TECHNOLOGY TRANSFER PRESENTS

DEREK STRAUSS

ALAN RODRIGUEZ

THE SMART DATA PROTOCOL

A REVOLUTIONARY DATA PROVENANCE, SECURITY, AND PRIVACY SOLUTION

ONLINE LIVE STREAMING

JUNE 12-13, 2024

DUE TO TIME ZONES, THIS CLASS WILL TAKE PLACE IN 2 AFTERNOONS
FROM 2 PM TO 6 PM ITALIAN TIME

info@technologytransfer.it
www.technologytransfer.it

ABOUT THIS SEMINAR

The Internet's original creators worked on technologies to bind contracts to data. They imagined digital contracts attached to our data everywhere it moves; contracts that assert ownership, record provenance, limit use by others and even revoke access. Had these ideas of binding software to data been allowed to mature, the digital landscape would look and function entirely differently.

The Smart Data Protocol binds software contracts to data while formulating data products that control who, where, when, and how others use your data, unlocking unprecedented revenue-generating opportunities combined with significant risk reduction.

Smart Data empowers data products with secure, private & trusted data sharing within and between organizations. A trusted data products foundation forms the cornerstone of AI technologies, underscoring their reliability, ethical use, and efficacy. At its core, AI relies on data as its lifeblood, drawing insights and making decisions based on the information it ingests. A foundation built on trusted data products ensures the integrity, quality, and ethical sourcing of data, mitigating biases and inaccuracies that could skew AI-driven outcomes.

This foundation engenders trust among users, stakeholders, and society at large, fostering confidence in AI systems' outputs and ethical compliance. It's the bedrock upon which responsible AI flourishes, fostering innovation while prioritizing privacy, fairness, and transparency, essential for sustainable and beneficial integration of AI technologies into our lives.

The leadership opportunity to create data products based on revolutionary thinking.

Data security and privacy are hot topics in the boardrooms of every organization. Chief Data and Analytics Officers increasingly need to take an active business leadership role in addressing the complex issues underpinning these topics. Business leaders are realizing that security and privacy cannot be delegated to IT and then forgotten.

This seminar addresses the key issues involved in adopting the Smart Data Protocol and provides insight into what Data, Analytics and AI Leaders need to know about developing data security and privacy solutions in the age of GenAI.

WHAT YOU WILL LEARN

- How the Smart Data Protocol combines modem cryptographic innovations with proven enterprise data technologies
- How Privacy Enhanced Technologies enable unimaginable data-sharing opportunities
- How Smart Data empowers data products with secure, private & trusted data sharing within and between organizations
- How Smart Data creates a functional Data Economy to source specialized datasets for advanced AI training while compensating creators

OUTLINE

1. Introduction to Data Security and Data Privacy fundamentals

These are key topics for today's AI & Data Executive, and they need to be addressed in collaboration with the Chief Privacy Officer and the Chief Information Security Officer.

We will briefly discuss:

- Ownership - Individuals own their own data
- Transaction Transparency - If an individual's personal data is used, they should have transparent access to the algorithm design used to generate aggregate data sets
- Consent - If an individual or legal entity would like to use personal data, one needs informed and explicitly expressed consent of what personal data moves to whom, when, and for what purpose from the owner of the data
- Privacy - If data transactions occur all reasonable effort needs to be made to preserve privacy
- Currency - Individuals should be aware of financial transactions resulting from the use of their personal data and the scale of these transactions
- Openness - Aggregate data sets should be freely available
- Algorithm Transparency - Inclusiveness/exclusiveness of certain sectors of the population based on use of Algorithms

2. "Consent Technology" – securing, protecting, and monitoring data everywhere it moves, at the data level

While a layered security approach will always provide the best protection, our current approaches leave data vulnerable and unprotected at its source. We hear about data breaches and ransomware attacks almost daily. Once the perimeter is breached, or identity is compromised by social engineering, the underlying data is exposed. This hoard of gold doesn't need to be taken. It needs to be copied at near-zero cost and leave no trace. Everywhere our data is copied and stored, it remains inert and passive, with no capacity to control how others access and use it and no capacity to take defensive action and intelligently mitigate risks.

We need another layer around an individual's data – a Data Container. These data containers wrap the data in software that provide a range of intelligent or "smart" capabilities such as (1) data access control and consent revocation, (2) an immutable state engine for proof of data provenance, and (3) intelligent risk awareness and mitigation. Smart Data imbues our existing data with self-awareness, group intelligence, programmability, and automation. This is accomplished by binding smart contracts to data that control who, when, where, and how others access and use the contained data everywhere smart data is shared or monetized.

3. The data risk-reward paradox and the in evitability of Smart Data

Data and security leaders often find themselves in a quandary. The Data Science community and the analytics teams have a seemingly insatiable demand for free — and immediate — access to all the data generated by the organization. This can be challenging when your role is to secure the organization's data.
On the one hand, there is a need to unleash innovation, and on the other hand, there is a need to control

risk. This can create conflict, friction, and drama in the best of cultures.

Due to increasing pressure to innovate and drive value out of existing enterprise data assets, the business may accept high-risk use cases as a competitive necessity. In some extreme cases, businesses shelve high-value use cases until later due to their high risk. Both situations are undesirable and place senior data and security leaders in challenging "no-win" situations. How can Smart Data address this quandary?

4. The Open Data Object Standard and the Data State Engine

How can data protect itself without relying entirely on the established layers of defense, including physical barriers like network security and firewalls, operating system security, and identity and access management to networks and applications? There are several examples of proven enterprise-ready technologies that have been developed to address this key issue.

In addition, Blockchains already provide communities with cryptographic verifiable State Engines, which are trusted by tens of millions of users to create digital currencies and facilitate tens of millions of transactions a day. The expanding trust in the integrity of these shared community-operated State Engines has empowered a rapidly expanding set of Blockchain use cases across all major industries.

In the same way, a data container State Engine will empower a wide range of data integrity, provenance, and trusted use cases that are simply unavailable with today's data, security, and cryptographic paradigms.

5. Future Data Exchanges and their reliance on Privacy Enhanced Technologies (PETs)

There is immense value in data-sharing between organizations. In many industries, we see a significant increase in collaborations across use cases ranging from fraud detection, health contact tracing, and economic systemic risk analysis to enabling new forms of user personalization across digital services.

Of course, sharing data is not without risks. The benefits of data collaborations are balanced against customer privacy, data security, and control of competitively sensitive data. These tensions have resulted in shelving many promising data-sharing opportunities long before deployment.

However, an emerging set of technologies called Privacy Enhancing Technologies (PETs) have the potential to fundamentally redefine the dynamics of data-sharing by eliminating or reducing the risks associated with complex or multi-party data collaboration. As these technologies mature, they will demand a reexamination of mothballed data-sharing projects and the exploration of previously unimaginable opportunities.

6. Emerging Standards for Secure and Private Data Exchange

Emerging PETs have developed new approaches to clear the path to innovation. The speed at which organizations can adopt these new approaches will determine their capacity to get ahead of the game in data-driven innovation.

If the CDO community adopts a strategic approach to PETs, their organizations may finally escape the privacy versus value creation dilemma. PETs have the potential to fundamentally redefine the dynamics of data-sharing by eliminating or reducing the risks associated with complex or multi-party data collaboration. Smart Data acts as a standard for the choreography of PETs within and between organizations.

7. Modern Data Governance – managing Smart Data as a Product

Over the last decade, many Chief Data Officers followed one of two data governance strategies.

In a grassroots 'business-focused' strategy, each team pursuing individual use cases assembles the necessary data and technologies. This approach results in significant duplication of efforts and a tangle of redundant technology architectures that are costly to build, manage, and maintain.

Meanwhile, in a big bang 'technology-focused' strategy, a centralized team organizes, cleanses, and aggregates all organizational data assuming this effort will drive all use cases. This approach does enable some data reuse, but it's often not aligned with business use cases and therefore fails to support end users' specific needs. In response to the inevitable lack of business value, new use cases are funded and aligned with specific business priorities, often triggering a grassroots approach and its associated problems.

Companies are most successful when they adopt a 'data-product-focused' strategy, treating data like a product. Basing the Data Product's design on the Smart Data Protocol allows the organization to increase its effectiveness and speed of innovation. Smart Data empowers data products with secure, private & trusted data sharing within and between organizations.

8. Getting started with Smart Data

A practical guide to getting started on your journey with Smart Data.

WHO SHOULD ATTEND

This course is intended for any role involved in the planning and implementation of Data Security and Data Privacy solutions including:

- Executive Stakeholders – Data & AI
- Data, Analytics and AI Leaders
- Chief Privacy Officers
- Chief Compliance Officers
- Chief Information Security Officers
- Data Scientists
- Business Technology Partners
- Business Analysts
- Enterprise Architects
- Data & AI Architects

Speakers

Derek Strauss Founder, CEO and Principal Consultant of Gavroshe. Former Chief Data Officer at TD Ameritrade for approximately 5 years; was responsible for Data Governance, Data Science & Advanced Analytics, Data Architecture & Management, and Development and Maintenance of Enterprise-class Data Assets.

A career of over 3 decades, mainly in the Data Management and Information Resource Management (IRM) fields. Established Office of the CDO, Data Resource Management, Architecture and IRM Functions in multiple large Corporations. Established and managed numerous enterprise programs and initiatives in the domains of Big Data, Advanced Analytics, Business Intelligence, Data Warehousing, Data Quality Improvement and IRM. Bill Inmon's Corporate Information Factory and John Zachman's Enterprise Architecture Framework have been the foundational cornerstones of the above work.

Served as VP Programs for DAMA SW Ohio. Active member of MIT's Chief Data Officer Roundtable and Forum, and Founding Member of the International Society of Chief Data Officers. Co-authored DW 2.0: The Architecture for the Next Generation of Data Warehousing Inmon, Strauss and Neushloss (Book published 2008 by Morgan Kaufman, Series in Data Management Systems).

Alan Rodriguez is a product and data leader with 20+ years' experience envisioning and building cutting edge digital solutions. Alan has a passion for digital strategy, innovation, and emergent digital business models. He brings a balance of practical and philosophical thinking to all endeavors and believes technology must be thoughtfully designed to serve humanity.

Over the course of Alan's career he's invented and coded first-generation payment gateways at Chase/Paymentech, created first-generation global B2B trading & supply chain platforms at Quadrem/Ariba/SAP, and invented and created first-generation B2C and B2B marketing, preference centers, adtech, customer loyalty, community & engagement platforms at Tribal Worldwide/Omnicom.

As the CEO and Founder of Accesr – his team is creating media and data containers as programmable, transferable, encryptable, cacheable, and remotely controllable data building blocks designed to ensure the owners of data can constrain and direct it's uses everywhere it flows and grows.

INFORMATION

PARTICIPATION FEE

€ 750

The fee includes all seminar documentation.

SEMINAR TIMETABLE

2.00 pm - 6.00 pm (Italian Time)

HOW TO REGISTER

You must send the registration form with the receipt of the payment to:
info@technologytransfer.it

TECHNOLOGY TRANSFER S.r.l.
Piazza Cavour, 3 - 00193 Rome (Italy)

PAYMENT

Wire transfer to:
Technology Transfer S.r.l.
Banca: Credit Agricole
Agenzia 1 di Roma
IBAN Code:
IT 03 W 06230 03202
000057031348
BIC/SWIFT: CRPPIT2P546

GENERAL CONDITIONS

DISCOUNT

The participants who will register 30 days before the seminar are entitled to a 5% discount.

If a company registers 5 participants to the same seminar, it will pay only for 4.

Those who benefit of this discount are not entitled to other discounts for the same seminar.

CANCELLATION POLICY

A full refund is given for any cancellation received more than 15 days before the seminar starts. Cancellations less than 15 days prior the event are liable for 50% of the fee. Cancellations less than one week prior to the event date will be liable for the full fee.

CANCELLATION LIABILITY

In the case of cancellation of an event for any reason, Technology Transfer's liability is limited to the return of the registration fee only.

DEREK STRAUSS
ALAN RODRIGUEZ

The Smart Data Protocol

June 12-13, 2024

Registration fee:
€750

first name .....

surname .....

job title .....

organisation .....

address .....

postcode .....

city .....

country .....

telephone .....

fax .....

e-mail .....

Stamp and signa-

If registered participants are unable to attend, or in case of cancellation of the seminar, the general conditions mentioned before are applicable.

Send your registration form with the receipt of the payment to:
Technology Transfer S.r.l.