and analyze personal data. Consequently, privacy risks increasingly arise not from isolated data collection events but from the large-scale integration of heterogeneous information sources (Narayanan, & Shmatikov, 2008). The Deep Personal Privacy (DPP) framework highlights that privacy protection cannot be guaranteed through local safeguards applied to individual datasets or algorithms.

Because privacy impedance composes across multiple information channels operating in parallel, effective regulation must adopt a system-level perspective. Adding new data sources, enabling cross-platform integration, or allowing unrestricted inference can substantially reduce total privacy impedance, thereby accelerating the rate at which useful knowledge about an individual is generated.

Policy Implications

The DPP framework suggests that privacy regulation should focus on controlling the dynamics of knowledge extraction rather than solely regulating data collection events. Regulation can be expressed in terms of two quantities: the privacy current $I_{privacy}(t)$, representing the rate of knowledge generation, and Deep Personal Privacy DPP(T) (Note 1), representing the cumulative depth of privacy over time.

Regulatory Thresholds

1. Instantaneous Privacy Current Threshold

$I_{privacy}(t) \leq I_{max}$(data type)

This threshold limits the maximum permissible rate of knowledge extraction for a specific category of data and prevents sudden privacy collapse events that may occur when additional information channels become available.

Cumulative Privacy Depth Threshold $DPP(T) \geq DPP_{min}$(data type, T)

This constraint ensures that uncertainty regarding an individual cannot be reduced too rapidly over time, capturing the cumulative nature of privacy erosion.

Definition — Regulatory Privacy Capacity

Regulatory Privacy Capacity (RPC) is defined as the maximum level of knowledge pressure V(t) that a system can sustain while maintaining privacy current below a predefined regulatory threshold.

$$RPC = \max V(t) \text{ such that } I_{privacy}(t) \leq I_{max} \quad (27)$$

This concept provides regulators with an operational mechanism for evaluating whether an information ecosystem can sustain additional data integration or inference processes without exceeding acceptable privacy risk levels.

The figure below illustrates how regulatory mechanisms effectively increase privacy impedance Z, thereby reducing the privacy current and slowing the rate of knowledge extraction about individuals. However since $Z_{total} = \Sigma (1 / Z\_i)$ and $I_{privacy} = V / Z_{total}$ We got the below graph.

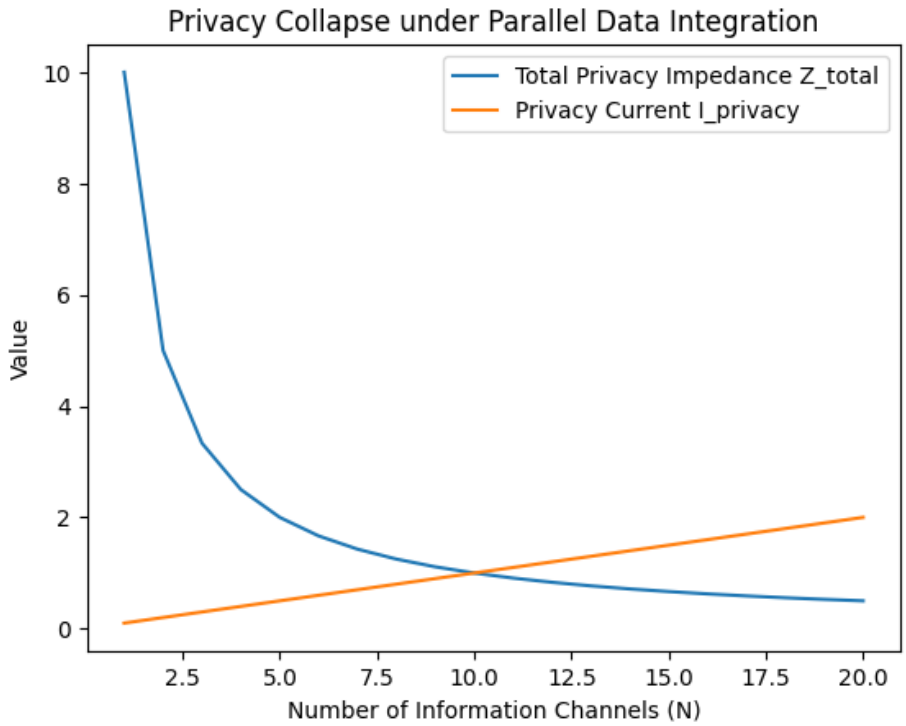

Figure 2

As privacy impedance increases due to legal safeguards, technical protections, or institutional constraints, the privacy current decreases. This relationship provides regulators with a conceptual tool for designing policies aimed at controlling knowledge extraction rates.

Regulatory Significance

By expressing privacy protection in terms of knowledge flow and system-level impedance, the DPP framework enables regulators to monitor and constrain inference processes directly. This approach is particularly important in high-sensitivity domains such as medical, financial, and mental health data, where privacy risks arise primarily from cross-dataset integration and longitudinal analysis.

8. Sensitivity-Based Categorization of Minimum DPP Thresholds (Illustrative)

This section proposes an illustrative sensitivity-based categorization for minimum Deep Personal Privacy (DPP) thresholds. The categorization is intended for analytical and regulatory discussion rather than as a prescriptive standard. The thresholds are expressed in units of hours per bit, reflecting the interpretation of Z/V as the time required to produce one bit of effective knowledge about an individual.

The proposed sensitivity tiers are grounded in three normative considerations: the potential harm associated with rapid inference, the reversibility or irreversibility of disclosure, and the externalities produced by large-scale inference across integrated information systems.

The Table below summarizes the proposed normative sensitivity tiers and their corresponding minimum Deep Personal Privacy thresholds.

Table 2

Sensitivity Level	Example Data	DPP_{min} (hours/bit)	Regulatory Meaning
Low	Preferences, basic interests	5–10	Prevent instantaneous profiling
Moderate	Location data, basic financial information	20–50	Slow behavioral inference and mobility profiling
High	Medical and mental health data	100–300	Strong epistemic protection and prevention of rapid knowledge formation

The table summarizes the proposed normative sensitivity tiers. These values are illustrative and intended to demonstrate how minimum Deep Personal Privacy thresholds may be operationalized across different categories of personal information.

Low Sensitivity Data (Non-Sensitive Interests)

$$\text{DPPmin (7 days)} = 5\text{–}10 \text{ hours/bit} \tag{28}$$

For low-sensitivity data, the potential harm resulting from rapid inference is generally limited, reversible, and often context-dependent. Such information is frequently already partially observable or voluntarily disclosed, and incorrect inference carries relatively low risk.

Moderate Sensitivity Data (Location and Basic Financial Information)

$$\text{DPP}_{\text{min}} \text{ (7 days)} = 20\text{–}50 \text{ hours/bit} \tag{29}$$

Moderately sensitive data enables meaningful behavioral inference, including habit formation, economic status estimation, and mobility profiling. Aggregation across time and platforms significantly amplifies inference capability, which justifies a higher minimum DPP threshold.

High Sensitivity Data (Medical and Mental Health Data)

$$\text{DPPmin (7 days)} = 100\text{–}300 \text{ hours/bit} \tag{30}$$

Highly sensitive information carries substantial personal and societal risks due to the depth of inference that such information enables. Inference in this domain may affect identity, employability, insurance eligibility, and social standing, which justifies significantly higher privacy depth thresholds.

Interpretation

For highly sensitive domains such as medical and mental health information, privacy protection should ensure that each bit of effective knowledge requires a substantial amount of time to be produced.

$$I_{max} = 1 / \text{DPP}_{\text{min}} \text{ (bits/hour)}$$

This transformation allows regulators or system designers to translate minimum privacy depth requirements into operational constraints on the rate of knowledge extraction within an information system.

9. Threshold-Triggered Response Policy

The DPP framework operates privacy protection through threshold-based regulatory responses. When measured privacy indicators exceed predefined limits, the system must trigger corrective actions that restore acceptable levels of privacy impedance.

Two complementary thresholds govern these responses: an instantaneous privacy current threshold and a cumulative privacy depth threshold.

9.1 Instantaneous Threshold Response

Condition: $I(t) > I_{max}$

When the privacy current exceeds the permissible maximum, an immediate operational response is required. Possible responses include tightening API access policies, reducing the resolution of shared data, introducing statistical noise, or enforcing explicit limits on inference rates.

9.2 Cumulative Privacy Depth Response

Condition: $DPP(T) < \text{DPP}_{\text{min}}$

When cumulative privacy depth falls below the minimum acceptable threshold, a broader system-level

intervention becomes necessary. Such responses may include removing parallel data channels, prohibiting cross-dataset linkage, separating identifiers from behavioral data, or revoking third‑party data sharing privileges.

Proposition — Regulatory Stability

If the instantaneous privacy current remains bounded by a regulatory threshold $I(t) \leq I_{max}$ for all t within a time window T, then the cumulative Deep Personal Privacy is bound from below.

Formally: If $I(t) \leq I_{max} \Rightarrow DPP(T) \geq T / I_{max}$

Proof Sketch. Deep Personal Privacy is defined as:$DPP(T) \int_0^T 1/I(t)\ dt$

If $I(t) \leq I_{max}$ for all t, then $1 / I(t) \geq 1 / I_{max}$. Integrating over the interval [0, T] yields:

$$DPP(T) \geq dt = T / I_{max} \quad (31)$$

This result shows that controlling the current privacy automatically guarantees a minimum cumulative privacy depth. In regulatory terms, limiting the rate of knowledge extraction ensures that privacy erosion cannot occur arbitrarily fast.

Regulatory Summary

Table 3. Sensitivity-Based DPP Thresholds

Sensitivity Tier	**Examples of Data**	**DPP_{min} (7 days) (hours/bit)**	**Derived I_{max} (bits/hour)**	**Normative Justification**
Low Sensitivity	Non-sensitive interests, general preferences	5–10	0.10–0.20	Harm from inference is limited, reversible, and context dependent. Information is often voluntarily disclosed, and incorrect inference poses relatively low risk.
Moderate Sensitivity	Location data, financial metadata	20–50	0.02–0.05	Inference enables behavioral profiling and economic classification. Effects are persistent and amplified through aggregation.
High Sensitivity	Medical data, mental health data, PHI	100–300	0.003–0.01	Inference may be deeply personal, often irreversible, and capable of causing substantial long‑term harm even without explicit disclosure.

The table summarizes the relationship between sensitivity tiers, minimum Deep Personal Privacy thresholds, and the corresponding maximum permissible privacy current values. These thresholds illustrate how regulatory policies can be operationalized using measurable knowledge‑flow indicators.

10. Algorithm for Computing Deep Personal Privacy (DPP) on a Real Graph

10.1 Graph Model

The information ecosystem surrounding an individual can be represented as a graph G = (V, E), where nodes correspond to entities capable of generating, storing, or processing information and edges represent potential information transfer or inference pathways.

• Node p denotes the individual whose privacy is being analyzed.

• Other nodes represent platforms, databases, data brokers, sensors, and inference agents.

• Each edge $e = (u \rightarrow v)$ corresponds to an information flow or inference pathway.

• Every edge is associated with a time-dependent privacy impedance Ze(t), where larger values indicate greater difficulty of information transfer or inference.

• Each actor j is associated with a time-dependent knowledge pressure Vj(t).

10.2 Computing Effective Privacy Impedance

Our goal is to compute the effective impedance between the individual p and a given inference target j, denoted Zeff(p→j)(t).

Using a path-based approximation:

1. Select dominant K paths from p to j.

2. For each path π compute impedance series: $Z\pi = \sum Ze$.

3. Combine the paths in parallel: $1 / Z_{eff} = \sum(1 / Z\pi)$.

Algorithm 1 — Practical Computation of DPP on a Graph (Kleinberg, & Tardos, 2005)

Input: Graph G=(V, E), individual node p, actor set A, impedances Ze(t), knowledge pressures Vj(t), time horizon T, number of dominant paths K.

Output: DPP(T)

Steps:

1. For each actor, j compute K-shortest impedance-weighted paths from p.

2. Compute Zπ for each path.

3. Compute effective impedance: $1/Z_{eff} = \sum(1 / Z\pi)$.

4. Compute the privacy current: $I (p \rightarrow j) = Vj / Z_{eff}$.

5. Aggregate currents: $I_{total} = \sum I (p \rightarrow j)$.

6. Compute the DPP(T) = $\sum(\frac{1}{I_{Total}})\ \Delta t$.

Proposition — Monotonic Privacy Collapse under Parallel Paths

If an additional independent information pathway is added in parallel, effective privacy impedance strictly decreases.

Proof Sketch: Since $1/Z_{eff} = \sum(1 / Z\pi)$, adding a positive term increases the right-hand side and therefore decreases Z_{eff}. The dominant computational step is computing the K-shortest paths in an impedance-weighted graph. Approximate complexity: O(K (E log V)).

10.3 Figure — Privacy Flow on Graph Network

This conceptual figure illustrates multiple inference pathways between an individual node p and inference actors. Each path carries a privacy impedance value. When additional parallel paths are introduced, the effective impedance decreases, increasing the privacy current.

Graphically, the figure represents:

p → platform → broker → inference actor

p → wearable device → cloud → inference actor

p → social network → data marketplace → inference actor

The parallel structure highlights the systemic nature of privacy collapse.

Theorem — Network Privacy Collapse Bound

Let k independent inference pathways connect an individual p to an actor j. Let Z_{min} denote the smallest impedance among these paths.

Then the effective privacy impedance satisfies: $Z_{eff} \leq Z_{min} / k$

Proof Sketch: Since 1/Zeff =, ≥ k / Zmin, it follows that Zeff ≤ Zmin / k. (32)

This theorem formalizes a central insight of the DPP model: as the number of independent information channels grows, effective privacy impedance collapses approximately inversely with the number of pathways.

Numerical Example (Medical Case)

Consider two parallel pathways from individual p to actor j.

Path 1 impedance: Z = 3 + 4 + 5 = 12.

Path 2 impedance:

$$Z = 6 + 3 + 3 = 12. \quad (33)$$

Parallel combination:

$$1/\text{Zeff} = 1/12 + 1/12 = 1/6 \rightarrow \text{Zeff} = 6. \quad (34)$$

If V = 0.6 bits/hour:I = V / Zeff= 0.6 / 6 = 0.1 bits/hour. (Doyle, & Snell, 1984)

For T = 7 days (168 hours): DPP = (Z/V) × T = (6/0.6) × 168 = 1680 hours. (This corresponds to approximately **10 hours per bit** over the window, which can be compared against the medical threshold tier defined earlier.)

11. Direct Connection to Multi-Agent Games / Nash Q-Learning / Privacy Nodes

In this framework, **DPP becomes the "currency" of a strategic game** among multiple agents.

11.1 Game Definition

Defender D: the individual, a regulator, or a privacy-preserving system. **Adversarial / collecting agents** $A_1, \dots, A_m$: AdTech platforms, data brokers, insurers, etc. **State Space (Examples):** A state $s_t$may include: Which channels are active (location ON/OFF, sensors, third-party sharing), Noise or differential privacy level (ε), Degree of identification or link ability, Edge-level impedances $Z_e(t)$derived from current configurations.

Action Space

Defender actions: Block a channel (raise $Z_e$to a very high value or infinity), Add noise (increase effective Z_e), Separate identifiers (increase Zalong cross-linking paths), Rate-limit inference (increase Zover time).

Attacker actions: Acquire a new data source (reduce Z_{eff} via parallel composition), Improve inference models (increase V), Perform identifier linking (reduce Z), Increase budget or incentives (increase V).

11.2 DPP-Based Reward Functions

To make DPP the optimization objective:

Defender reward (Note 2) $r_D(t) = \lambda \cdot DPP_{\text{gain}}(t) - c(a_D)$ $(Doyle, \& Snell, 1984)$

where $DPP_{\text{gain}}(t) = \frac{Z(t)}{V(t)}\,\Delta t,$ and $c(a_D)$denotes a *utility cost* (e.g., reduced convenience or service quality).

Attacker A_j **reward** $r_{A_j}(t) = \alpha \cdot I_{p\to j}(t)\,\Delta t - c(a_{A_j}),$ meaning the attacker benefits from increasing the knowledge flow.

11.3 Nash Q-Learning (Concise) (Kong, Chen, Yang, Cheng, Zhang, & He, 2023; Lin,& Ma, 2023)

At each state s, all players select actions, resulting in updated Z_{eff}, V, and consequently I and DPP. The Q-update for player i is: $Q_i(s, a_i, a_{-i}) \leftarrow (1-\eta)Q_i + \eta\left[r_i + \gamma \max_{a_i'} \mathbb{E}_{a'_{-i}\sim\pi^*_{-i}} Q_i(s', a_i', a'_{-i})\right],$ where π^* denotes a Nash equilibrium strategy (or an approximation thereof).

11.4 "Privacy Nodes" as Critical Nodes

Following the proposed framework (e.g., Mind / Identity / Anonymity), define a set of **critical privacy nodes** C. Define a **weighted DPP** emphasizing sensitive nodes:

$$DPP_C(T) = \int_0^T \sum_{c\in C} w_c \frac{Z_c(t)}{V_c(t)}\, dt,$$

where higher weights $w_c$are assigned to especially sensitive dimensions such as mental health or medical condition.

11.5 Simple Policy Rule (Implementation-Oriented)

Threshold-based defensive policy:

If $I_{\text{PHI}}(t) > I_{\text{PHI}}^{\max},$ then immediately block channels, add noise, or separate identifiers.

If $DPP_{\text{PHI}}(7d) < DPP_{\text{PHI}}^{\min},$ then prohibit the addition of new data sources (prevent parallel composition).

Ready-to-Use Research Package (Concise Summary)

Definition: $(T) = \int_0^T \frac{Z(t)}{V(t)}\, dt,$

Network property: $\frac{1}{Z} = \sum_i \frac{1}{Z_i}$(parallel channels)

Regulation: thresholds on $I$and DPP by sensitivity (high for PHI).

Computation: graph-based evaluation using K-path series/parallel composition or Laplacian methods.

Game-theoretic framing:

Defender Dmaximizes DPP minus utility cost; attacker Amaximizes knowledge current minus cost; Nash Q-learning (Kong, Chen, Yang, Cheng, Zhang, & He, 2023; Lin,& Ma, 2023) is used to approximate equilibrium behavior.

11.6 A Simple Numerical Example of a "Game" Between a Defender (D) and an Attacker/Collector (A), With DPP as the Currency

We use a minimal formulation: $I = \frac{V}{Z}$ (privacy current) over a time window $\Delta t = 1$ hour: $DPP_{\text{gain}} = \frac{Z}{V}\Delta t = \frac{Z}{V}$.

Players and ActionsDefender D

a. **Relax** (no hardening): $Z = 5$, cost $c_D = 0$

b. **Protect** (hardening): $Z = 10$, cost $c_D = 2$

Attacker A

a. **Low effort**: $V = 2$, cost $c_A = 0.5$

b. **High effort**: $V = 4$, cost $c_A = 2$

Reward Functions

Defender reward: $r_D = \lambda \cdot \frac{Z}{V} - c_D$, **Attacker reward:** $r_A = \alpha \cdot \frac{V}{Z} - c_A$

We choose simple parameters: $\lambda = 1,\ \alpha = 10$.

Payoff Matrix Computation

For each outcome, compute: N$DPP = \frac{Z}{V},\ I = \frac{V}{Z}$.

1) D =Relax ($Z = 5$), A =Low ($V = 2$):

a. $DPP = 5/2 = 2.5,\ I = 2/5 = 0.4$

b. $r_D = 1 \cdot 2.5 - 0 = 2.5,\ r_A = 10 \cdot 0.4 - 0.5 = 3.5$

A =**High** ($V = 4$)**:**

a. $DPP = 5/4 = 1.25,\ I = 4/5 = 0.8$

b. $r_D = 1.25,\ r_A = 10 \cdot 0.8 - 2 = 6$

2) D =Protect ($Z = 10,\ c_D = 2$)

A =**Low** ($V = 2$)**:**

a. $DPP = 10/2 = 5,\ I = 2/10 = 0.2$

b. $r_D = 5 - 2 = 3,\ r_A = 10 \cdot 0.2 - 0.5 = 1.5$

A =**High** ($V = 4$)**:**

a. $DPP = 10/4 = 2.5,\ I = 4/10 = 0.4$

b. $r_D = 2.5 - 2 = 0.5,\ r_A = 10 \cdot 0.4 - 2 = 2$

Summary Table 4. = (DPP and Rewards)

Actions	$NDPP = Z/V$	$I = V/Z$	r_D	r_A
Relax + Low	2.5	0.4	2.5	3.5 ,
Relax + High	1.25	0.8	1.25	6
Protect + Low	5	0.2	3	1.5
Protect + High	2.5	0.4	0.5	2

Nash Equilibrium Analysis

The attacker always prefers **High effort**:

a. If Relax: $6 > 3.5$

b. If Protect: $2 > 1.5$

Assuming the attacker chooses **High**, the defender's best response is:

a. **Relax**, since $1.25 > 0.5$

Nash equilibrium: (Relax, High)

Interpretation:

As long as λ is small (privacy is "not valuable enough"), the defender prefers not to pay the cost of hardening—even though this increases the privacy current.

How DPP Truly Becomes a "Currency"

Change only one parameter: the regulator increases λ, assigning greater normative value to privacy.

Let $\lambda = 2$:

a. Relax + High: $r_D = 2 \cdot 1.25 = 2.5$

b. Protect + High: $r_D = 2 \cdot 2.5 - 2 = 3$

Now the defender prefers **Protect**.

The equilibrium shifts to: (Protect, High)

That is, increasing λ loads the game with a normative value of privacy and pushes the system toward policies that increase DPP.

12. Conclusion

This article introduced a new conceptual and analytical framework for understanding privacy in contemporary information societies through the concept of Deep Personal Privacy (DPP). The central innovation of the paper lies in reconceptualizing privacy not as control over data collection, but as epistemic impedance governing the formation of knowledge about individuals within networked inference systems.

By translating the structural logic of Ohm's Law into the informational domain, the article formalizes the dynamics of privacy through the relation I_privacy = V / Z, where knowledge pressure V drives inference while total privacy impedance Z constrains the rate at which knowledge about an individual can be generated.

Within this framework, Deep Personal Privacy (DPP) is defined as the cumulative resistance to knowledge extraction over time. Unlike traditional privacy metrics that measure the quantity of collected data or provide local guarantees, DPP captures the systemic difficulty of transforming distributed data into stable knowledge across integrated information networks.

Several theoretical contributions follow from this formulation. First, the paper demonstrates that privacy degradation is inherently nonlinear under parallel aggregation of information channels, meaning that even small additional sources of information may significantly reduce effective privacy impedance. Second, classical privacy metrics such as k-anonymity, differential privacy, ENP, and DC can be interpreted as partial components within a broader impedance-based model of knowledge extraction. Third, the framework establishes formal connections between information theory, graph theory, and game-theoretic modeling, enabling both analytical and computational evaluation of privacy dynamics.

Beyond its theoretical significance, the DPP model also provides practical regulatory insights. By expressing privacy protection in terms of measurable quantities such as privacy current and cumulative privacy depth, the framework enables the formulation of operational regulatory thresholds that govern the rate of knowledge

extraction rather than merely the collection of data.

Taken together, the concept of Deep Personal Privacy offers a unified perspective that links philosophical analysis of privacy with the structural realities of contemporary data ecosystems. By focusing on the dynamics of knowledge production within networked inference systems, the framework provides a new analytical lens for understanding privacy in the age of large-scale data integration, artificial intelligence, and algorithmic governance.

References

Lin, Q., & Ma, H. (2023). SACHA: Soft Actor-Critic with Heuristic-Based Attention for Partially Observable Multi-Agent Path Finding. arXiv:2307.02691

10.3 A_Resistors_in_Series_and_Parallel, University Physics II - Thermodynamics, Electricity, and Magnetism (OpenStax)**.** Retrieved from https://phys.libretexts.org/Bookshelves/University_Physics/University_Physics_(OpenStax)

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature, 54*(2), 442-492.

CO Guidance. (2024). The UK's privacy regulator (ICO) explicitly advises that inferred data about special-category attributes *must* be treated as special-category personal data if used to decide or act on that inference.

Cover, T. M., & Thomas, J. A. (2006). *Elements of Information Theory*. Wiley.

Doyle, P. G., & Snell, J. L. (1984). *Random Walks and Electric Networks*. Mathematical Association of America, Chapter 2–3. Effective Resistance and Electrical Networks.

Dwork, C., & Roth, A. (2014). The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science.

EU GDPR – Recital 71. Retrieved January 7, 2021, from https://gdpr-info.eu/recitals/no-71/

Gavison, R. (1980, January). Privacy and the Limits of Law. *The Yale Law Journal, 89*(3), 421.

Gottlieb, C. C. (1996). Privacy: A Concept Whose Time Has Come and Gone. In David Lyon & Elia Zuriek (Eds.), *Computer, Surveillance, and Privacy* (p. 156). Minneapolis: University of Minnesota Press.

Guan, H., Yu, L., Zhou, L.-X., Xiong, L., Chowdhury, K., Xie, L.-L., Xiao, X.-S., & Zou, J. *Privacy and Accuracy-Aware AI/ML Model Deduplication,* Accepted by SIGMOD 2025. This is a pre-print version.

Helen. N. (1999, May). The Meaning of Anonymity in an Information Age. *The Information Society, 15*(2), 141-144.

HIPAA (Health Insurance Portability and Accountability Act). An official website of the United States government.

Hongladarom, S. (2016). *A Buddhist Theory of Privacy.* Singapore: Springer Singapore, p. 16.

Issa, I., Kamath, S., & Wagner, A. (2016). *An Operational Measure of Information Leakage*. IEEE Transactions on Information Theory.

Jegorova, M., Kaul, C., Mayor, C., O'Neil, A. Q., Weir, A., Murray-Smith, R., & Tsaftaris, S. A. (2022). Survey: Leakage and Privacy at Inference Time. Retrieved from https://arxiv.org/pdf/2107.01614

Kleinberg, J., & Tardos, É. (2005). *Algorithm Design*. Boston, MA, USA: Pearson Education, ch. 7, pp. 330-356.

Kong, G., Chen, F., Yang, X., Cheng, G., Zhang, S., & He, W. (2023). Optimal Deception Asset Deployment in Cybersecurity: A Nash Q-Learning Approach in Multi Agent Stochastic Games. *Applied Sciences, 14,* 357. https://doi.org/10.3390/app14010357

Laurie, G. (2002). *Genetic Privacy: A Challenge to Medico-Legal Norm.* Cambridge: Cambridge University Press, p. 6.

Millikan, R. A., & Bishop, E. S. (1917). *Elements of Electricity.* American Technical Society. p. 54.

Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. *Proceedings of the IEEE Symposium on Security and Privacy.*

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, Calif.: Stanford Law Books, p. 16.

Nissim, K. (2020, September). Differential Privacy: Why, How and Where to?. *Privacy in Challenging Times: The 8th Technion Summer School on Cyber and Computer Security*.

Rokach and Maimon. *Data Mining with Decision Trees,* 1-52.

Schoeman, F. D. (1984). Privacy: philosophical dimensions. In Schoeman, F. D. (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (p. 3). Cambridge: Cambridge University Press.

Serjantov, A., & Danezis, G. (2002, April). Towards an Information Theoretic Metric for Anonymity. *PET'02: Proceedings of the 2nd international conference on Privacy enhancing technologies,* 14 April 2002, pp. 41-53.

Shannon, C. E. (1948, October). A Mathematical Theory of Communication. Reprinted with corrections from *The Bell System Technical Journal, 27*, 379-423.

Solove, D. J. (2009). *Understanding Privacy.* London: Harvard University press, pp. 1-2.

Sweeney, L. (2002, October). k‑Anonymity: A Model for Protecting Privacy. *International Journal on Uncertainty, Fuzziness and Knowledge‑based Systems*, *10*(5), 557-570.

Ullah, I., Boreli R., &Kanhere, S. S. (2023). Privacy in targeted advertising on mobile devices: a survey. *International Journal of Information Security, 22*, 647-678 https://doi.org/10.1007/s10207-022-00655-x

Westin, A. (1984). The origins of modern claims to privacy. In Ferdinand D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 56-59). Cambridge: Cambridge University Press.

Yair, O. (2024). Personal Privacy in the Age of the Internet. *Spines,* 136-154.

Yair, O. (2025, November). The Information and Communication Technologies Expose Our Personal Identity and violate our Personal Identity. *International Journal of Blockchain Applications and Financial Technology.*

Zuboff. The Age of Surveillance Capitalism, 70.

Notes

Note 1. Formal definition represented on paragraph 6.

Note 2. The parameter λ represents the normative weight assigned to privacy protection, capturing how much the defender values incremental gains in Deep Personal Privacy relative to utility loss.

Regulatory Interpretation of λ

The parameter λcan be interpreted as an **external regulatory parameter**.

Under this interpretation, laws or regulatory authorities prescribe a **minimum value of** λ according to the sensitivity of the data type. For example:

- **General information** $\rightarrow \lambda = 1$
- **Financial data** $\rightarrow \lambda = 5$
- **Medical / mental health data** $\rightarrow \lambda = 20$

In this way, regulation effectively **injects a moral and normative value of privacy into the game**. **Connection to DPP as a "Currency"**

Through λ, new Deep Personal Privacy (DPP) becomes an explicit **strategic currency**: it determines how much utility, performance, or convenience a defender is willing—or required—to sacrifice in order to preserve privacy. The regulatory choice of λtherefore shapes the equilibrium of the multi-agent game by assigning concrete value to privacy protection rather than treating it as a purely technical constraint.

Connection to DPP as a "Currency"

Through λ, new Deep Personal Privacy (DPP) becomes an explicit **strategic currency**: it determines how much utility, performance, or convenience a defender is willing—or required—to sacrifice in order to preserve privacy. The regulatory choice of λtherefore shapes the equilibrium of the multi-agent game by assigning concrete value to privacy protection rather than treating it as a purely technical constraint.

[7] **α (Alpha)** represents the *unit value of knowledge* (per bit) for the attacker/collector agent A_j— that is, how much value the agent derives from gaining one additional bit of effective information about the individual p.

Intuitive Interpretation:

- If $\alpha = 1$: Each additional bit of knowledge yields a reward of 1 for the attacker.

If $\alpha = 10$: Each bit is worth 10 — indicating that the system (or market, or model) places very high value on

private knowledge.