SENDĀTRIX

SDX Technical Publications

SDX-TP-001

Version 1.0

Industry Perspectives on Trust, Database Security, and Structural Protection

An industry discussion examining privileged access, operational necessity, governance, Zero Trust, and the role of architecture in protecting sensitive information.

SENDĀTRIX

U.S. Patent No. 9,405,927

Industry Perspectives on Trust, Database Security, and Structural Protection

Table of Contents

Industry Perspectives on Trust, Database Security, and Structural Protection

Executive Summary

Organizations across every industry continue to invest heavily in cybersecurity, Zero Trust initiatives, least-privilege access, encryption, monitoring, and regulatory compliance. Yet one fundamental question remains surprisingly unsettled:

Do database administrators require routine visibility into sensitive production data to perform their responsibilities effectively?

To explore this question, a public discussion was initiated among database administrators, CISOs, security architects, consultants, software developers, educators, and other technology professionals. Participants were encouraged to express their own views and experiences without being directed toward a particular conclusion.

What followed was not a debate about a single technology or product. Instead, it became a broader discussion about trust, privileged access, operational necessity, Zero Trust, governance, and the evolving role of architectural controls in protecting sensitive information.

While participants often disagreed on implementation strategies, several important patterns emerged. Many experienced professionals reported that routine visibility into sensitive production data was rarely required for day-to-day administration. Others emphasized that trusted administrators should continue to possess unrestricted access because trust remains fundamental to the profession. Still others proposed workflow-driven authorization models, data masking, and architectural changes intended to reduce unnecessary exposure.

Perhaps the most significant observation was not the diversity of opinions, but the evolution of the discussion itself. What began as a question about database administration gradually became a broader examination of whether modern security should rely primarily on trusted individuals or increasingly on structural controls that limit routine exposure regardless of intent.This publication documents that discussion, summarizes the perspectives expressed by its contributors, and identifies the broader themes that emerged regarding privileged access to sensitive data.

Industry Perspectives on Trust, Database Security, and Structural Protection

1. Background

Organizations face a continuing challenge in protecting sensitive information. Cybersecurity investments continue to grow, regulations governing privacy and data protection are becoming increasingly stringent, and organizations are adopting Zero Trust architectures, least-privilege access models, data masking technologies, identity management, and expanded monitoring.

Despite these advances, one assumption has remained largely unquestioned for decades:

Should privileged database administrators retain routine visibility into sensitive production data simply because they administer the systems that store it?

Historically, the answer has often been "yes." Database administrators have been entrusted with broad privileges because they are responsible for maintaining database performance, availability, backups, recovery, troubleshooting, migrations, upgrades, and operational continuity. Trust has traditionally been viewed as one of the defining characteristics of the profession.

However, modern security thinking has begun to challenge long-standing assumptions about privileged access. High-profile data breaches involving stolen credentials, insider threats, compromised administrative accounts, and increasingly sophisticated attacks have prompted organizations to reconsider whether unrestricted visibility into sensitive information should remain an accepted architectural practice

Figure 1. The Evolution of Data Protection Thinking

From trusting people to designing systems that protect data.

At the same time, many organizations have adopted compensating controls such as data masking, role-based access restrictions, privileged access management, and workflow-based authorization to

reduce unnecessary exposure. These efforts suggest an industry-wide recognition that protecting sensitive data is no longer solely a matter of perimeter security or user authentication, but also of limiting routine visibility wherever practical.

Against this backdrop, a simple question was posed publicly:

Does a database administrator really need to see sensitive data to perform the responsibilities of the role?

The purpose was not to promote a particular technology, product, or architectural philosophy. Rather, it was to invite experienced professionals to share their perspectives based on real-world operational experience.

What began as a question about database administration evolved into a broader discussion about trust, responsibility, and the future of enterprise data protection.

Industry Perspectives on Trust, Database Security, and Structural Protection

2. Methodology

This publication documents a public discussion that took place on LinkedIn during July 2026 concerning privileged access to sensitive production data.

The discussion began with a straightforward operational question:

"Could your DBA see sensitive data if they wanted to?"

No participant was asked to support a particular position. Contributors were free to agree, disagree, challenge assumptions, propose alternative approaches, or share their own professional experiences.

Participants represented a broad range of technical disciplines, including database administration, cybersecurity, security architecture, software development, consulting, education, enterprise operations, and executive leadership.

The purpose of this publication is not to measure statistical consensus or advocate a particular technology. Rather, it documents the perspectives expressed during the discussion, identifies recurring themes, and traces how the conversation evolved over time.

Each contributor has been reviewed individually. Their comments have been summarized, key themes identified, and representative quotations retained where appropriate to preserve the intent of the discussion.

The objective is to provide an organized record of the ideas, concerns, and observations shared by experienced technology professionals regarding privileged access to sensitive data.

Industry Perspectives on Trust, Database Security, and Structural Protection

3. The Discussion Begins

The discussion did not begin as a debate about Zero Trust, least privilege, or architectural security. It began with a simple observation drawn from professional experience.

The following LinkedIn post posed a straightforward question about the reality of privileged access within modern enterprise systems. There was no expectation at the time that it would develop into a broader industry discussion.

Original LinkedIn Post

At most places I worked, if we wanted to, we could see sensitive data.

I don't mean that as an accusation. That is how the systems worked.

I was a developer. I had access. Patient records, personal financial information—it was all there if you looked. Not because someone made a mistake. Because that is how most healthcare IT environments are built.

And the thing that stuck with me was the reaction when I asked about it at different organizations.

Invariably, it was almost like a, "Yeah, duh. Of course we can see it if we want to." Like it was obvious. Like I was asking a strange question.

And to me, that was troubling.

The architecture assumed people wouldn't look. That was the entire protection model for privileged database access: trust.

Could your DBA see your sensitive records right now if they wanted to?

In most organizations, the answer is yes. And that is a design problem, not a people problem.

The responses began almost immediately. Most participants did not dispute the underlying premise. Instead, they acknowledged that privileged database administrators generally could access sensitive production data if they chose to.

With that operational reality largely accepted, the discussion quickly evolved beyond the original question. Rather than asking whether the access existed, participants began asking whether it was still necessary.

4. Perspectives from the Discussion

As the discussion expanded, participants expressed different philosophies regarding trust, operational responsibility, governance, and the role of architecture in protecting sensitive information.

Although individual opinions varied considerably, several distinct perspectives emerged. The viewpoints often overlapped, and many contributors expressed elements of more than one. Collectively, they provide a useful framework for understanding how experienced technology professionals view privileged access to sensitive production data.

Industry Perspectives on Trust, Database Security, and Structural Protection

The following sections summarize the principal perspectives expressed during the discussion.

4.1 Trust-Based Perspective

A significant number of participants viewed trust as a foundational requirement of database administration. From this perspective, organizations employ database administrators because they are expected to manage critical systems responsibly and ethically. Broad administrative privileges have historically been accepted as a necessary aspect of maintaining enterprise databases, and professional integrity remains an essential safeguard.

Contributors representing this viewpoint generally argued that technical controls cannot completely replace trust. Regardless of how security architectures evolve, organizations will always depend upon trusted personnel to administer systems, recover from failures, troubleshoot operational issues, and maintain business continuity.

Several participants also noted that privileged access is accompanied by professional accountability. Audit logging, organizational oversight, and established operational procedures were viewed as appropriate mechanisms for discouraging misuse while allowing administrators to perform their responsibilities effectively.

This perspective reflects the long-standing operational model in which trusted administrators possess broad technical capabilities, with governance and accountability serving as the primary controls against inappropriate access.

Representative Contributors and Quotations

Frank Cattelino

Frank Cattelino emphasized trust as a foundational requirement of database administration.

> *"I believe the first requirement of a DBA is trust."*

Frank argued that organizations should hire trustworthy database administrators whose professional integrity forms the foundation of responsible stewardship over sensitive information.

William McEvoy

> *"My DBA's have top secret clearance. They may see the data but they are sworn to protect it..."*

Tony Lambert

> *"Sometimes your DBA has been security cleared for exactly this reason though."*

Industry Perspectives on Trust, Database Security, and Structural Protection

Kevin Clarke

Kevin described consciously training himself to focus only on the information necessary to resolve a user's problem while deliberately ignoring unrelated sensitive information that happened to be visible.

His experience illustrates the role of professional ethics when sensitive information remains technically visible.

Trust-Based Perspective — Summary

Contributors representing this perspective consistently emphasized that trust is not merely a desirable characteristic of database administrators but an essential requirement of the profession itself. While opinions differed regarding whether architectural controls should further reduce routine visibility into sensitive information, few suggested that trust could ever be completely removed from enterprise operations.

4.2 Operational Necessity Perspective

A second group of participants focused less on trust and more on the practical realities of enterprise operations. These contributors acknowledged that unrestricted visibility into sensitive information may not always be desirable, but argued that certain operational situations continue to require direct access.

Examples frequently cited included production troubleshooting, application debugging, database migrations, disaster recovery, performance analysis, and investigating unexpected application behavior. Participants emphasized that complex operational environments often present situations that cannot be anticipated in advance, making occasional access to production data both practical and necessary.

Importantly, this perspective did not necessarily advocate unrestricted or continuous visibility. Rather, contributors generally viewed sensitive data access as an operational requirement that should occur only when justified by legitimate business or technical needs.

This viewpoint reflects a pragmatic understanding of enterprise operations, recognizing that while unnecessary exposure should be minimized, certain responsibilities may continue to require controlled access to sensitive information.

Representative Contributors and Quotations

Robert Nye

"Maybe a transaction to change a phone number failed... I need those to verify I'm working in the right record for the right person."

Robert argued that while many database operations can occur without viewing sensitive information, certain data correction and support scenarios require direct verification that the correct individual's record is being modified.

Industry Perspectives on Trust, Database Security, and Structural Protection

Jacob H.

"Yeah there's a bug regarding a few records."

"Which records?"

"You don't need to know, just fix it."

This comment demonstrates that software support often begins with identifying a specific record.

Craig Oliver

Craig Oliver described the issue from a healthcare development perspective.

He explained that there were occasions during debugging where seeing actual production information became necessary.

"To debug things, we needed to be able to see the data a lot."

"If I cannot see the data I cannot see if the results are valid."

"At some point you have to trust someone else or we never move forward."

Vanessa Eiroa

- Vanessa noted that developers may sometimes need access to underlying data when investigating unexpected results, while emphasizing that such access should remain subject to appropriate oversight.

Her comments reflected both operational necessity and the importance of governance and oversight.

David Ford

David Ford focused on the operational consequences of security restrictions, particularly their potential effect on timely technical support.

"Having been a DBA and developer for more decades than I care to think about, I've observed that 'security' is often what keeps me from doing my job ... especially doing it in a timely manner."

Operational Necessity — Summary

Contributors representing this perspective generally accepted that unnecessary exposure should be minimized whenever practical. Their primary concern, however, was preserving the ability to resolve operational issues that cannot always be anticipated in advance. From this viewpoint, the challenge

is not whether access should ever occur, but under what circumstances it becomes operationally justified.

4.3 Governance and Oversight Perspective

While some contributors emphasized trust and others focused on operational necessity, a third group approached the issue from the standpoint of governance. Their comments centered less on whether privileged access should exist and more on how organizations should control, document, approve, and audit its use.

Rather than relying solely on technical safeguards or personal trust, these participants advocated formal processes that ensure access to sensitive information occurs only when justified, authorized, and accountable.

Suggestions included workflow-based approvals, multi-person authorization, immutable audit trails, privileged access management, separation of duties, and formal review processes for exceptional access requests. From this perspective, access to sensitive information should not be eliminated where legitimate operational needs exist, but should occur within clearly defined governance frameworks designed to provide accountability and transparency.

Several contributors observed that regulatory requirements and compliance obligations have accelerated the adoption of these governance practices, particularly within healthcare, financial services, and other highly regulated industries.

This perspective reflects the continuing evolution of enterprise security from unrestricted administrative authority toward increasingly structured oversight of privileged operations.

Representative Contributors and Quotations

Gus Gwynne

- Gus argued that production access should require approval, credentials should be issued only when necessary, and access should be temporary, documented, and auditable.

Gus argued that privileged access should become an exceptional event managed through formal governance rather than routine administrative practice.

David V. Corbin

David V. Corbin described a real-world governance model based on distributed authorization.

Instead of allowing one administrator unrestricted access, his organization required multiple individuals to participate in the authorization process.

Access required multiple parties and partial passphrases before sensitive production information could be reconstructed.

David's experience demonstrated that some organizations already distribute trust among multiple individuals rather than concentrating it in a single administrator.

Industry Perspectives on Trust, Database Security, and Structural Protection

Jared Wyles

Jared Wyles emphasized governance, accountability, and controlled access to identifiable production information.

There is generally no reason to access identifiable live patient data during routine work.

- He further emphasized approvals, audit trails, traceability, and accountability as safeguards for exceptional access.

Jared argued that organizations should treat identifiable production data as an exception requiring formal oversight rather than a routine operational resource.

Richard Bennett

Richard described progressively restricting production visibility across developers, analysts, and database administrators.

His comments reflected governance through organizational policy rather than technical architecture.

Governance and Oversight — Observation

Contributors representing this perspective generally accepted that legitimate access to sensitive information will occasionally be necessary. Their emphasis, however, was that such access should be governed through documented workflows, approvals, auditing, and accountability rather than exercised as a routine administrative privilege.

4.4 Zero Trust and Least-Privilege Perspective

Another recurring perspective emphasized the continued expansion of Zero Trust principles into database administration. Participants expressing this viewpoint questioned whether privileged administrators should retain unrestricted routine visibility simply because they possess administrative responsibilities.

Instead, they argued that access should be granted only when operationally necessary, limited to the minimum information required, and removed once the specific task has been completed. Several contributors viewed this approach as a natural extension of least-privilege principles that are already widely applied to networks, identities, and applications.

Rather than questioning the integrity of administrators, these participants viewed reduced routine visibility as an architectural improvement that better aligns enterprise systems with contemporary security practices.

This perspective represents a shift away from assuming broad administrative visibility as the default operating model and toward minimizing routine exposure wherever practical.

Industry Perspectives on Trust, Database Security, and Structural Protection

Robert Nye

Robert Nye consistently framed the discussion through the principles of Zero Trust rather than traditional administrative authority. He emphasized that access decisions should be based on the specific operation being performed rather than on broad role-based privileges.

"Right Person. Right Credentials. Right Equipment. Right Operation."

His comments reflected a security model in which trust is continuously evaluated within the context of each authorized activity rather than granted simply because an individual holds an administrative position.

Michael de Geus

Drawing on his experience in executive protection, Michael de Geus broadened the discussion beyond database administration by observing that the most difficult threats often originate from individuals who already possess legitimate credentials and authorized access.

"An insider doesn't need to defeat your security.

They were invited through it."

His observations reinforced the principle that security should not focus exclusively on preventing unauthorized access, but also on limiting the consequences of authorized access whenever practical.

Myroslav R.

Throughout the discussion, Myroslav repeatedly challenged participants to reconsider long-standing assumptions regarding privileged database access.

Rather than accepting administrative visibility as inevitable, he continually returned to a more fundamental question:

"How do you prevent the DBA?"

His comments encouraged participants to consider whether architectural approaches might reduce routine exposure instead of relying primarily on trusted administrative roles.

Jared Wyles

Jared emphasized that identifiable production information should rarely be required during normal operational activities. His comments aligned closely with least-privilege principles by arguing that access to sensitive information should occur only when operationally justified and accompanied by appropriate oversight.

Industry Perspectives on Trust, Database Security, and Structural Protection

---

"There is generally no reason to access identifiable live patient data during routine work."

His perspective reflected a growing preference for minimizing routine visibility rather than assuming unrestricted administrative access.

Zero Trust and Least-Privilege — Observation

Contributors representing this perspective generally agreed that trusted administrators will remain essential to enterprise operations. Their primary argument, however, was that trust alone should no longer determine routine access to sensitive information. Instead, access should be continuously evaluated, limited to the minimum information necessary for the task being performed, and removed when no longer required.

For these participants, Zero Trust extended beyond authenticating users and devices. Increasingly, it also meant reducing routine exposure of sensitive information itself.

4.5 Structural Protection Perspective

As the discussion evolved, a smaller but particularly noteworthy perspective began to emerge. Rather than concentrating exclusively on who should be permitted to access sensitive information, several participants questioned whether modern architectures could reduce or even eliminate routine exposure by changing how sensitive information is stored, protected, and made available.

This viewpoint shifted the conversation beyond governance and authorization toward architectural design. Instead of relying primarily on trusted individuals, oversight processes, or compensating controls, these contributors suggested that future systems may increasingly reduce routine exposure through structural approaches that separate normal operational activities from direct visibility into sensitive information.

Although participants proposed different methods for achieving this objective, they shared a common observation: architectural design itself can become an active security control rather than simply a platform upon which other controls operate.

This perspective does not represent a consensus position. Rather, it reflects an emerging line of thought that complements existing security practices by exploring whether structural separation can reduce routine exposure while preserving legitimate business operations.

Robert Nye

Robert repeatedly emphasized the concept of separating trust from authority. Rather than relying upon a single privileged administrator, he described architectures in which authorization decisions are distributed across multiple independent elements.

"Right Person. Right Credentials. Right Equipment. Right Operation."

Industry Perspectives on Trust, Database Security, and Structural Protection

His comments illustrated that structural separation can strengthen security by ensuring no single factor alone is sufficient to expose sensitive information.

Anthony Derbidge

Anthony consistently encouraged participants to think beyond traditional database controls and consider architecture itself as the primary security mechanism.

Rather than adding additional protective layers around existing systems, he suggested rethinking the underlying design so that sensitive information is inherently more difficult to expose.

Anthony's perspective reflected the belief that durable security begins with architectural design rather than with incremental security controls applied after the fact.

Myroslav R.

Throughout the discussion, Myroslav repeatedly challenged assumptions regarding privileged database access.

His recurring question,

"How do you prevent the DBA?"

---

shifted attention away from administrator trustworthiness and toward whether system architecture itself could reduce or eliminate routine visibility into sensitive information.

His comments helped move the discussion beyond administrative policy and toward structural design.

Craig Oliver

Although Craig described situations where production information occasionally became necessary for troubleshooting, he also acknowledged that not every operational activity requires direct visibility into sensitive identities.

His observations reflected a broader recognition that many routine technical tasks can be performed using structural information, metadata, or non-identifiable data, reserving access to sensitive information for exceptional circumstances.

Structural Protection — Observation

Unlike the earlier perspectives, contributors representing this viewpoint focused less on determining who should receive privileged access and more on questioning whether routine privileged visibility should remain an architectural assumption at all.

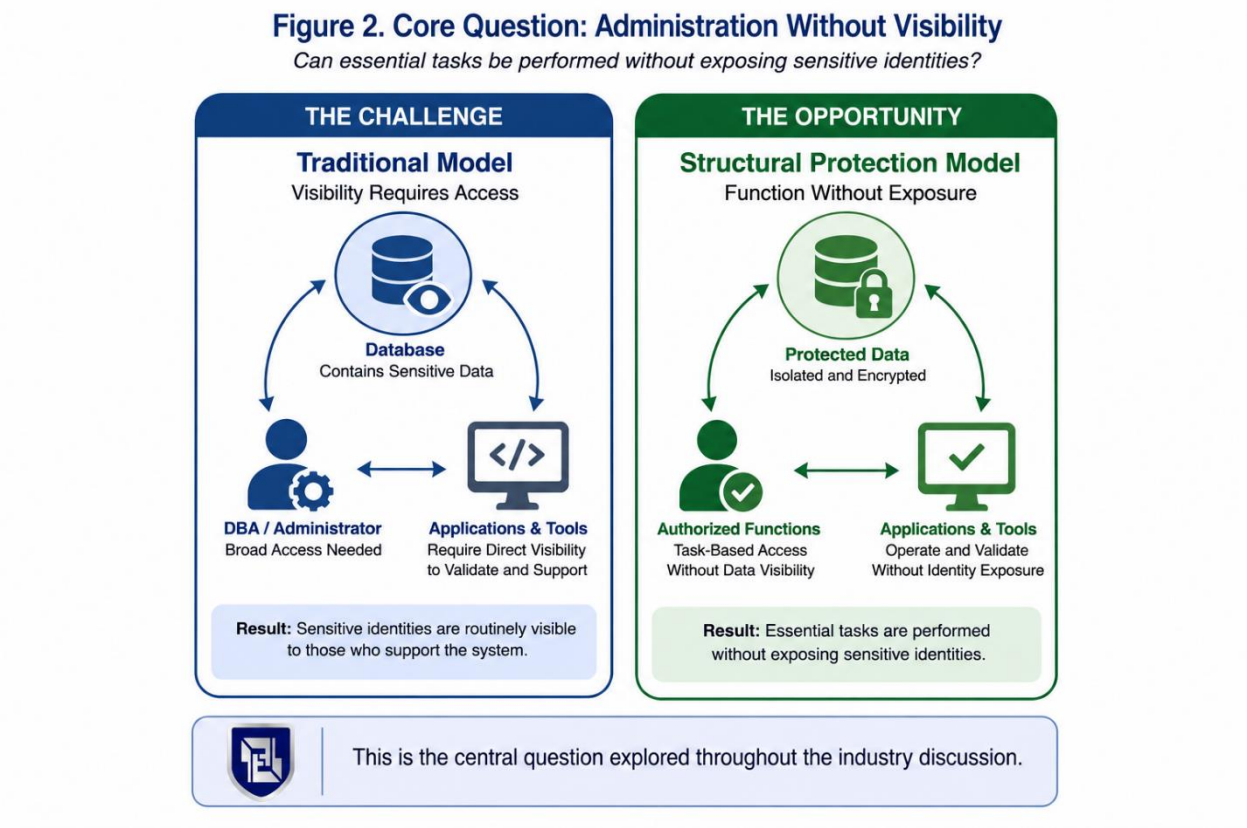
Industry Perspectives on Trust, Database Security, and Structural Protection

Rather than replacing encryption, authentication, authorization, or governance, these participants viewed structural approaches as complementary mechanisms capable of reducing routine exposure before traditional security controls are required.

Although relatively few contributors expressed this perspective directly, the broader discussion gradually evolved toward many of the same questions, suggesting growing interest in architectures that minimize routine visibility rather than simply controlling access to it.

Industry Perspectives on Trust, Database Security, and Structural Protection

5. Themes That Emerged



Theme 1 — Trust Remains Essential

Nearly every contributor acknowledged that trust remains fundamental to enterprise operations. Few questioned the professionalism or integrity of database administrators. Instead, the discussion explored whether architecture is able to reduce the amount of trust any single role must carry while preserving operational effectiveness.

Theme 2 — Routine Visibility Is Increasingly Questioned

Although opinions differed regarding implementation, many participants questioned whether unrestricted routine visibility into sensitive production data should continue to be accepted as the default architectural model.

Theme 3 — Security Is Expanding Beyond Perimeter Defense

Several contributors observed that modern threats increasingly originate from individuals and systems that already possess legitimate credentials. As a result, attention is shifting from preventing unauthorized access toward limiting the consequences of authorized access.

Industry Perspectives on Trust, Database Security, and Structural Protection

Theme 4 — Governance Alone May Not Be Sufficient

Workflow approvals, auditing, and accountability were widely supported. However, several participants suggested that governance mechanisms complement—but do not necessarily eliminate—the underlying architectural exposure.

Theme 5 — Architecture Is Becoming Part of the Security Model

Perhaps the most significant theme was the evolution of the discussion itself. What began as a conversation about database administration became a broader examination of whether architectural design can reduce routine exposure before traditional security controls are required.

6. Observations

The discussion did not produce unanimous agreement regarding the future of privileged database access. Contributors represented a broad range of professional backgrounds and operational environments, and their views reflected different balances among trust, operational responsiveness, governance, and architectural control.

Nevertheless, several consistent observations emerged.

Very few participants disputed that privileged administrators typically possess routine visibility into sensitive production data today.

Many contributors accepted this as an operational necessity, while others questioned whether evolving security practices may justify reducing such visibility through workflow, governance, or architectural change.

The discussion also suggested that Zero Trust principles are expanding beyond networks and identities toward the protection of sensitive information itself.

Perhaps most notably, the conversation gradually shifted away from asking **who** should have access — toward asking whether system architecture can reduce the need for routine access in the first place.

Rather than producing a single conclusion, the discussion revealed an industry reexamining long-standing assumptions about privileged access and enterprise data protection.

7. Future Questions

The discussion raises several questions that may shape future enterprise security architectures:

- Must sensitive information remain routinely visible inside operational databases?
- Can architecture reduce dependence on trusted individuals without reducing operational effectiveness?

Industry Perspectives on Trust, Database Security, and Structural Protection

- How should organizations balance rapid operational response with minimizing routine exposure?
- Can structural approaches complement encryption, authentication, authorization, and governance rather than replace them?
- As Zero Trust continues to evolve, should it increasingly apply to sensitive data itself rather than only to identities, devices, and networks?

These questions remain open for continued discussion, evaluation, and independent research.