

Building Brand Trust with Responsible Data Practices

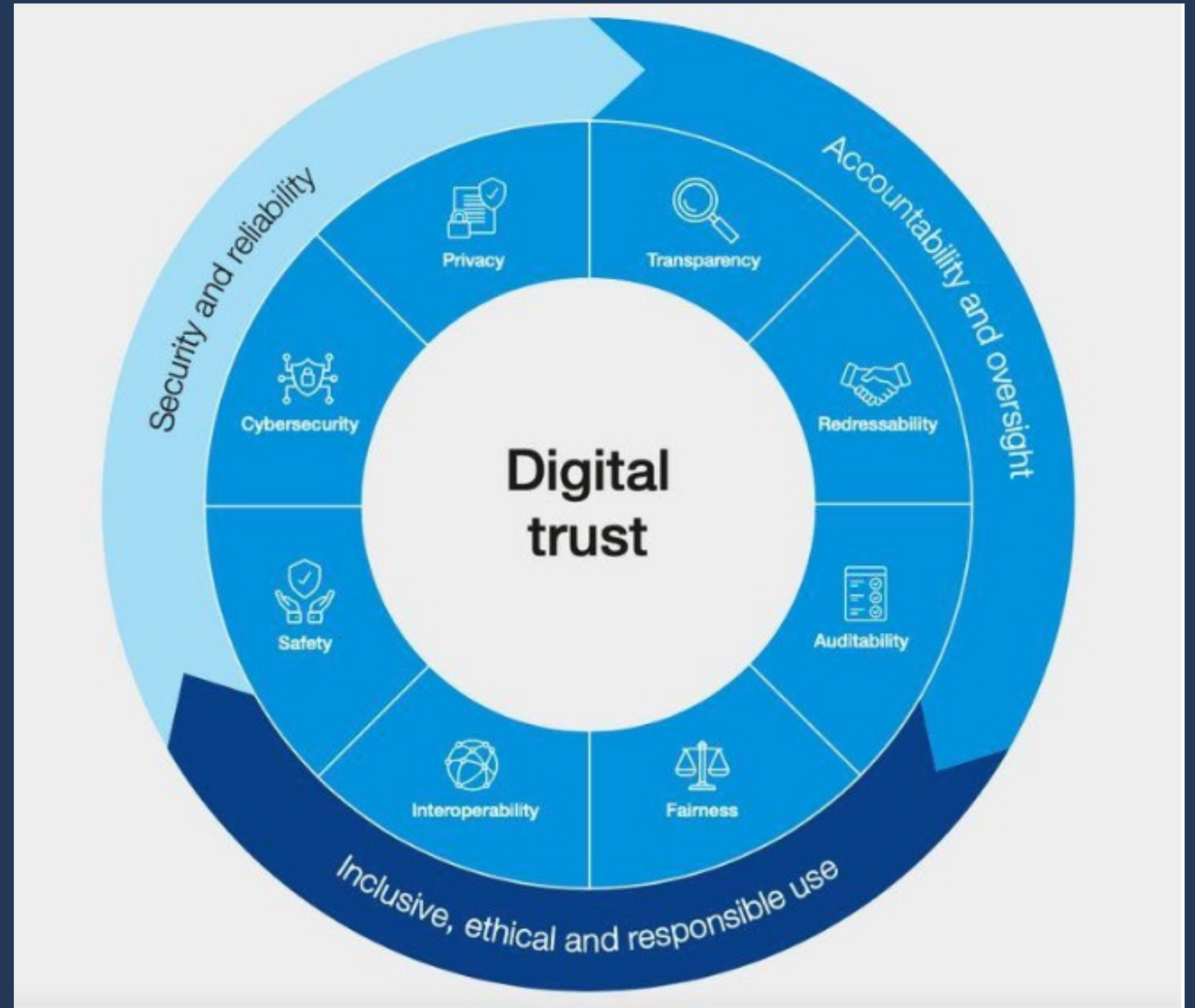
Privacy + Security Forum Fall Academy

November 12, 2025



Agenda

- Background
- Trust Standards
 - Legal
 - Industry
 - Follow the Arrow
- Business Enabling Trust
 - Risks and Benefits
 - Operational Design
 - Technical Design



Speakers



Matthew Coleman

Partner – AI, Cyber, Privacy & Data
Orrick, Herrington & Sutcliffe LLP



Jeffrey Dunifon

Sr. Director, Privacy & Data
Security Counsel
Dexcom



William Marden

Director of Privacy and
Compliance
New York Public Library

Background

Digital Trust



“Digital trust is...

individuals’ expectation that digital technologies and services – and the organizations providing them – **will protect all stakeholders’ interests and uphold societal expectations and values”**

– World Economic Forum Digital Trust Initiative

85%

respondents of a survey of more than 1,300 business leaders and 3,000 consumers globally **say that knowing a company's privacy policies is important before making a purchase.**

Source: *Why digital trust truly matters*, McKinsey ([link](#))

46%*

often or always consider another brand if the one they are considering purchasing from **is unclear about how it will use their data.**

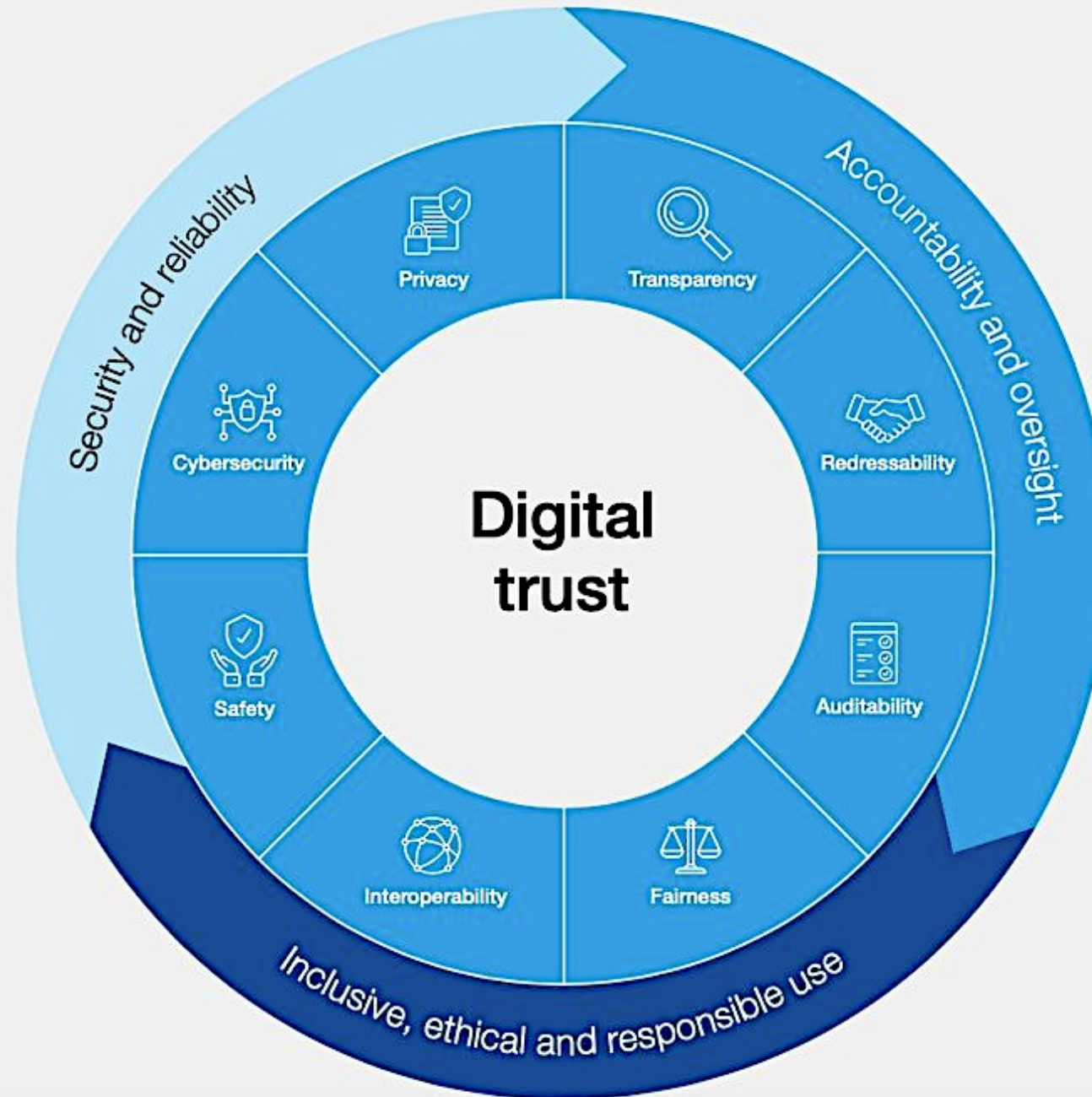
* Increases to **50%** for Millennial/Gen Z respondents, **56%** for B2B buyers, and **58%** for APAC respondents.

Source: *Why digital trust truly matters*, McKinsey ([link](#))

>10%

organizations that are best positioned to build digital trust are also more likely than others to see **annual growth rates of at least 10 percent on their top and bottom lines.**

Source: *Why digital trust truly matters*, McKinsey ([link](#))



Sources: WEF Digital Trust Framework, WEF ([link](#)); Earning Digital Trust, WEF with Accenture, KPMG, and PwC ([link](#)); Measuring Digital Trust: Supporting Decision-Making for Trustworthy Technologies, World Economic Forum with Accenture ([link](#))

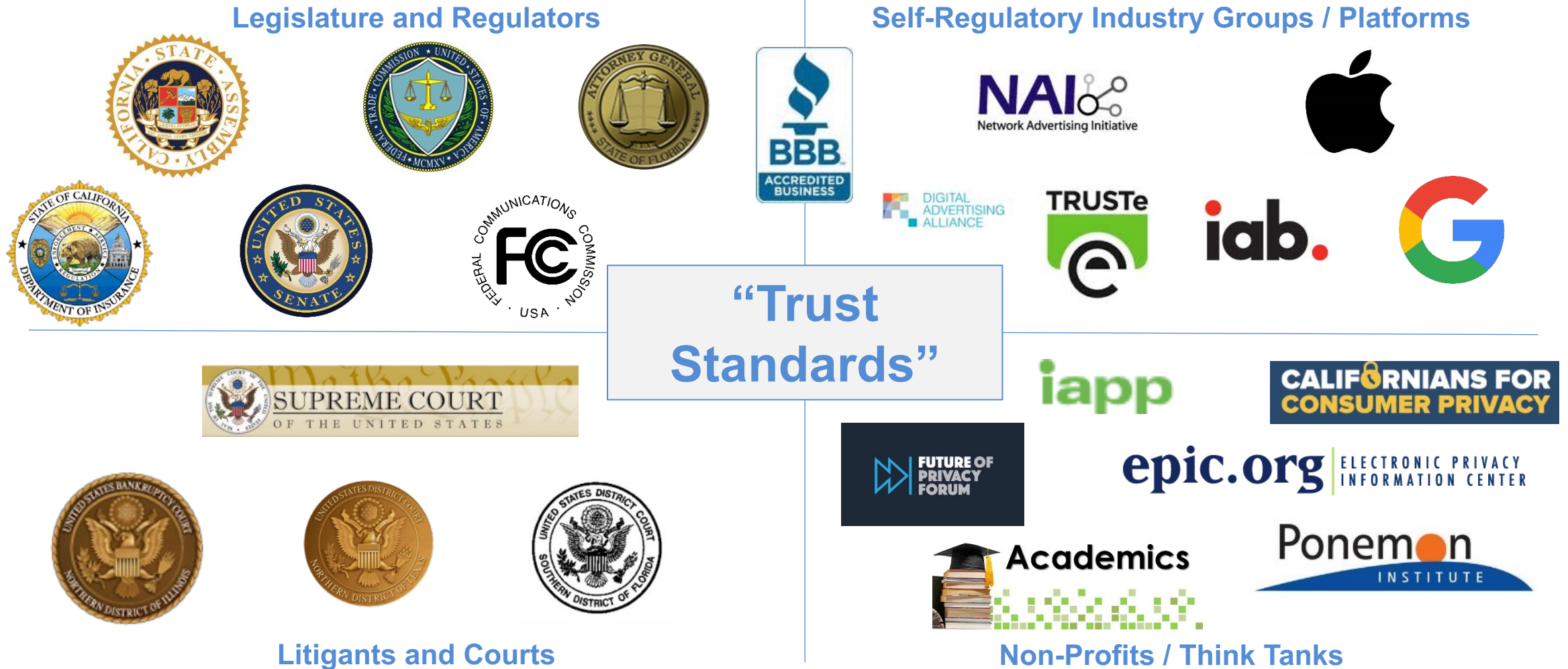
See also: Why digital trust truly matters, McKinsey ([link](#)); Understanding the Full Digital Trust Ecosystem, ISACA ([link](#))

Trust Standards

Legal



Basis for U.S. Trust Standards



New York Public Library

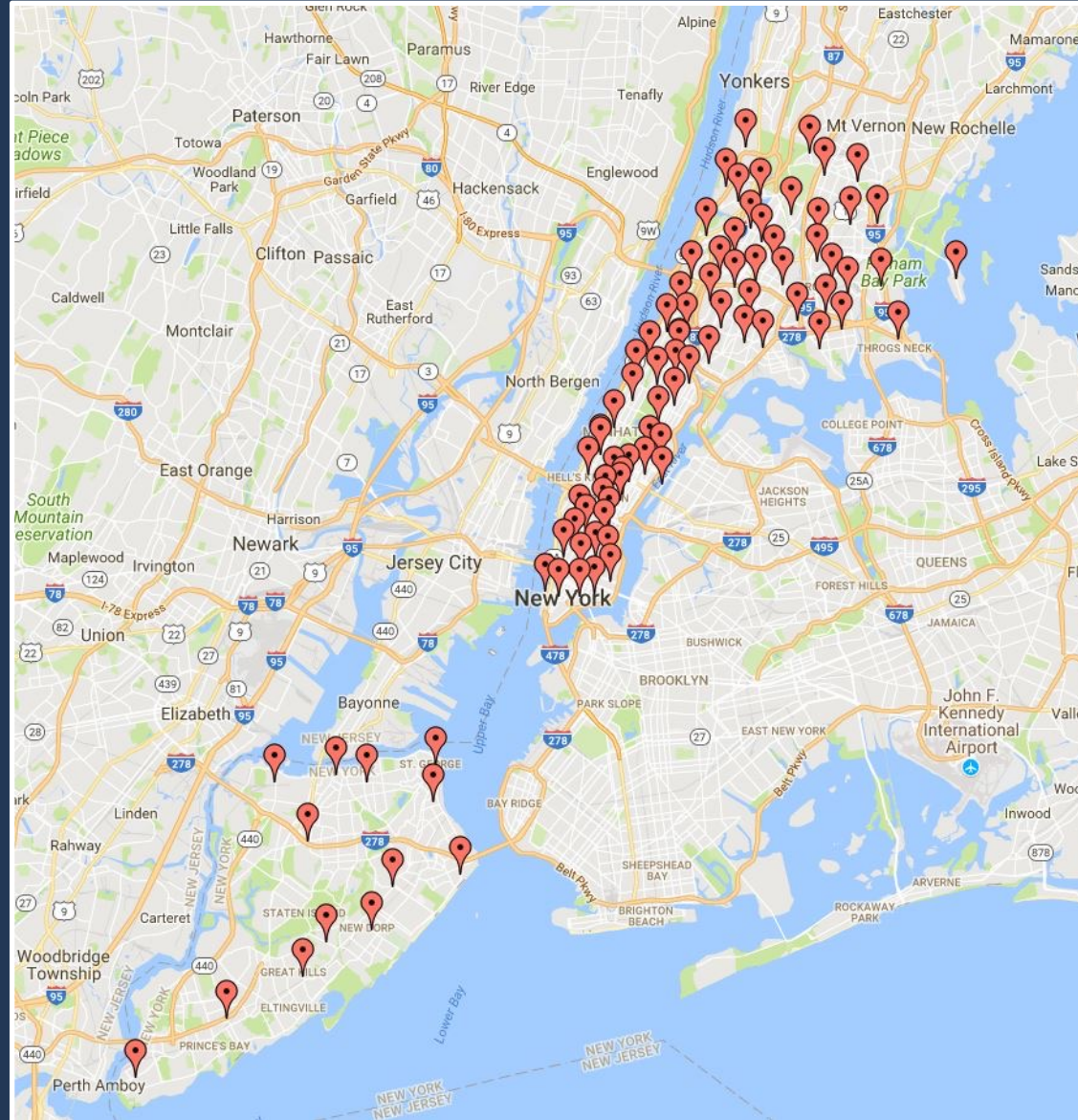


- Fourth-largest library in the world (per cataloged no. of items)
- Largest public library in the U.S.
- Staff of 2,500 people delivering library services across the Bronx, Manhattan, and Staten Island through a network of 88 neighborhood branches, online access, plus four internationally-renowned research centers:
 - Stephen A. Schwarzman Building (SASB)
 - Library for the Performing Arts (LPA) at Lincoln Center
 - Schomburg Center for Research in Black Culture
 - Thomas Yoseloff Business Center

Serving 3 of NYC's 5 boroughs: Bronx, Manhattan, and Staten Island



88 branches and 4 research libraries



New York Public Library: The Numbers



- 2.4 million library card holders
- 17 million items (print and non-print) borrowed annually
- 5.3 million reference queries
- 24 million website visits (www.nypl.org)
- Over 5,000 publicly-available computers, utilized in 1.5 million sessions
- 2.5 million sessions connecting to NYPL's WiFi network
- 1.3 million people attended a library program

Types of Library Data

Digital

- Circulation records
- Borrowing requests
- Reference questions (online chat, e-mail, etc.)
- Online catalog searches
- Online ticketing for events
- Applications for library cards
- In-library computer use

Analog

- Call slips (e.g., for research collections)
- Applications and order forms (library cards, events, etc.)
- Receipts for check-ins, check-outs, fines, etc.

Personal Knowledge



The library, as the unique sanctuary of the widest possible spectrum of ideas, must protect the confidentiality of its records in order to insure its readers' right to read anything they wish, free from the fear that someone might see what they read and use this as a way to intimidate them....

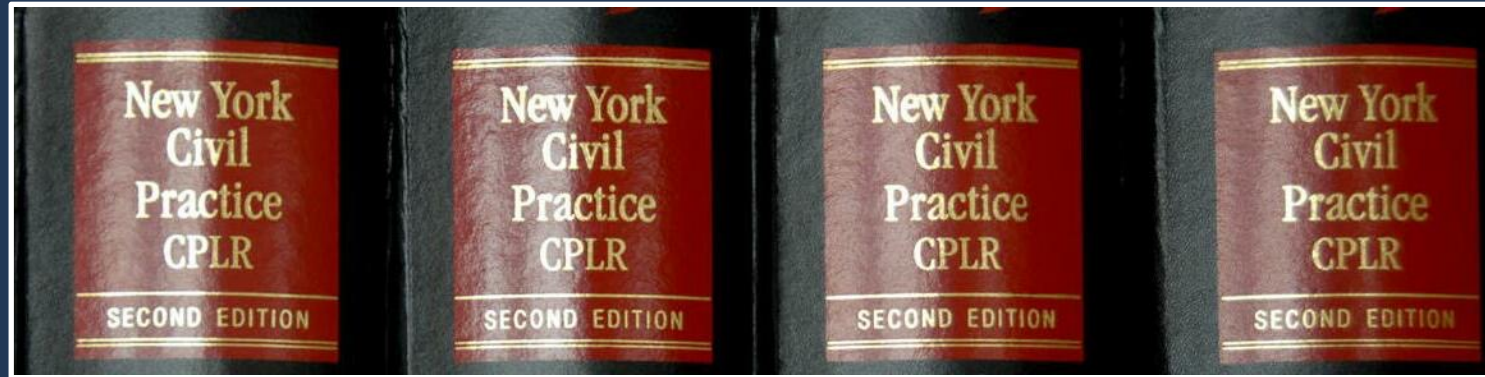
— Supporting documentation for 1981 passage of the New York State Library Privacy Law (NYS Statute CPLR §4509)



Without such protection there would be a chilling effect on our library users as inquiring minds turn away from exploring varied avenues of thought because they fear the potentiality of others knowing their reading history.

— Supporting documentation for 1981 passage of the New York State Library Privacy Law (NYS Statute CPLR §4509)

New York State statute: CPLR §4509



"Library records...shall be confidential and shall not be disclosed except...to the extent necessary for the proper operation of such library and shall be disclosed upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute."

Dexcom



Who We Are

A global leader in Continuous Glucose Monitoring (CGM) technology for people with diabetes.

Mission

Empowering people to take control of diabetes through real-time glucose insights.

What Matters to Patients

- Accuracy and reliability of glucose readings
- Ease of use and seamless integration with daily life
- Improved health outcomes and quality of life

Dexcom

Examples of information collected from CGM users includes...

- **Personal Identifiers** like name, DOB, address, email address, phone number
- **Health Information** like glucose sensor readings and trends, diabetes diagnosis and related medical details, and other health-related inputs (e.g., insulin usage, meal data when entered)
- **Device and Technical Data** like device identifiers (e.g., transmitter ID, receiver serial number), mobile device type and operating system, app usage logs and connectivity status
- **Account and Service Information** like login credentials and account settings, preferences for notifications and data sharing, records of consent for marketing or analytics
- **Third-Party and Integration Data** like information from authorized third-party apps or healthcare providers, data shared through interoperability features (e.g., Dexcom Clarity uploads)



Digital Trust Standards in Health – Laws and Regulations

Requirements driven by legislation, regulation, case law, and other legal requirements

- [Privacy](#), for example, the [HIPAA Privacy Rule](#), [CCPA](#), and [GDPR](#), setting out privacy standards including access and other individual rights, breach notification obligations, and notice and consent requirements
 - [Cybersecurity](#), for example, the [HIPAA Security Rule](#), [FedRAMP](#), and [CMMC](#), establishing binding cybersecurity control requirements
 - [AI](#), for example, [HHS AI Strategic Plan](#) and [EU AI Act](#), establishing a framework for AI governance, classifying AI systems by risk levels, and imposing requirements to ensure safety, transparency, and accountability
 - [Data governance](#), for example, the [EU Data Act](#), seeking to enhance the data economy by making data more accessible and usable, fostering innovation, and ensuring fairness in data sharing among businesses and individuals
 - [Accessibility](#), for example, [Section 504 of the Rehab Act](#) and [Web Content Accessibility Guidelines](#), mandating that any organization receiving federal funding must ensure their websites and apps are accessible to individuals with disabilities
 - [Online Safety](#), for example, the [EU Digital Services Act](#) and [US state and federal online safety requirements](#) establishing protections for children and other vulnerable groups online
 - [Interoperability](#), for example, [21st Century Cures Act](#) and [Interoperable Europe Act](#) establishing technical standards to the interchange of data
-

Trust Standards

Industry



Digital Trust Standards in Health – Industry

Requirements driven by commercial objectives and participation in the marketplace

- **Internal Stakeholders** may identify opportunities specific to their functional operations. For example:
 - Marketing seeking to grow its marketable email list
 - R&D which may want to increase the availability of data usable for research and product development activities
 - Product design imperatives to improve the patient experience
 - **Business Partners** apply significant pressure on organizations to adjust Digital Trust practices to meet their own standards. This may include:
 - Platform providers like Apple and Google who have Digital Trust requirements for apps provided through their app stores
 - Strategic partners who receive information collected by organizations in the first instance, including from devices that they manufacture
 - Institutional customers who want to ensure that organizations are verifiably deploying controls that meet their expectations for suppliers
 - **Patients and Users** are broadly interested in understanding how data about them is processed and control over it. Serving these needs is key to the quality of the patient experience and may require adjustments to our service of data subject rights requests (like access) and improvements to UX design
-

Privacy as an institutional value

Privacy is essential to the exercise of free speech, free thought, and free association. Lack of privacy and confidentiality chills users' choices, thereby suppressing access to ideas. The possibility of surveillance, whether direct or through access to records of speech, research and exploration, undermines a democratic society.



ALA's five standard "Privacy Principles"

- **NOTICE:** There must be no personal data record-keeping systems whose very existence is secret.
- **ACCESS:** There must be a way for a person to find out what information about the person is in a record and how it is used.
- **CHOICE:** There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
- **SECURITY:** There must be a way for a person to correct or amend a record of identifiable information about the person.
- **ENFORCEMENT:** Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Library Trust Standards: How are they informed?

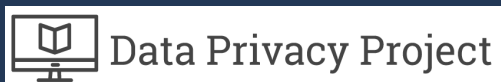
Industry standards and best practices

- Posted privacy policies (in the for-profit world)
- International standards and practices
- NIST (National Institute of Standards and Technology)
- PCI DSS (Payment Card Industry Data Security Standard)
- ISO (International Organization for Standardization)
- NISO (National Information Standards Organization)
 - *"NISO Consensus Principles on Users' Digital Privacy in Library, Publisher, and Software-Provider Systems"* (2015)



Library Trust Standards: How are they informed?

- ALA
 - Privacy “Bill of Rights”
 - Intellectual Freedom Committee (IFC)
 - IFC Privacy Subcommittee
- Library-related organizations focusing on privacy
 - Data Privacy Project (incl. @ Brooklyn Public Library)
 - Virtual Privacy Lab (San Jose Public Library)
 - Library Freedom Project
- Privacy policies in other libraries and non-profit institutions
- Organizations with a focus on privacy-related matters
 - Electronic Frontier Foundation (EFF)
 - Electronic Privacy Information Center (EPIC)
 - American Civil Liberties Union (ACLU)



NYPL's Trust Standards: How is it informed?

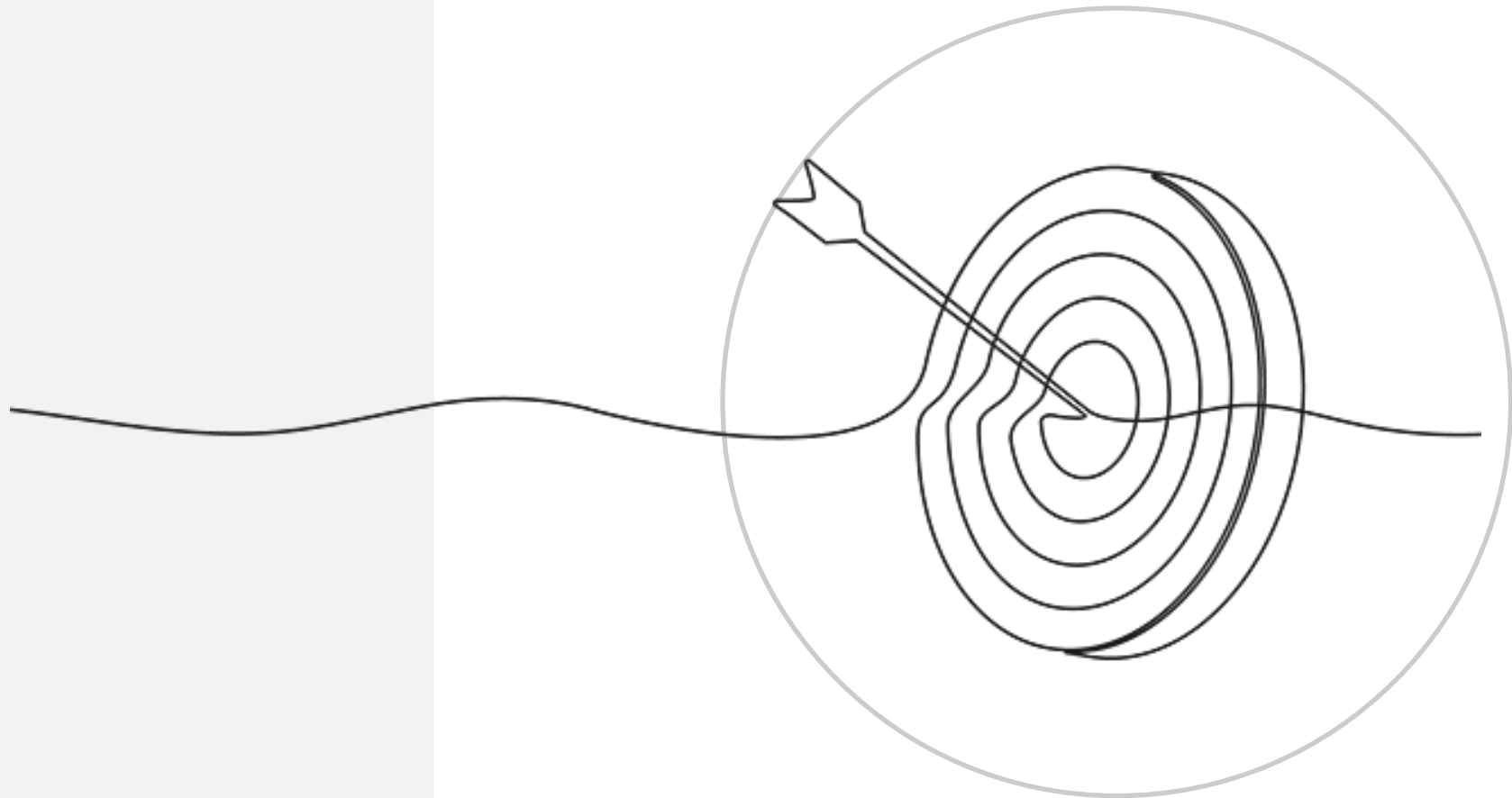
- Legal Dept.
- Board of Trustees
- Chiefs of NYPL divisions
- Privacy Advisory Committee
- Federal and state laws and statutes
- Case law

Trust Standards

Follow the Arrow



Follow the Arrow



Business Enabling Trust

Risks and Benefits



Direct Risks

Potential penalties arising from non-compliance with laws, regulations and standards relating to Digital Trust

01

Penalties and other financial damages.

- Frameworks for fines or private actions are commonplace in privacy, AI, and other digital trust regimes.
- For example, violations of the GDPR can lead to fines of up to 4% of annual global turnover or €20 million (whichever is higher). Class actions may also lead to multi-million-dollar settlements

02

Operational impacts.

- Regulators may impose restrictions on operations, suspend activities related to data, or mandate ongoing oversight and verification.

03

Algorithmic disgorgement.

- Regulators may mandate the deletion of AI models or algorithms that were developed using improperly obtained or processed data.

04

Contractual breach.

- Failures to comply with relevant requirements will often incur penalties associated with contracts, which may include coverage of the above costs for partners and contract termination

Indirect Risks

Potential penalties arising from non-compliance with laws, regulations and standards relating to Digital Trust

01

Reputational damage.

- Non-compliance on digital trust topics can severely damage an organization's reputation.
- Loss of trust from customers, partners, and the public could have long-term impacts on ability to operate in the marketplace, let alone grow.

02

Increased scrutiny.

- Once an organization is found non-compliant, it may face increased scrutiny from regulators and watchdogs in the future.
- This can lead to more frequent audits and higher compliance costs.

03

Distraction.

- Along with penalties directly impacting operations, managing the response to incidents of non-compliance can require significant internal bandwidth and expenditures on outside legal, technical, and communication resources.

Quantifiable Benefits

Using Digital Trust adoption to improve bottom line

01

User adoption.

- Increases to revenue based on enhanced digital marketing capabilities and user adoption.

02

Saving time and money.

- Reductions in resources spent on legal and regulatory analyses and oversight through streamlined workflows and automation.

03

Saving development resources.

- Development and design demand savings through adopting technology and services purpose-built to enable digital trust.

Unquantifiable Benefits

Using Digital Trust adoption to improve bottom line

01

Risk reduction.

- Overall reduction of risk arising from non-compliance/litigation, including avoidance and improved resiliency.

02

Reputational gains.

- Becoming a trusted data steward increases brand awareness and reputation.

03

Data enablement.

- Data enablement for a variety of business use cases, including AI model training.
- This is a key driver of growth and product development.

04

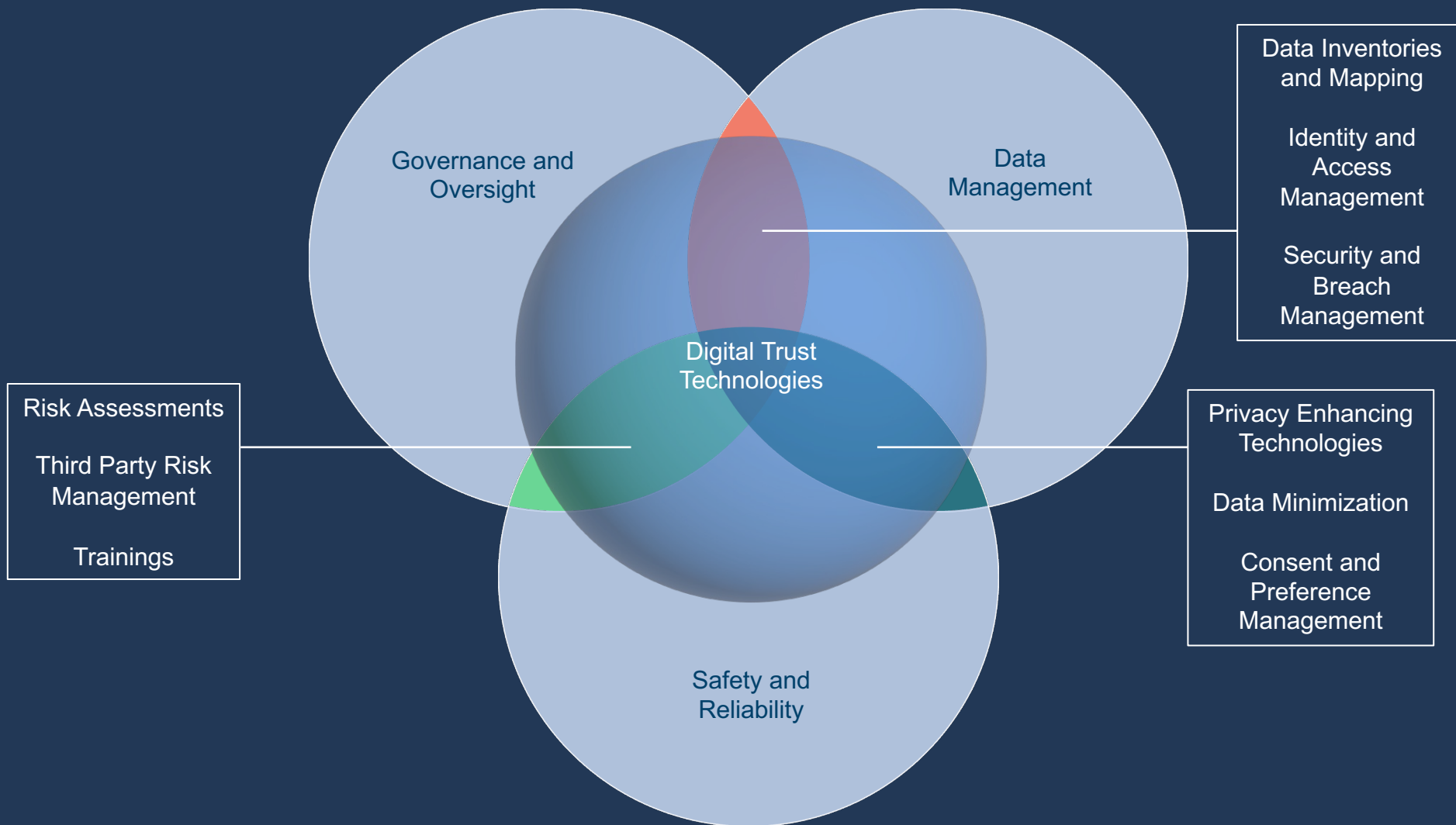
Improved insight.

- Better decision-making through improved understanding and management of data assets.

Business Enabling Trust

Operational Design





Enabling Digital Trust – Administrative Controls

Key governance and operational compliance activities that enable digital trust

- **Risk Assessment and Management**
 - Privacy, security, and AI risk evaluation, management, and monitoring activities for systems, processes, and vendors.
 - **Policy & Training**
 - Privacy and data protection training programs for employees.
 - **Data Incident Management**
 - Processes for detecting, reporting, and responding to data breaches or other reportable data protection incidents.
 - **Governance & Oversight**
 - Data governance frameworks, including accountable and empowered roles, responsibilities, and escalation paths.
 - **Audits & Compliance Reviews**
 - Periodic internal and external audits to ensure adherence to regulatory and internal requirements.
 - **Legal, Legislative, and Regulatory Monitoring**
 - Tracking for changes in laws and regulations to update policies and practices accordingly
-

Challenges to Operationalization

Potential contributors to investment and implementation challenges for Digital Trust

- **Build, Buy or Partner?**

- Although investments are often required by law and can present significant commercial opportunities, their fit within an organization's overall roadmap may not be sufficiently clear.
- Determining whether there are commercially available solutions may impact prioritization.

- **Whose Budget?**

- Costs associated with investments lack clear ownership. For example, Legal is often treated as a “customer”, which can create expectations that Legal fund other functions' implementation costs such as engineering and development.

- **How much?**


- While often cost-saving on relative short timelines, the upfront costs for implementing investments can be steep. many are driven by frequently complex technical and specialized requirements necessitating non-trivial development resources in IT and R&D.

- **Implementation is Complex**

- As implementation tasks are typically split between several functions (most commonly Legal, IT, R&D, Product, and Marketing), planning and coordinating resources presents challenges. This may be compounded by processes within and between these functions that involve large numbers steps and handoffs, creating opportunities for requests to lose context and priority.
-

Digital Trust in the Marketplace

Just a communication tool or part of a commercial strategy

 | **Trust Center** [Security](#) [Privacy](#) [Compliance](#) [More](#)

We're helping organizations comply with the EU AI Act while fostering responsible AI innovation.

[Learn more >](#)

TRUST CENTER

Security and privacy in the age of AI

Microsoft enables trustworthy AI by prioritizing security, privacy, and safety. Learn more about the commitments we've made to ensure your data is safeguarded, our practices are transparent, and your rights are protected.

Trust Center



It's You.

We want you to feel confident sharing your data with us. We understand that the data we hold represents people's lives and our team respects this significant responsibility as we work with your data.

Business Enabling Trust

Technical Design



227%

estimated ROI of adopting automated tools to manage (1) user notice, consent, and preferences and (2) internal privacy compliance workflows with a 7-month payback.

Source: 2024 Forrester Consulting Total Economic Impact™ study commissioned by OneTrust ([link](#))

Enabling Digital Trust – Data Management

Key activities and practical examples of technologies that enable digital trust

- **Permissioning data**

- [Transparency, consent, and preference management](#), to deliver notice and collect, store, and manage user consent and preferences for use, disclosure, and other processing (especially regulated activities like marketing and analytics)

- **Architecting data systems**

- [Tracking tech management](#), to help ensure that cookies and other tracking technologies are appropriately deployed (e.g., web scanning)

- **Altering or generating data**

- [Anonymization, pseudonymization, and obfuscation](#), to help protect data and decrease use restrictions by removing or obscuring certain information (e.g., hashing); this may also include generating synthetic datasets or other derivative information

- **Sharing and controlling data**

- [Data subject rights management](#), to streamline and automate data subject rights requests, like data access and [data transfer and interoperability protocols](#), to make data accessible internally and, as needed, for partnerships

- **Tracking data**

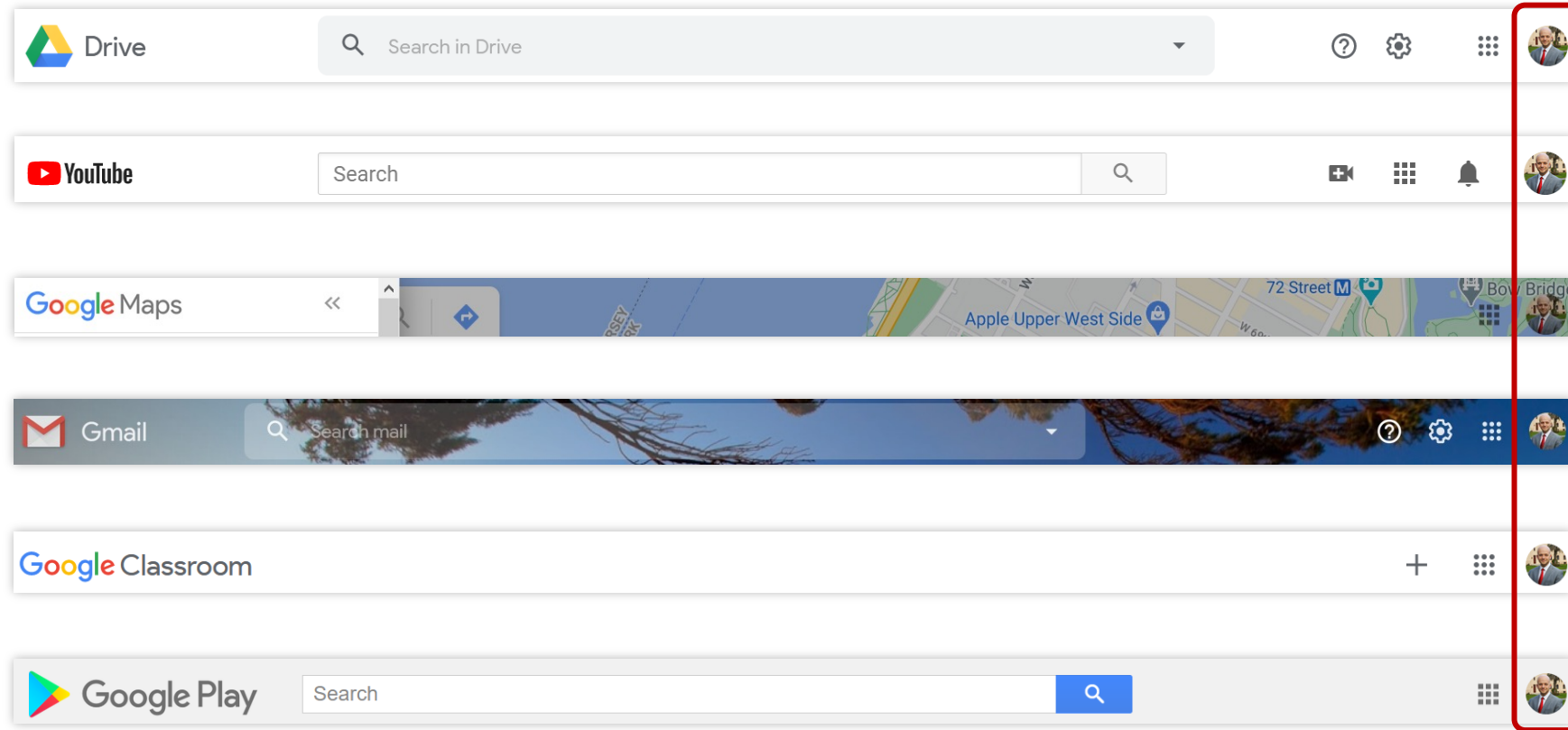
- [Data mapping and inventorying](#), to identify, classify, and map regulated data across systems and applications (e.g., structured data discovery)
-

Digital Trust in the Marketplace

Just a communication tool or part of a commercial strategy

DIFFERENT PLATFORMS

SAME LOG-IN



Digital Trust in the Marketplace

Just a communication tool or part of a commercial strategy


See and manage the data in your Google Account


Your data includes the things you do, like searches, and the things you create, like email.


Need a copy? [Download your data](#)



Popular Google services
















 Gmail
94,313 conversations

 Maps
Home: 635 W 42nd St, New York, NY

 Web & App Activity
ON

Your Google services

[EXPAND ALL](#)

 Account Email: matt.es.coleman@gmail.com	 Alerts 8 alerts	 Analytics 1 account
 Blogger 1 blog	 Calendar 5 calendars	 Chrome Last sync: August 28
 Contacts 151 contacts	 Drive 100+ files	 Gmail 94,313 conversations
 Keep 11 notes	 Maps Home: 635 W 42nd St, New York, NY	 Payments 1 payment profile
 Photos 12,351 photos	 Tasks 9 open tasks	 YouTube 2 playlists

Prioritizing Digital Trust – TOP TEN TAKEAWAYS

1. **Strategy.** Determine your data strategy from the top and align the business deliberately around it
2. **Context.** Understand how law and industry landscape changes impact that strategy
3. **Governance.** Appoint responsible personnel with mandates to implement and govern
4. **Communicate.** Consider internal and external marketing and lobbying strategy to support the strategy
5. **Invest.** Tactically build and partner to develop “technical spine” to facilitate digital trust

Prioritizing Digital Trust – TOP TEN TAKEAWAYS

6. **Consumers First.** Focus on consumer sentiment and protections from the jump
7. **Common Branding.** Consider common branding strategies to enable “first party” data
8. **Permissioning.** Design identity, access, consent and preference flows to enable maximum data use and sharing
9. **Third-Party Management.** Manage third-party risks to know where your data goes and how it’s used
10. **Compliance.** Build a data compliance program to support data enablement

Thank You

