

Market Verticals: Current and Future Challenges


Government

Peter Watkins

Province of British Columbia

Strong Authentication and Identity Information

Understanding current and future problems from a government perspective



Context: Many Levels of Government

Province of British Columbia: 4.8 million residents (small)

Federal Government of Canada

Provincial **Government of British Columbia (BCGov)**

Municipal Vancouver, Victoria, ...

Indigenous Nisga'a Lisims Government, Esquimalt First Nations, ...

Broader Public Sector Regional Health Authorities, WorkSafeBC, Technical Safety BC
ICBC (DMV and Insurance), BC Ferries, ...

Me!



- Health, Education, Transportation*, Natural Resources, Justice, Social, Economic Development, Employment...
- Vital events for people -- birth and death registrations, name changes
- Legal events for organizations -- registration and de-registration etc.
- Professional designations -- regulating bodies, Doctors, Lawyers, Engineers, Forresters, Architects, Accountants, ...
- Licenses and permits -- driving (personal, commercial), harvesting, building, gasfitting, welding...
- Important Assets - Land Title, Liens, etc

We provide the foundational identity information for our society and economy.

Current (legacy?):

- 30,000 Employees: userid/password
- 1 million accounts for Individual or Business users: BCeID userid/password
- Active directory, enterprise web single sign on paradigm

New:

- BC Services Card as Provincial Identity Information Program
- Fully subscribed* 4.3 million registered people
- Gov mobile app and gov issued EMV chip card - DL or Services Card
- Registered name, date of birth, address as verified identity information
- Careful privacy design, pairwise identifier scheme, conservative roll-out

Newest:

- Verifiable Organizations Network: Hyperledger Indy and friends: vonx.io
- orgbook.gov.bc.ca : Corporate registrations ---> licences, permits, and more

Perspectives on Strong Authentication

Damned if we (gov) don't do it

- Corporate controlled or other government controlled
- No effective recourse or accountability
- Challenges with recovery when lost - if they never really knew you - how can they fix it?
- Authn services can be a party to every transaction
- UX and public perception

Damned if you do it - self provisioned

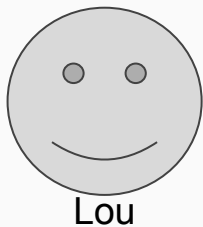
- One does not simply "self-provision" (U2F, SmartPhone Apps for TOTP) - UX
- Challenges with recovery when lost -- who knows you that can help you?
- We still need to bind your authentication to our records related to you

Damned if we (gov) do it

- Protection / defense obligations are off-the-scale
- Low usage rates -- gov specific secrets forgotten
- Authn services can be party to every transaction
- If we verified your identity at our counter then we do know you and can help recover lost / stolen -- but is that a bug or a feature?
- There are always users outside our borders -- we can't bring everyone to a registration counter

And lastly - lending problem when tied to benefits.

Perspectives on Digital Identity Information



Hi there! It's us here at the gov.
Thanks for authenticating now we remember you. Hi Lou!
Do you want to authorize Digital-Service.com to call us right now and get your name and date of birth?

Approve

Cancel

- This is a problem even when it's Digital-Service.gov
- The api's know who's calling/called. Event data is not fun to manage when personal information is involved
- Calling AnyCompany.com everytime is not much better
- Scaling this into digital economy will be a problem
- Need to issue to Lou and enable Lou to share government issued identity information without calling back to the gov every time

Digital-Service.com

Request +
Authorization

Response +
Data

api.somegov/idim/namedob
or a callback (same effect)

guid1, Bob, May 15, 1972
guid2, Lou, Dec 9, 1989
guid3, Sam, Jun 21, 1955

Perspectives on Digital Services, Digital Government, Digital Economy

**Awesome
Digital Services
That Work Great**

Sweet!

Not possible without
strong authentication and
digital identity information
-- standards and interop --

Face-to-face
Papers
Fax

meh

grrrr

Things you can do that
are not very important
or valuable

**Things you need
to do that are
very important
or valuable**

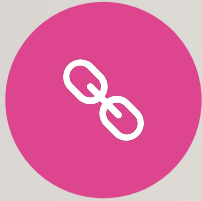
Healthcare

(see [PDF](#))

Supply Chain

Jim Masloski

W3C WORKSHOP ON STRONG AUTHENTICATION & IDENTITY



SUPPLY CHAIN
(IDENTITY/VERIFIABLE CLAIMS)



**INVOLVEMENT OF
ACTORS**
PARTIES IN TRANSACTIONS



**PARTICIPATION AT
THE PARTY LEVEL**



CODIFYING
THE IDENTITIES OF PARTIES AND
THE ABILITY TO MAINTAIN
CONFIDENTIALITY

CONSIDERATIONS ON VERIFIABLE CREDENTIALS

- Availability to the information
- Cross platform application
- Number of parties needing access to different pieces of the data
- Ability to authenticate the information by responsible parties
- Out of the box thinking on how to build this out in the supply chain industry
- Take into consideration the legal requirements as they currently stand in the supply chain arena



CUSTOMS
D I R E C T
SUPPLY CHAIN & LOGISTICS

ISF Header & Line Details

Page 1 of 1

JOB NUMBER		ISF0000002	
CUSTOMS REF		8QV-48790364085	
CUSTOMS STATUS		CLEAR ISF ADD	
DATE		15-Nov-2018	
IMPORTER BF ANALYTICAL INC 7600 43RD AVE OMAHA NC 68223 UNITED STATES REG: 52-112345000		MAIN SHIP-TO PARTY JOHN DOE INC 6500 3RD ST SEATTLE WA 67423 UNITED STATES	
SELLING PARTY SHENZHEN BESTOM LIGHT LIMITED NO SONGGANG TOWN 22 DONGFANG ROAD BAO'AN SHENZHEN 51800 CHINA		BUYING PARTY JANE DOE INC 500 4RD ST NEW ORLEANS LA 43456 UNITED STATES EIN: 71-122332000	
SCHEDULED CONTAINER STUFFING LOCATION SHENZHEN LUCKY LOGISTICS LTD SOUTH DONGMEN RD 9F NORTH WING WINJINDU CUSTOMS MANSION SOUTH SHENZHEN 518002 CHINA		CONSOLIDATOR SHENZHEN PONY LOGISTICS LTD NORTH AVENGER RD 9F NORTH WING WINJINDU CUSTOMS MANSION SOUTH SHENZHEN 518002 CHINA	
FIRST ACCEPTED DATE 15-Nov-2018	LAST ACCEPTED DATE 15-Nov-2018	SCAC OOLU	OWNER REFERENCE LLLLCC88B13010
US CBP ENTRY NUMBER	CONSIGNEE ID EIN:41-199899000	ISF BOND HOLDER 41-199899000	
BOND ACTIVITY CODE	BOND TYPE CONTINUOUS BOND	SURETY CODE	BOND REFERENCE NUMBER
EXTRA ORGANIZATIONS			
MANUFACTURER SHENZHEN LIMITED NO SONGGANG TOWN BALLY ROAD SHENZHEN 5180 CHINA			
BILL OF LADING BM: ENXCCC8B13010 (STATUS: S2 - ISF bill is NOT on file in AMS immediately after filing the ISF.) ME: OOLU2611817032			
TARIFF 8541402000	ORIGIN CN	MANUFACTURER SHENZHEN LIMITED	PRODUCT CODE

Legal

Scott David @ScottLDavid

Director of Policy

Center for Information Assurance and Cybersecurity

University of Washington - Applied Physics

Laboratory

Law and DIDs

S.O.D.D.I.* in Seattle

Presentation to W3C – Strong Authentication and Identity Workshop

By Scott L. David

University of Washington – Applied Physics Laboratory
Information Risk Research Initiative

December 10, 2018

*SODDI – Is a criminal defense of Mistaken identity: “Some other dude did it”

DID Law Fork - Mild vs. Wild Paths

- Two faces of DID legal setting
 - Mild or *Wild*



Mild DID Law Path



Mild DID Law Challenge/Opportunity

- **Practice = Compliance**
 - Navigate existing (anachronistic) laws, rules and contracts in DID
- **Authority = Past as Precedent (Kojève)**
 - Existing law and legal paradigms/institutions
 - Varies among national jurisdictions
 - Many artifacts of appropriations of capitalism and centralizations of nation state
 - Focus on traditional embodiments of value
 - “Property” concepts (IP, data “ownership,” etc.)
 - Hierarchical governance/liability in organizations based on “causation”
- **Value = cost savings of de-risking**
 - Identity is emerging “cost center” for organization
 - Jurisdictional arbitrage-venue shopping
 - “Zero-sum game” gestalt
- **Identity = locus of (duty and liability) and (rights and value)**
- **Today’s duties are derived from yesterday’s problems**
 - Analogies in property law
 - GDPR from 1970s era FIPPs

Wild DID Law



"...and by tomorrow, I'll need a list of specific unknown risks that we'll encounter with this project."

Wild DID Law Challenge

- Secondary effects of Moore's law (etc.) yielded downstream **exponential increase in interaction volumes** and densities
- **Interactions breed risk**
- **Risk is increasing exponentially**
- Existing laws/institutions are not built to de-risk these new interaction phase spaces
 - Distributed flows blind hierarchical organizations
- Yesterday's Institutional (and individual) existential narratives dissipate
- Challenge/Opportunity is to “re-intermediate” interactions with new DID-based structures and narratives

Wild DID Law Opportunity

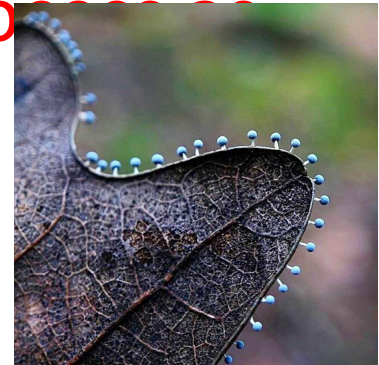
- **Practice = Innovation**
 - Create new containers and pathways for intangible value flows
- **Authority = Future Opportunities (Kojève)**
 - New “unmapped” complex shared risk space
 - Bridge from old solutions to new solutions
 - Old laws to new contracts
 - Old institutions to distributed organizations
 - Bridge as capitalism and nation state cede power/meaning to distributed structures
 - Focus on newly available measurements to establish value
 - Focus on measuring relationship (metrics for edges, not nodes)
 - Focus on value extraction when data is converted into information – Meaning integrity
- **Value = profit center of leveraging relationships (and de-risking)**
 - Efficiencies of avoiding avoidable harms
 - Identity as profit center for organization
 - Contracts to release legal jurisdictional arbitrage
 - “Non-Zero-sum game” gestalt in new complex interaction spaces
- **Identity = embodiment of relationship**
 - Information creates us, not vice versa
- **Duties are derived from projections of tomorrow’s opportunities**

Wild DID Law – Identities are Key

- Identities (of people, entities and things) are the key in distributed systems.
- Each has multiple simultaneous identities (all relationship based)
- Why did “identity” get distributed?
 - Paul Baran diagram (shown later) shows dissipated institutional power
 - Much “identity” is based on relationships with institutions.
- With DIDs, distributed power/institutional structures
 - Not a lot of precedent
 - Not like co-ops – not hierarchical
 - Need new institutional information and risk sharing structures
 - Biological systems yield helpful models
- Resilient distributed structures grow organically
 - Self-assembly among multiple similarly situated stakeholders. (COIs)
 - Recognize that not starting from entirely clean slate
 - Appropriations of late capitalism will continue to operate (In our souls)
 - If aware of this, can design to harness that “energy of mutual appropriation”

Risks Create Organisms and Organizations

- What are current and emerging DID practices?
- What are processes to create feedback loops to refine and develop those practices?
- “Rule of law is as much about procedure as substance”
 - Due process (5th and 14th amend).
 - Substantive
 - Procedural



4 Step Ladder of Institutional Construction

- Processes of institutional construction/law are built from practices
 - Practices
 - Adopt as rule (legislative/contract process)
 - To get
 - Best Practices
 - Apply enforcement (judicial/enforcement process)
 - To get
 - Standards
 - Include operations (executive/operating process)
 - To get

Institutions

How harvest/create practices for socio-technical DID systems?

- **Tools and Rules**

- Technology Tools
- Legal Rules

- For “Tools” measure performance of tech against specifications

- Process is Technical Standard setting
 - Output is specifications (and IP DMZ)

- For “Rules” measure performance of people and institutions against rules, laws, norms, etc.

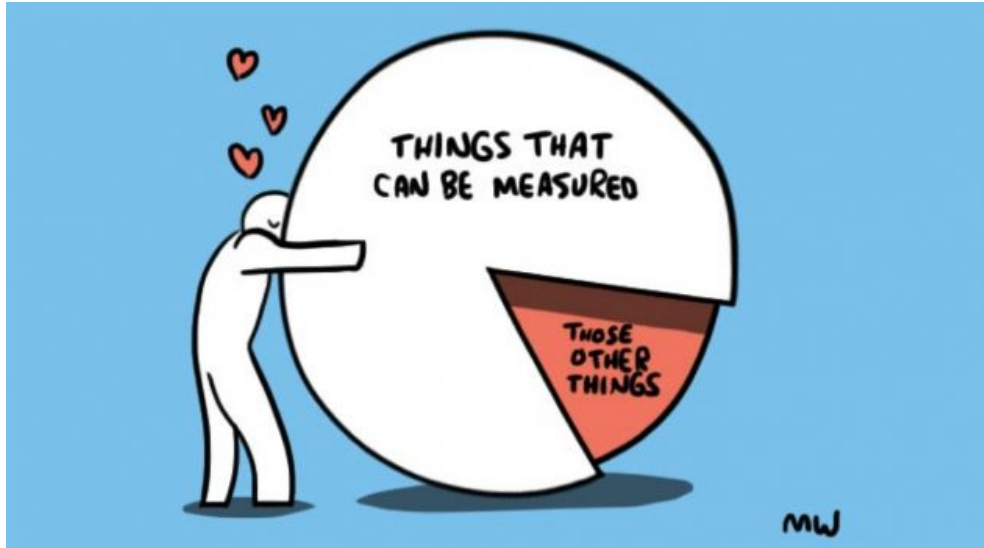
- Process is creating public and private enforceable duties
 - Legislative processes (and APA for regulations)

What Measurements Needed for DID Tools and Rules Development?

- What risks and what performance metrics are relevant for reliable DID systems?
 - Data?
 - Information?
 - Identity?
 - Other?
- You can't protect it if you don't know (or agree) what "IT" is
- We measure risk into existence
 - The threat is present in the system
 - Our measurement/observation allows us to perceive and mitigate risk
 - Carcinogens – capacity to mutate is already present in system
 - All financial collapses in US and UK since 1800 – Seeds of all financial collapse are sown in response to prior crisis
 - All IP – Create property narrative to enable accumulation (retard dissipation)

So, what specifically should we measure to reduce emerging DID interaction risks?

(recalling that “what gets measured gets done”)



DID Stakeholders need reliable and shared *qualitative* metrics to reduce risk

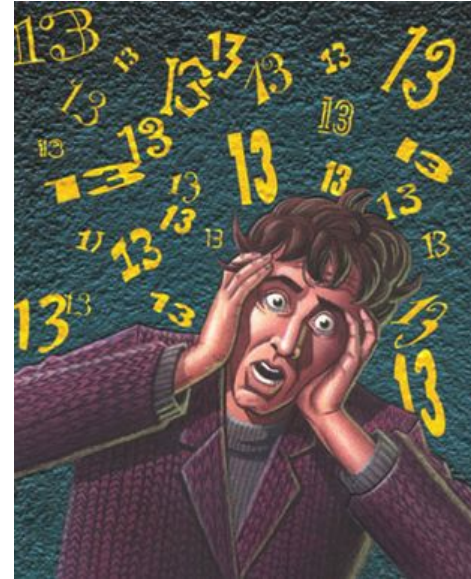


Sic Hunt Dracones



Taming the DID Wild Law Path

- Risks compel de-risking practices
 - What do different sorts of emerging threats and vulnerabilities suggest about future DID practices?
- Invite DID solutions for 13 information risk trends



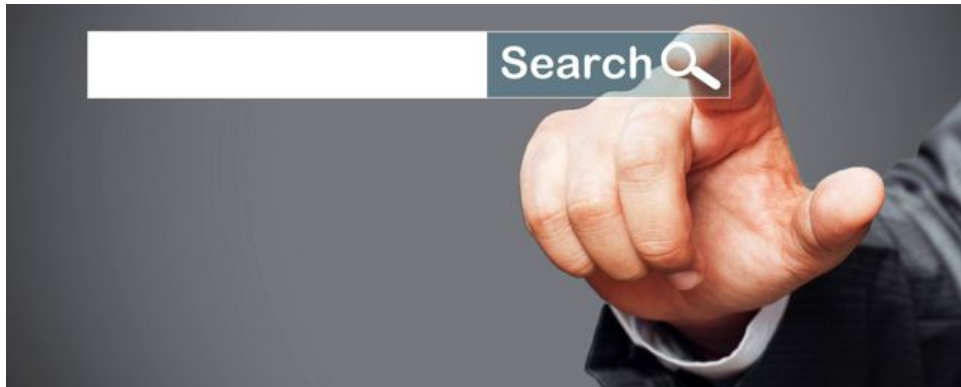
Global Identity/Information Risk Trends

- 13 global risk trends include:
 - **Secrecy is Dead** (but privacy and security are not)
 - **Distributed Information Architecture** (blinds hierarchical organizations)
 - **Complexity** (is its own “sovereignty”)
 - **Socio-Technical Systems** (force non-technical variables into system design)
 - **Information Democratization** (collapses scale & alters security paradigms)
 - **Data Technology is Dual-Use** (it can be used for bad or good)
 - **People are “Data Producers”** (without institutional support)
 - **Big Data Insights Invert** (and Re-Invent?) **Critical Analysis**
 - **“Synthetic Intelligence”** (is a Counterforce to AI)
 - **The Internet Is Not a Public Park** (it is privately operated commercial space)
 - **Data is Not Information**
 - **Power Laws In Bureaucracies Make Security-By-Secrec**
 - **AAA Risks Threaten Information Systems**



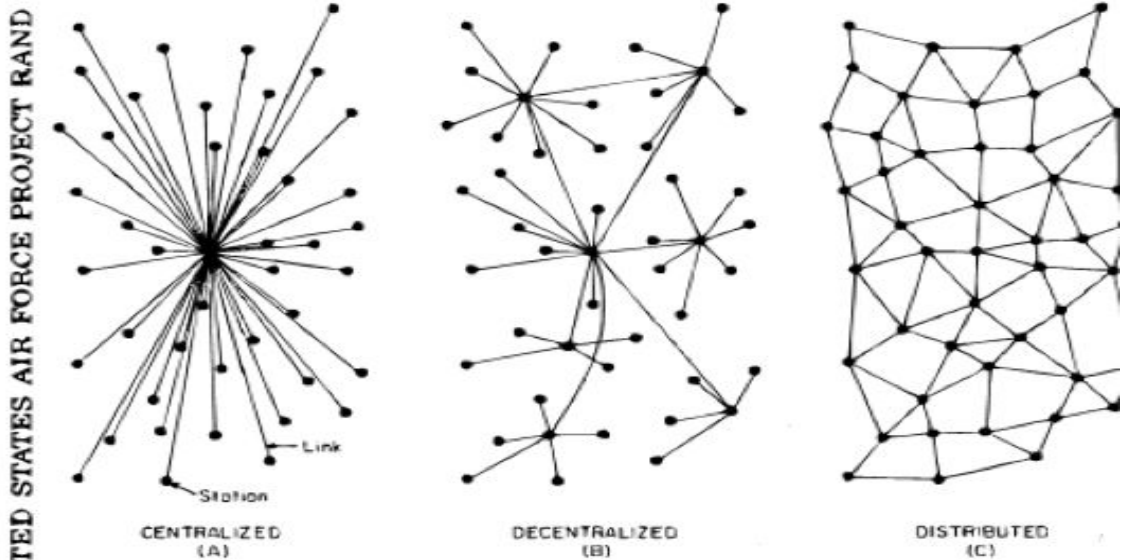
Death of Secrecy (the insight/intrusion “slider”)

- Secrecy died from vast system technical interoperability and collective quest for insight
 - *Insight* of observer is *intrusion* to observed



Distributed Information Architectures

Render hierarchies blind



UNITED STATES AIR FORCE PROJECT RAND

FIG. 1 - Centralized, Decentralized and Distributed Networks

The Sovereignty of Complexity

Statistical outliers can be artifacts of misapplied Gaussian distribution models



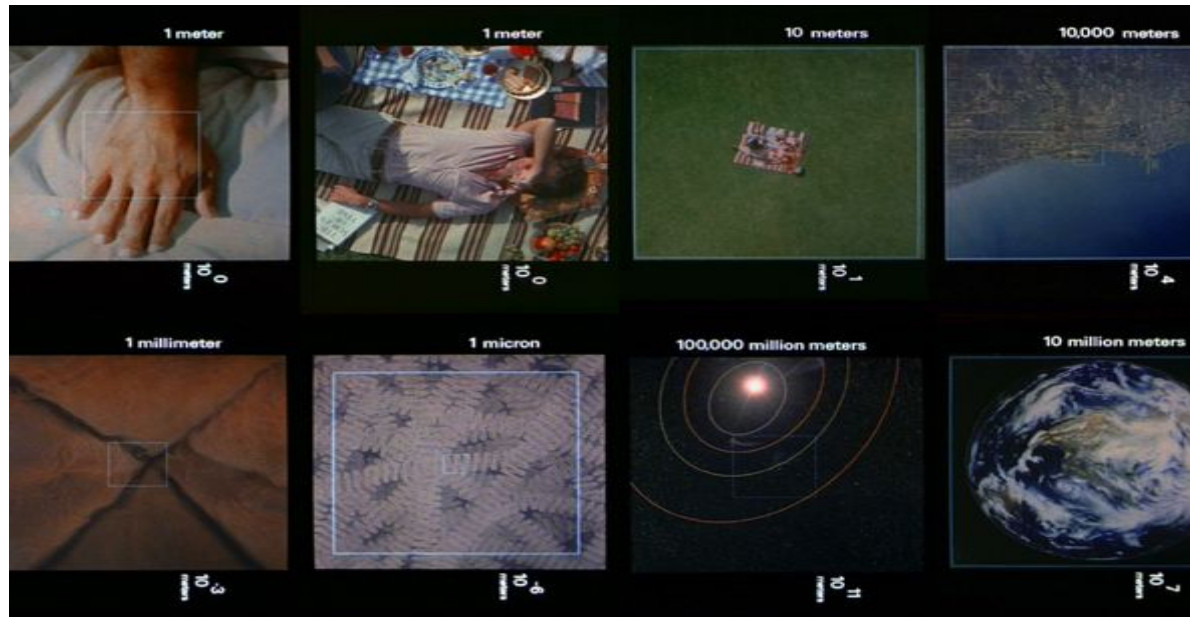
Socio-Technical Systems -

force non-technical variables into security design



Information Democratization Collapses Scale

Invites consideration of scale-independent policies for fractal structures



Data Technology is “dual use”

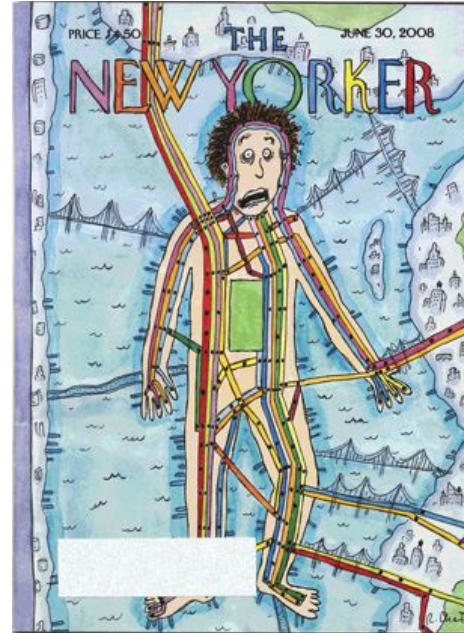
It can do harm or good

(Like Nitrogen-Based Fertilizer)



People are Data “Producers”

Without Institutional Support



Big Data Insights Invert (and Re-Invent?) Critical Analysis

THE FAMILY CIRCUS



8-5

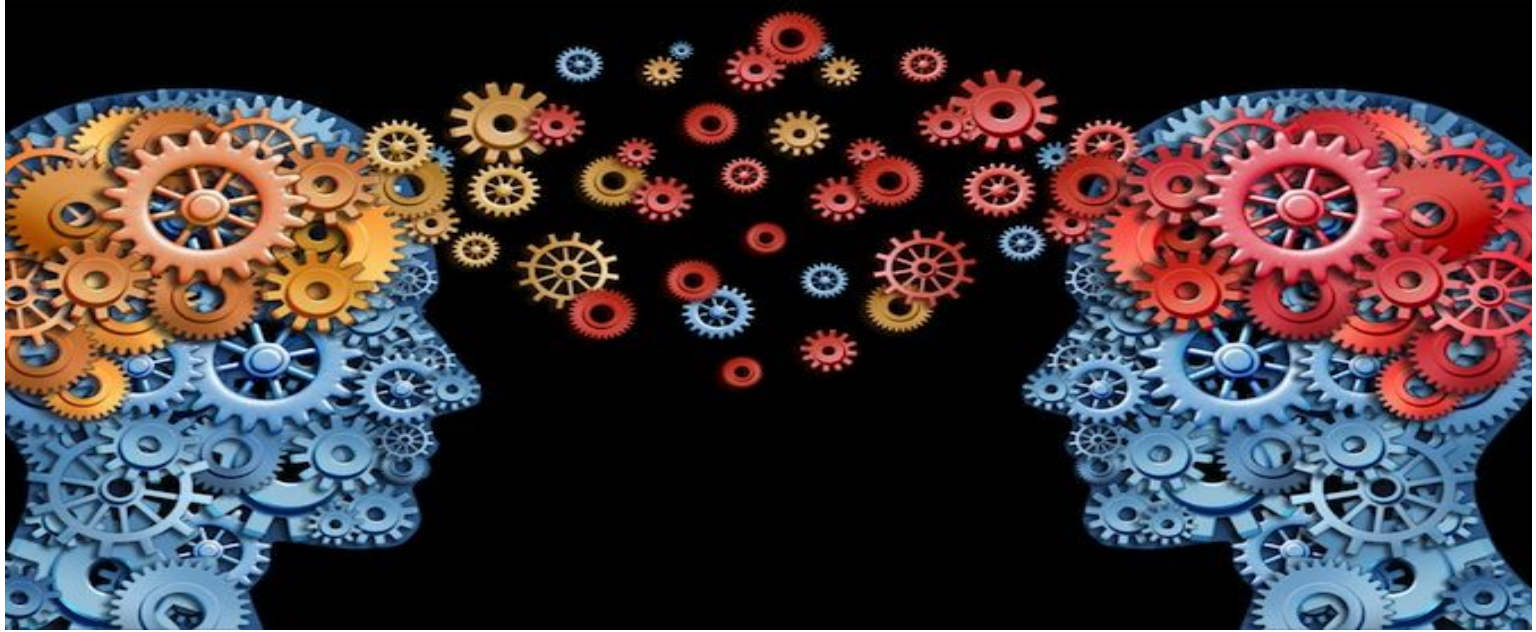
© 1988 by Disney, Inc.
and Fox Control Systems, Inc.

[Handwritten signature]

"I wish they didn't turn on that seatbelt sign so much! Every time they do, it gets bumpy."

Synthetic Intelligence

Is a counterforce to the existential anxiety caused by AI



The Internet is Not a Public Park

It is a privately-operated commercial space



“Data” is Not “Information”

Many system architecture problems dissipate when the distinction is applied



Ceci n'est pas une pipe.

Magritte

Power Laws In Bureaucracies Raise Secrecy/Reliability Costs

As the cell gets larger...

...the **surface area to
volume ratio**

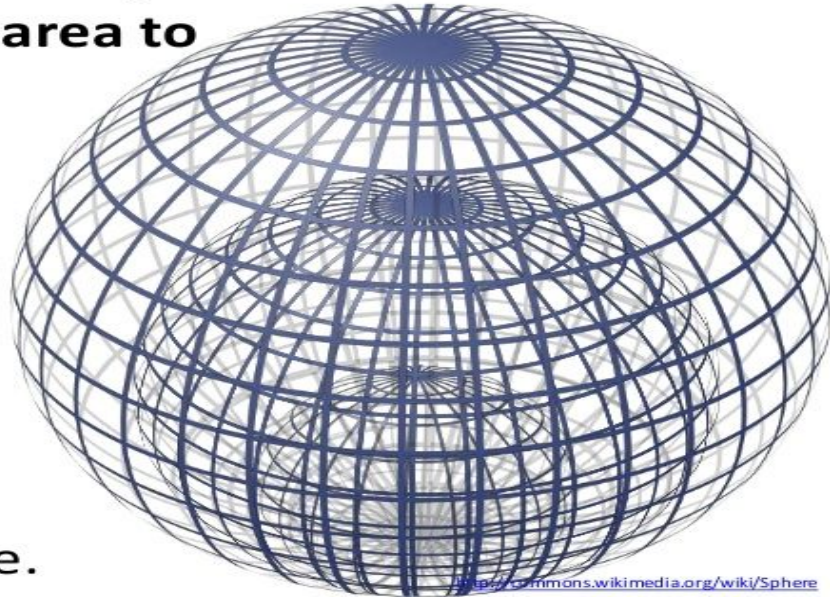
actually gets
smaller...

...so the

**exchange
processes**

become **less
efficient** with

increasing size.



“AAAA” Threats to Identity/Information Systems



Attacks, Accidents and Acts of Nature



Good Luck

- Let's continue the conversation
- sldavid@uw.edu
- @ScottLDavid

ONCE
UPON
A
TIME

John Fontana