Data Privacy and Security: Reflections on Construction Management Research

NSF Workshop Keynote

By Prof. Carrie Sturts Dossick, Ph.D., P.E.

CONSTRUCTION MANAGEMENT
UNIVERSITY of WASHINGTON
College of Built Environments

CTOP LAB
Communication, Technology and Organizational Practices

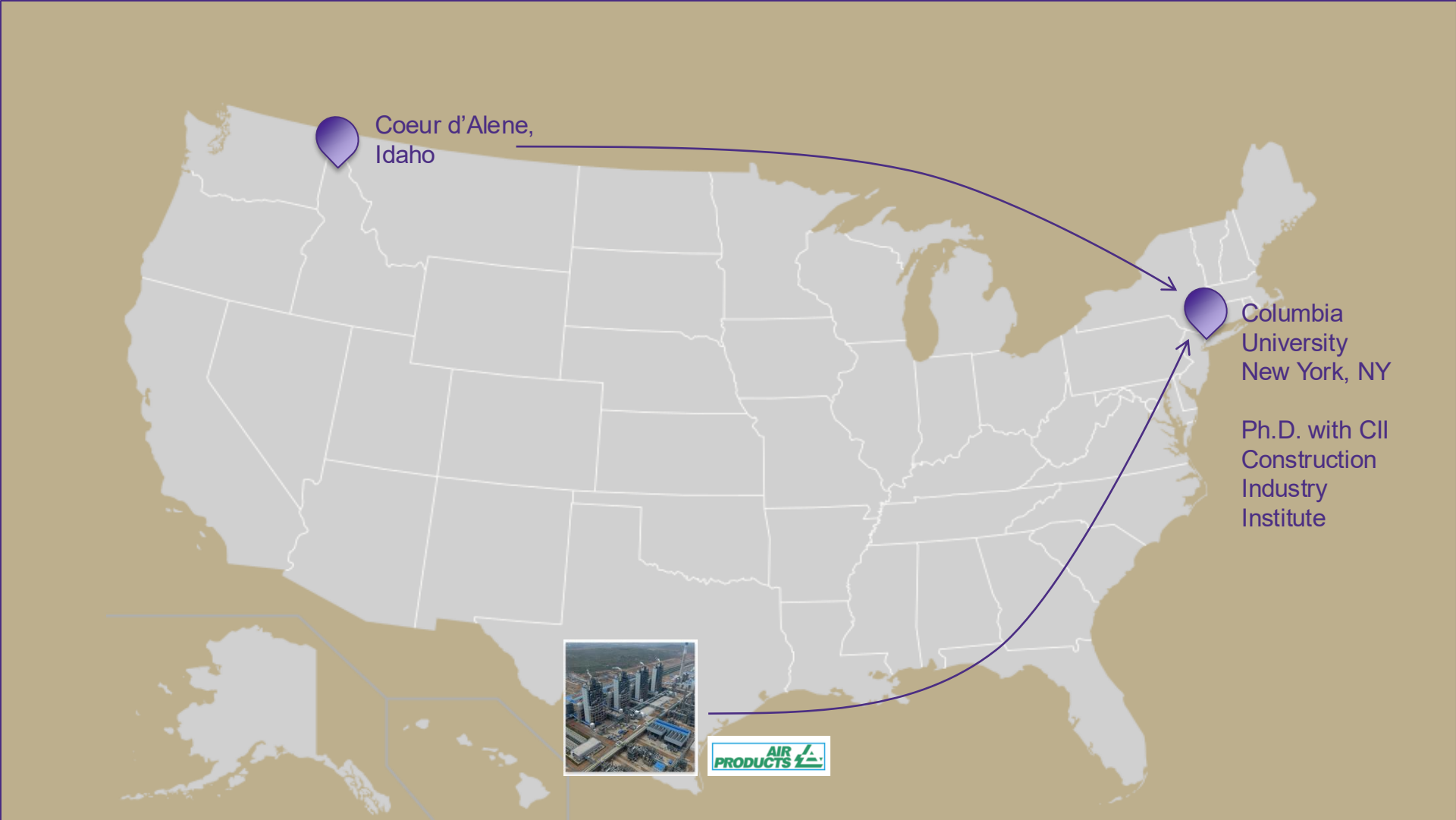
Today's Agenda

> The Promise and Complexity of Industry Partnerships

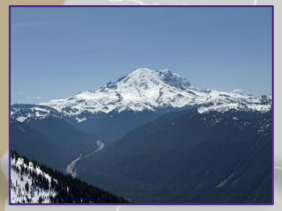
> What IRB Misses: Organizational Data Governance
> Private Companies vs. Public Institutions
> Three Pillars: Corporate/Institutional Risk, IP, Cybersecurity
> Emerging Issues & Best Practices
> What Our Field Still Needs

Coeur d'Alene,
Idaho

Columbia
University
New York, NY


Coeur d'Alene,
Idaho
Columbia
University
New York, NY
Ph.D. with CII
Construction
Industry
Institute
AIR
PRODUCTS

University of Washington Seattle, WA



Coeur d'Alene, Idaho

Columbia University New York, NY

Exponent Failure Analysis Menlo Park, CA

Parsons Corporation Los Angeles, CA

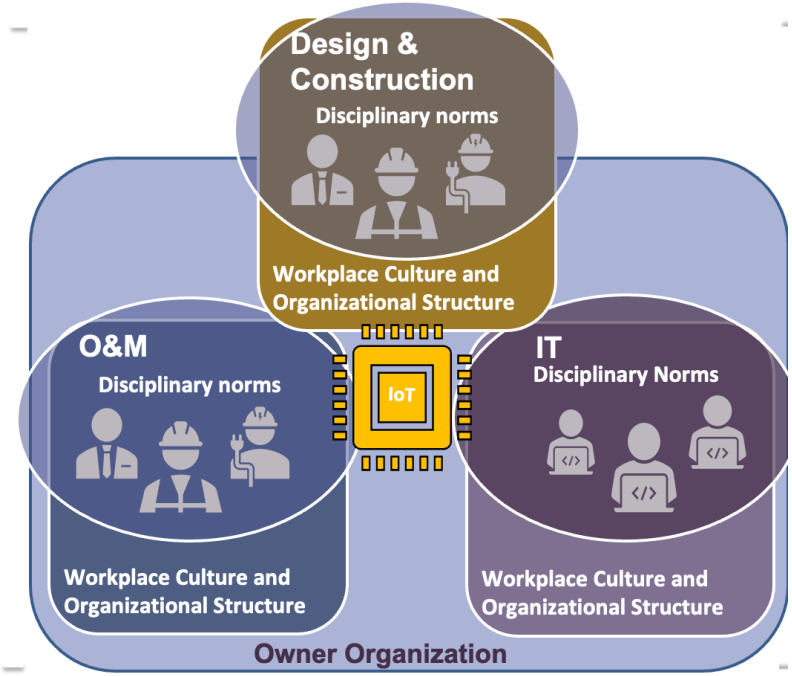
The Promise & Complexity of Industry Partnerships

20+ years of industry-partnered research:
Port of Seattle, Sound Transit, GSA, USACE, DOE/NNSA, Turner, Skanska, Mortenson, WSDOT, Microsoft

Each partnership involves sensitive organizational data: project schedules, BIM models, cost data, IoT sensor streams, cybersecurity configurations

This talk: reflection and a framework for the field

What IRB Misses: Organizational Data Governance



IRB covers: informed consent, anonymization of human subjects, protection of personal data, vulnerable populations

In CEM research, our partners are organizations, not just people. Their data carries IP, competitive risks, and cybersecurity risks IRB was never designed to address.

Key consideration: protecting organizational interests

Inherent Tensions Between Priorities and Contexts

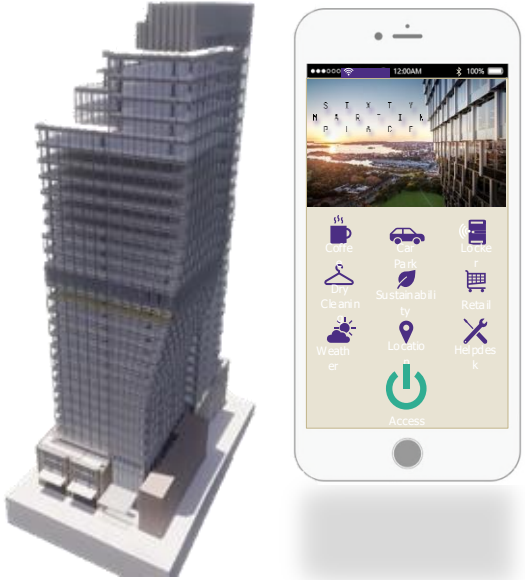
Research

- Publications
- Open source code
- Published datasets

Industry

- Capital Projects
- Market position
- Institutional Mission

Private Companies vs. Public Institutions



Source: 60 Martin Place - Copyright © Investa

Different organizational types carry fundamentally different risk profiles for data governance.

Private partners (Skanska, Turner, Mortenson): Competitive sensitivity, trade secrets, legal liability, and brand protection.

Public partners (Army, SoundTransit, Port of Seattle): Public interest, public perception, privacy and security concerns, national interest

Both require tailored governance frameworks negotiated upfront in research agreements

Pillar 1: Corporate/Institutional Risk

Industry partners face reputational, regulatory, and competitive risks from research participation.

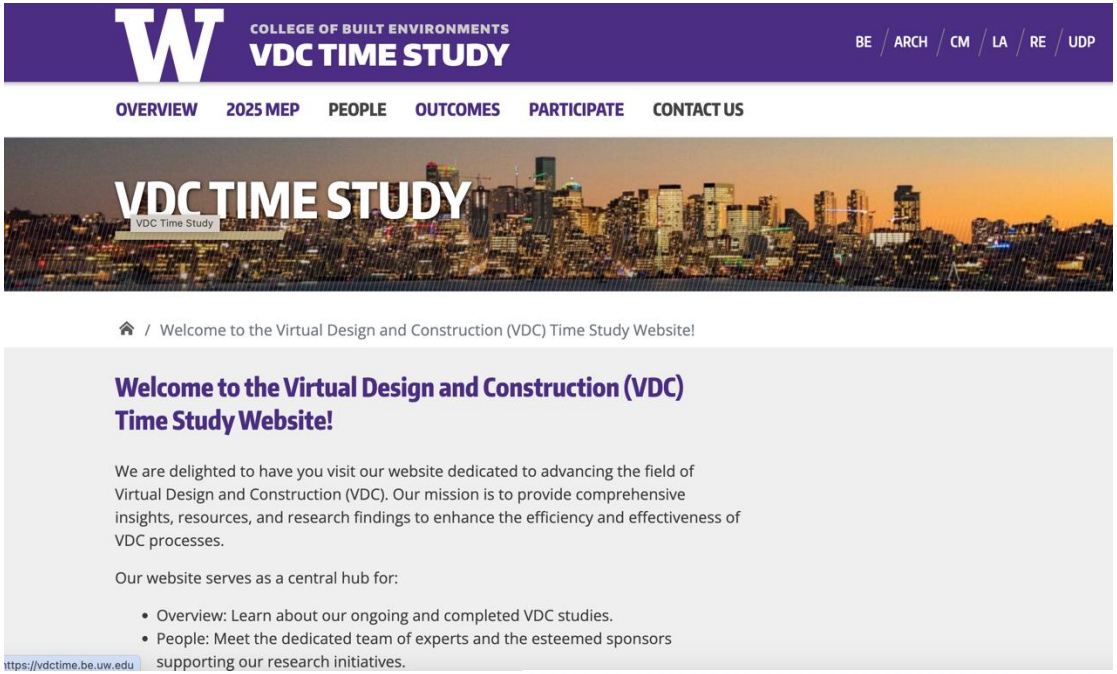
In tension with publication rights and academic freedom.

Reputational risk: Findings may reflect poorly on partner practices, safety performance, or energy outcomes.

Competitive risk: VDC benchmarks, estimating workflows, cost data need confidentiality protocols

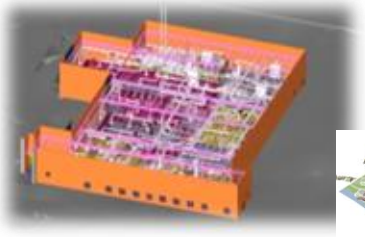
Claims and Disputes: records from active project used in legal actions

Example 1: http://vdctime.be.uw.edu

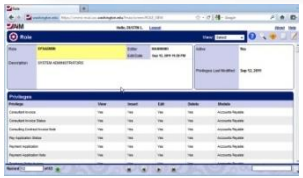


MCAA NECA SMACNA

Pillar 2: Intellectual Property



BIM
GIS



Reports

Data

Who owns the data collected? Who owns the research outputs?

When working with industry products: BIM models, as-built documentation, cost databases, and project schedules.

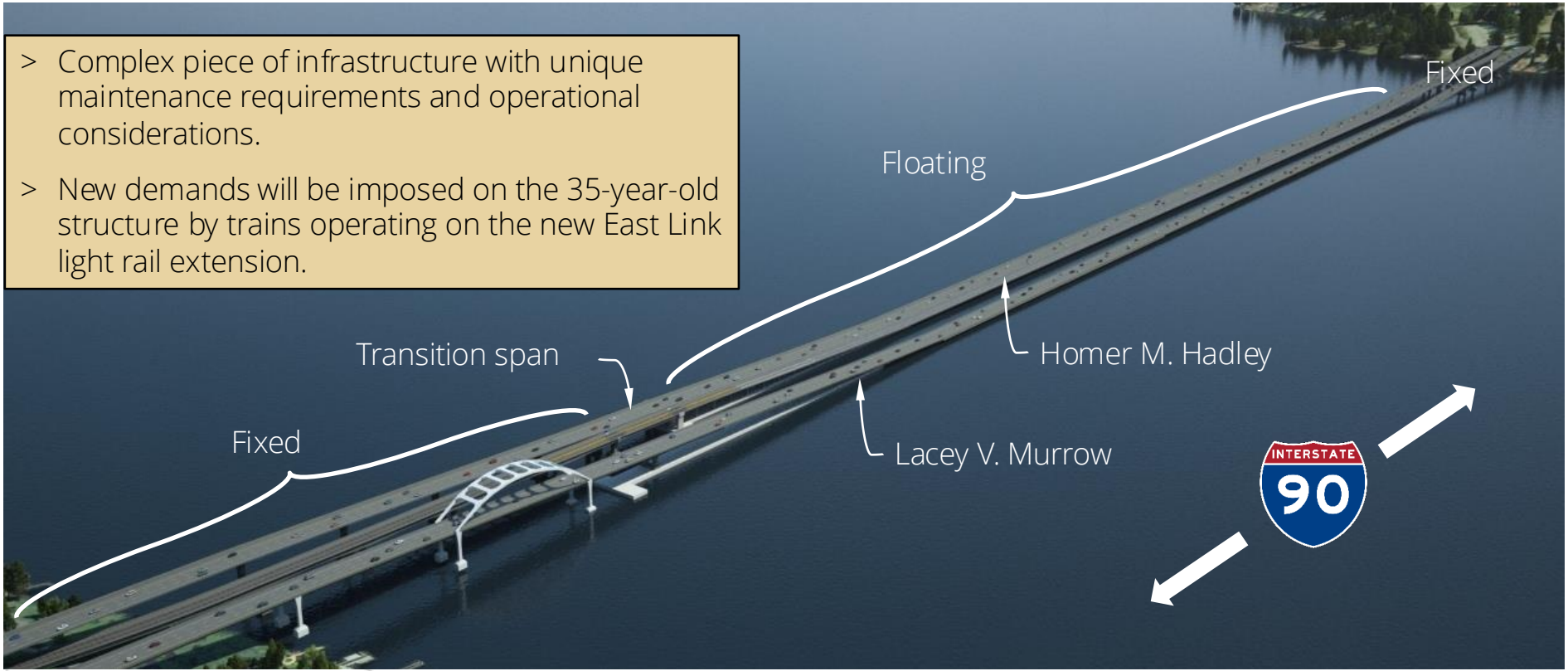
When studying industry practices: estimating, design analysis, digital fabrication workflows

Recommendation:

- **IP ownership clauses prevent disputes and protect the researcher independence**

Example 2: I-90 Digital Twin Proof of Technology Project

- Complex piece of infrastructure with unique maintenance requirements and operational considerations.
- New demands will be imposed on the 35-year-old structure by trains operating on the new East Link light rail extension.



Courtesy: WSP USA

Innovation and Partnerships

WSDOT

CHALLENGE SEATTLE

Bentley®

Microsoft Azure

T-Mobile

SIERRA WIRELESS IS NOW SEMTECH

wsp

COMPASS

CIVIL & ENVIRONMENTAL ENGINEERING
UNIVERSITY of WASHINGTON
College of Engineering

eScience Institute
ADVANCING DATA-INTENSIVE DISCOVERY IN ALL FIELDS

COLLEGE OF BUILT ENVIRONMENTS
UNIVERSITY of WASHINGTON

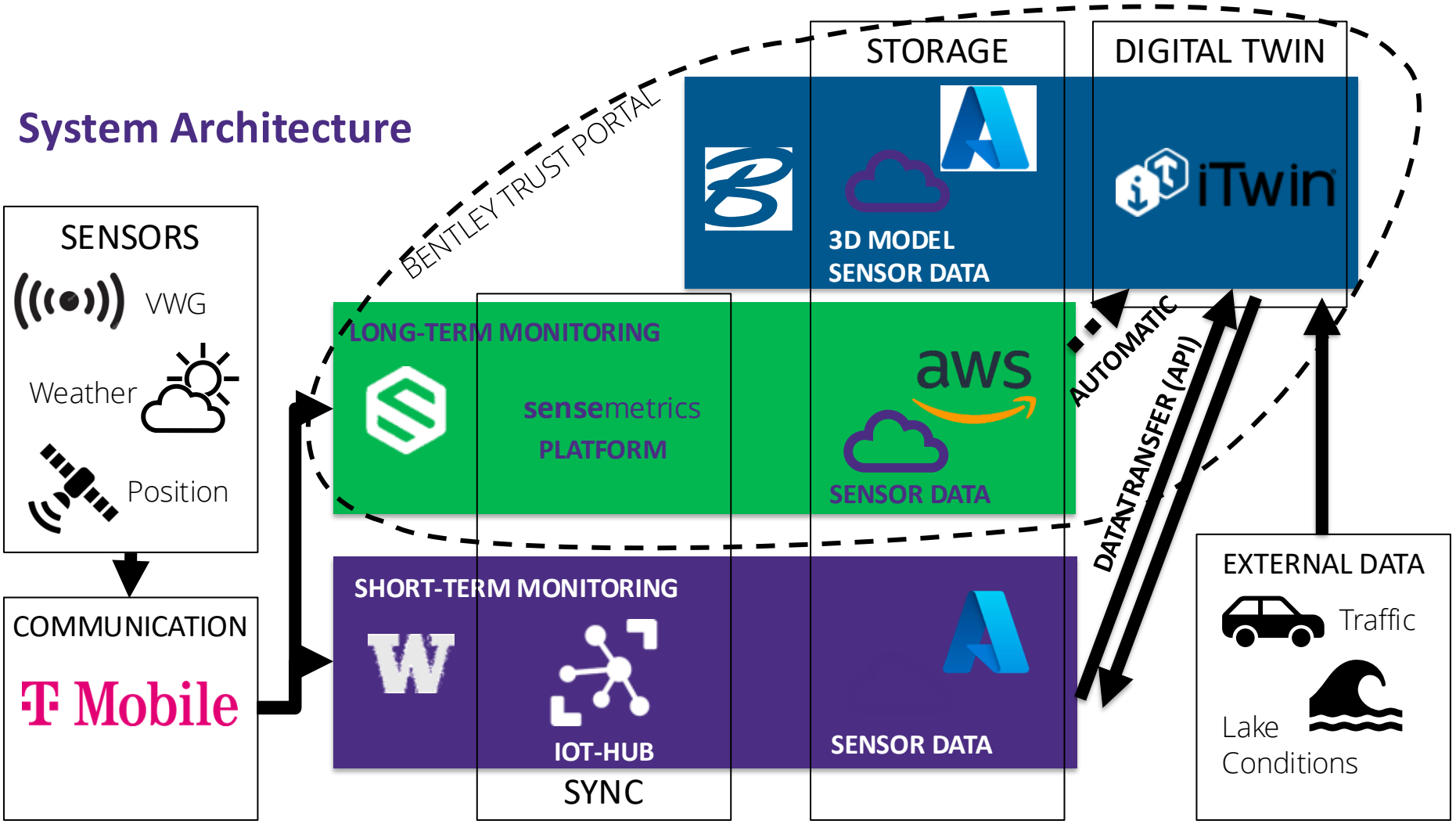
U.S. Department of Transportation
Federal Highway Administration

ABC UTC IBT

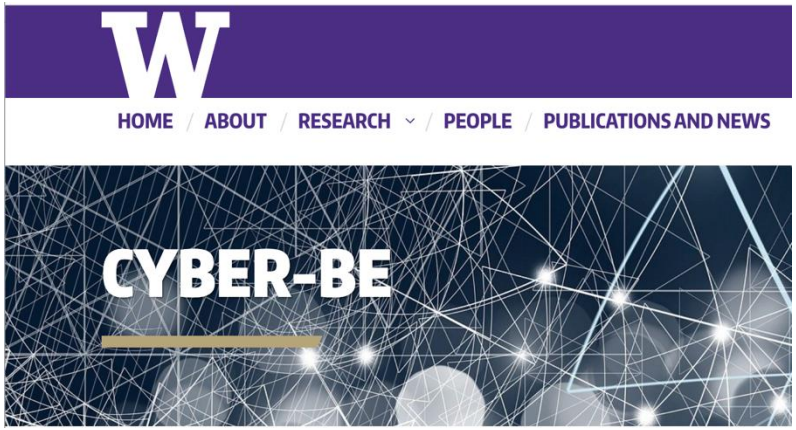
MOBILITY INNOVATION CENTER
at the UNIVERSITY of WASHINGTON

STIC
State Transportation Innovation Councils

System Architecture



Pillar 2: Cybersecurity



NSF SaTC: http://cyber.be.uw.edu

IoT white paper series: policy landscape, risk, and data privacy for the built environment

Connected buildings, smart sensors, and digital twins create new attack surfaces — and new research responsibilities.

NSF SaTC project (#1932769): IoT, smart buildings, and the OT/IT/construction time orientation mismatch.

Key finding: cybersecurity is an organizational problem, not just a technical one.

Recommendations:

- Develop cybersecurity plans for data collection and management
- Coordinate with industry partners policies

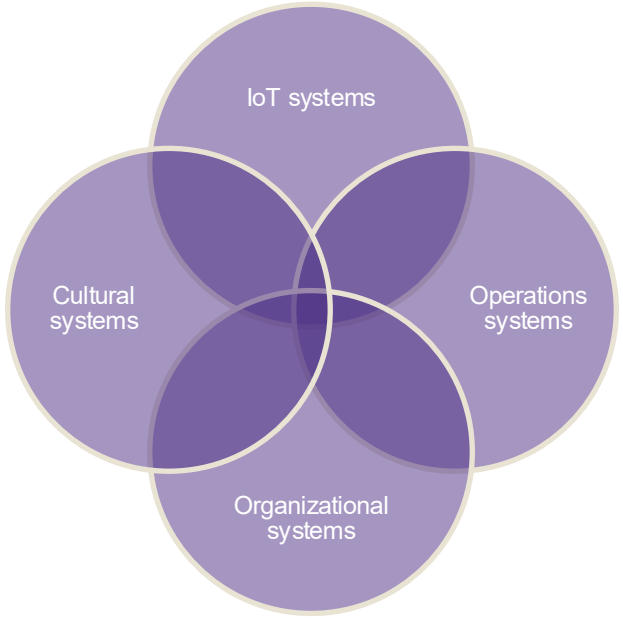
Example 3: IoT Risk is real

https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems

https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/?sh=7faee20c1a09

Example 4: 2024 Port of Seattle

Lack of data governance policies



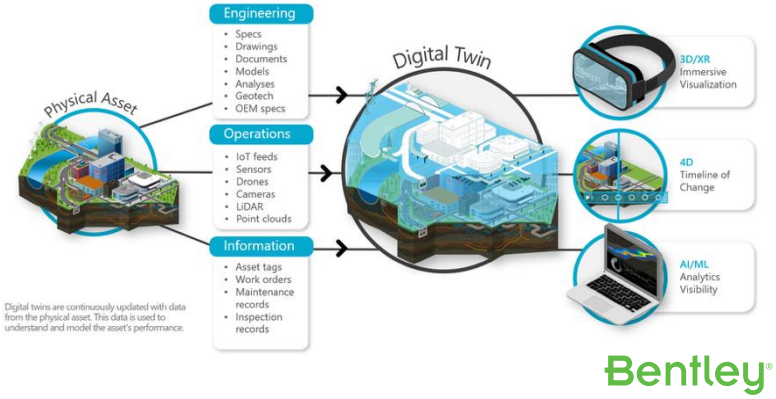
From NSF SaTC project: cybersecurity is treated as IT's problem, not the whole organization's.

OT, IT, and construction staff operate on different time horizons — creating governance gaps.

Most organizations lack formal data governance policies for research partnerships. Researchers often discover sensitive data mid-project — not at the start.

Gap: No standard framework exists for data governance in CEM industry-partnered research

Emerging Issues in Data Governance



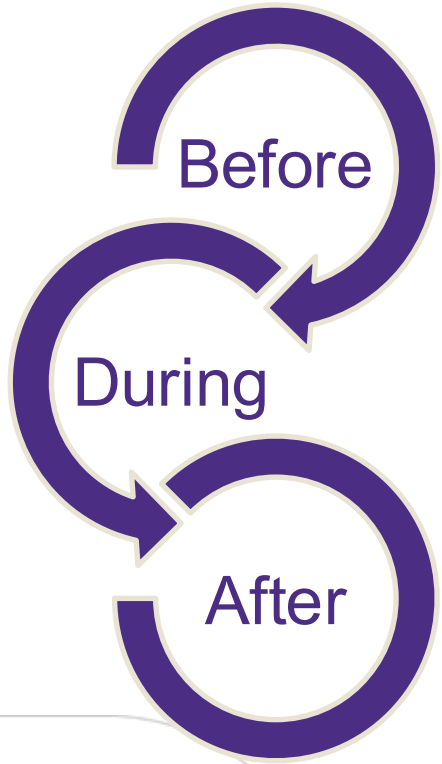
AI and ML on proprietary project data

- **Who owns insights derived from partner data?**
- **Can research outputs be published without revealing trade secrets?**

Digital twin data ownership

- **Long-term stewardship across project lifecycle**
- **Ownership changes**
- **Multi-partner federated environments**

Best Practices: A Framework for Researchers



Negotiate IP ownership, publication rights, and embargo periods. Clarify cybersecurity disclosure protocols and data handling requirements upfront in the research agreement.

Apply data minimization — collect only what you need. Anonymize organizational identifiers. Use secure storage and access controls proportional to data sensitivity.

Partner review before publication; define data retention and destruction policies

What Our Field Still Needs

Standardized data governance templates for CEM industry research partnerships — modeled on what legal and clinical research communities already have

Coordination with University research governance and management (Office of Sponsored Programs)

Doctoral training that includes IP, cybersecurity, and corporate risk literacy — not just IRB. Community-shared case studies of governance agreements (de-identified).

This workshop is a starting point

Closing Reflections

Takeaways

- Data governance in CEM goes beyond IRB
- We must negotiate protocols upfront
  - Corporate/Institutional Risk,
  - IP, and
  - Cybersecurity

Open Questions

- How do we build community norms for sensitive industry data?
- What governance tools would most help research?

cdossick@uw.edu | cerc.be.uw.edu

CONSTRUCTION MANAGEMENT
UNIVERSITY of WASHINGTON
College of Built Environments

CTOP LAB
Communication, Technology and Organizational Practices