CPSC 436C Cloud Computing

Winter 2025 Term 1 (September 16, 2025)

Tony Mason (fsgeek@cs.ubc.ca), Lecturer

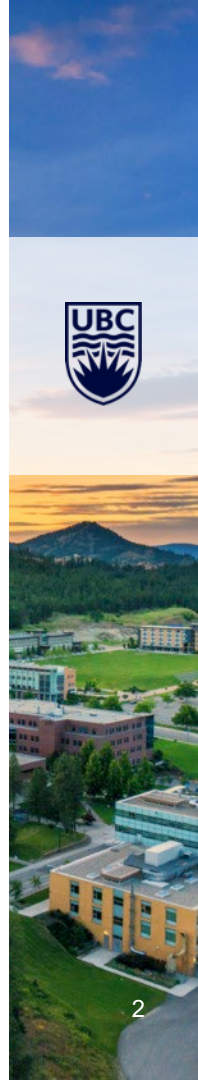
Logistics

Tony's Office Hours:

- **Wednesday September 17 @ 14:00-15:00 (Discord)**
- **Monday September 22 @ 16:00-17:00 (Discord)**
- **Random discord/twitch streaming**

TA Office Hours: TBA

Project 1 Due September 22 @ 11:00 AM PT

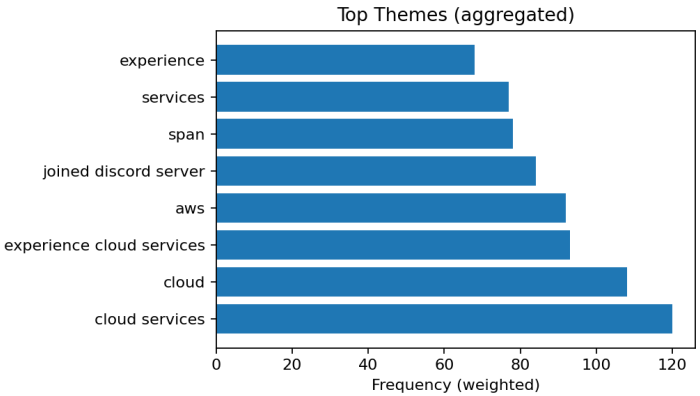


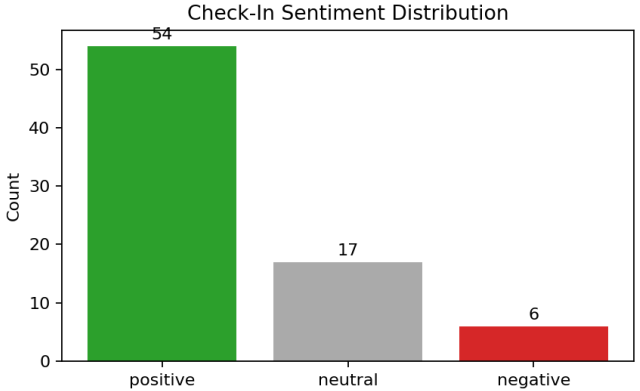
Check-In #1 Sentiment Summary

Aggregate only; IDs hashed; no quotes

Sentiment via VADER; themes are weighted n-grams

We'll act on top themes next class





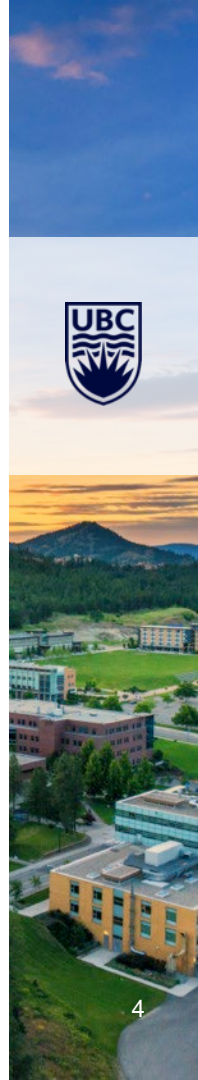
Course Changes

Key observations leading to change:

- Onboarding friction: Canvas page added
- Cloud credits: I'm not happy either, but this one is outside my control.

You provided feedback, I operationalized it. Note that I used cloud analytic tools to do so, but in a privacy aware, privacy preserving fashion (all PII stripped).

Of course, the *data* came from the cloud. Do *you* know Canvas' data privacy track record?



Canvas Track Record

Vulnerability Type	Potential Impact on Users & Data	Status
Improper Access Control (CVE-2021-36539)	Unauthorized access to private or unpublished course files (e.g., draft exams, sensitive student work, research data).	Patched
Publicly Exposed File URLs (2024 Incident)	"Private" files became discoverable via public search engines if their URLs were shared, completely bypassing normal permission checks.	Patched
Privilege Escalation (Broken Access Controls)	Users with one role (e.g., teacher) could potentially access data from a higher-privileged role (e.g., administrator PII).	Patched
Cross-Site Scripting (XSS)	Could allow an attacker to steal user session cookies (impersonating a student or instructor) or execute unauthorized code in their browser.	Patched
Server-Side Request Forgery (SSRF)	An attacker could force the Canvas server to make requests to internal services or malicious external sites, potentially leaking data.	Patched

Quick Check-in

Show of hands: Who identified something to predict?

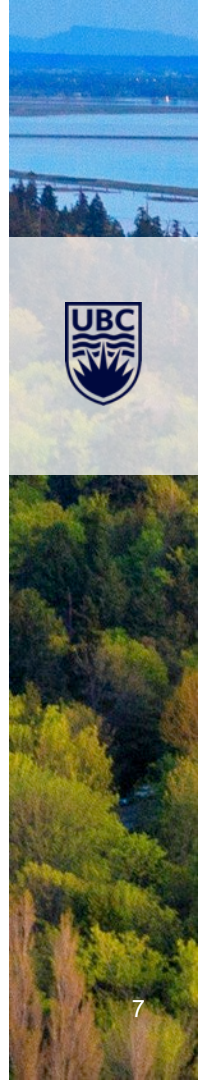
Quick Share: Most memorable experience?

Remember: This is about learning together.

Controlling Information

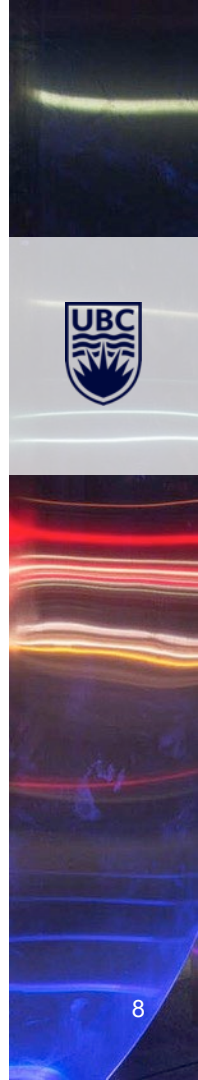
Today: Governmental Control

Thursday: Commercial Control



Question

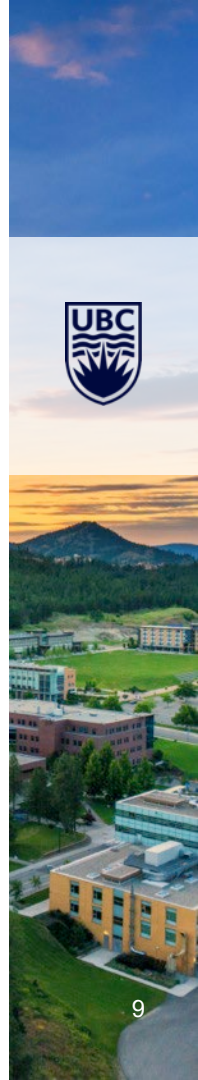
Who benefits and who is exposed when cloud providers block domain fronting to comply with national laws?



Domain Fronting

Cloud architecture pattern: separate TLS connection endpoint from content origin

- CDN Architecture
  - Designed for *performance*
  - Is **not** end-to-end security (or rather the “end” is the CDN edge)
- Multi-tenancy: many origins, whose rules apply?
- Edge Computing: **performance** is the primary goal
  - What other security/performance trade-offs do we make in cloud design?
- Cloud providers sell “simple” service that hide complex routing.
  - Complexity is hidden
  - **Who owns the problem?**



Cloud Implementation

By 2018 Google, Amazon, **and** Microsoft had blocked domain fronting.

- Rationale: “this is a violation of our terms of service”
- Explanation: “exploit between routing and content delivery”

So again: *Who benefits and who is exposed when cloud providers block domain fronting to comply with national laws?*

Perspectives

Actor	Perspective on Blocking Domain Fronting
Sovereign Nation A (e.g., seeking social stability)	Benefits: Strengthens national laws, asserts digital sovereignty, controls information flow seen as destabilizing. Exposed?: To criticism from external actors.
Sovereign Nation B (e.g., seeking to project influence)	Benefits: Can now more effectively control the narrative within its cyberspace. Exposed?: To techniques it itself might use.
Cloud Provider (Western - AWS, GCP, Azure)	Benefits: Complies with law, reduces liability, maintains market access. Exposed?: To accusations of being an arm of state censorship.
Cloud Provider (Chinese - Alibaba, Tencent, Huawei)	Benefits: Their operational model is inherently validated. They avoid the public relations dilemma faced by Western firms. They demonstrate alignment with state goals. Exposed?: To criticism in international markets; a calculated trade-off.
Journalist / Activist	Exposed: Loses a tool for secure communication and circumvention. Benefits?: (None from the blocking itself)
Everyday Citizen	Exposed: Potentially to greater surveillance and a more limited information ecosystem. Benefits?: Potentially to a more "stable" online experience, as defined by their state; protection from external disinformation?

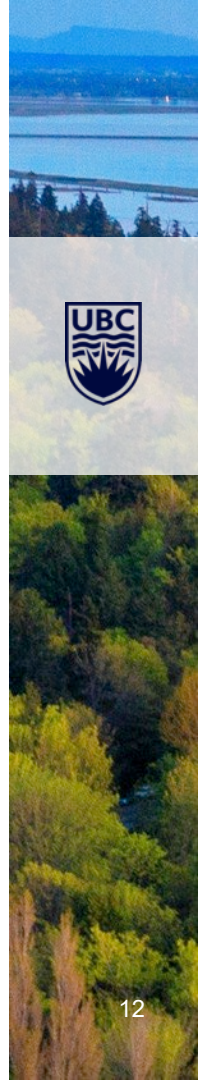
Global Perspective

Western companies:

- Domain fronting: verify the SNI matched HTTP host header
- Content must come from the front-end domain
- No man-in-the-middle attacks
  - Except the *service provider* of course

Observations:

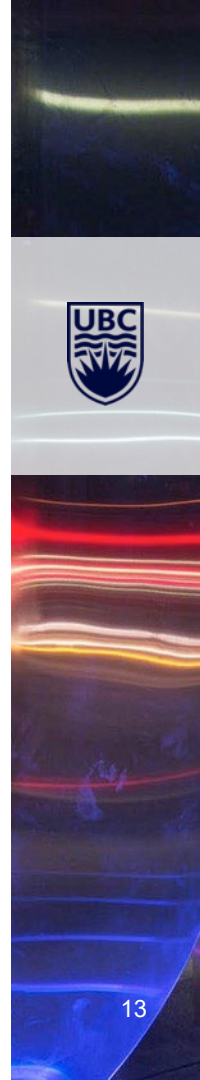
- Russia pressure on Google/Amazon about Telegram using domain fronting
- China concerns about apps doing the same thing
- Security researchers pointing out this was an exploit being used “in the wild”



Global Perspectives

Eastern Companies:

- Inverse problem:
  - Domestic governmental data control requirements
  - International requirements that differ
- Alibaba: dual stack
- Huawei: global expansion
  - Alternative to NSA (e.g., Latin America)
- Yandex (Russia)
  - Blocks domain fronting
  - Governmental data controls



Cloud Fundamentals

Shared Responsibility

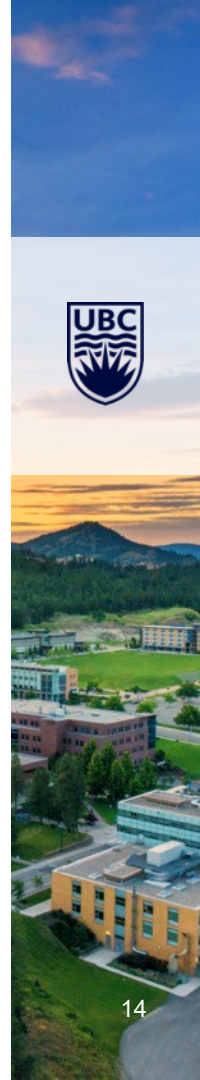
- Users
- Cloud Providers
- Content Providers

Who is responsible for preventing censorship circumvention?

Is this even a security question?

Cloud Providers Promise:

- Global reach
- Local compliance
- Domain fronting shows how these aren’t compatible



Question

Does every region of the world *need* its own cloud computing?

- Data control
- Is it *possible* to provide true neutrality – or is ownership the requirement?

Data Control

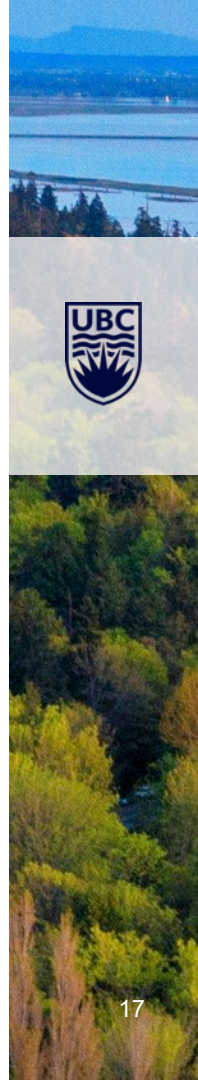
Layers & techniques (with quick examples):

- IP/ASN blocking; BGP hijacking/route filtering
- DNS tampering (poisoning/injection), SNI filtering, TLS fingerprinting
- HTTP keyword filtering; active probing; traffic shaping/throttling
- QUIC/HTTP/3 blocking; ECH (Encrypted ClientHello) implications
- Detection signals and typical error modes (false blocks, collateral damage)

Data Control

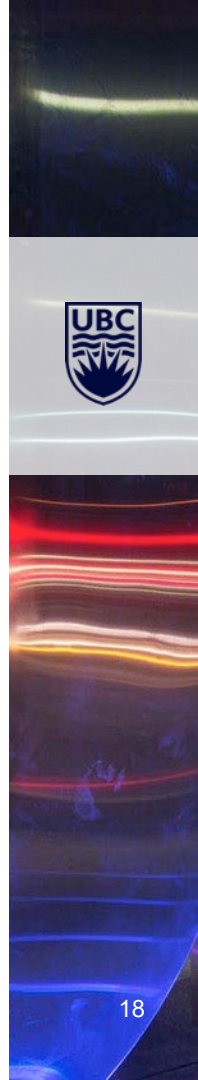
Countermeasures & Trade-offs

- DNS over HTTPS/ TLS; ESNI/ECH; SNI encryption – where it works/fails
- Tor and pluggable transports (obfs4, meek, snowflake); bridge discovery
- Domain fronting (history, deprecation, ToS/policy constraints)
- Decoy routing / refraction networking (TapDance/Refraction)
- CDNs, multi-CDN strategies; cost and policy boundaries
- Measurement frameworks (OONI, ICLab) and safe participation



Challenge

You are the next generation of architects. The current global cloud infrastructure is not a law of nature; it is a set of design choices that concentrate power and create dependence. If you were tasked with designing a cloud for the 'Non-Aligned Movement,' what would its core architectural principles be?



Responsible Handling of Sensitive Materials

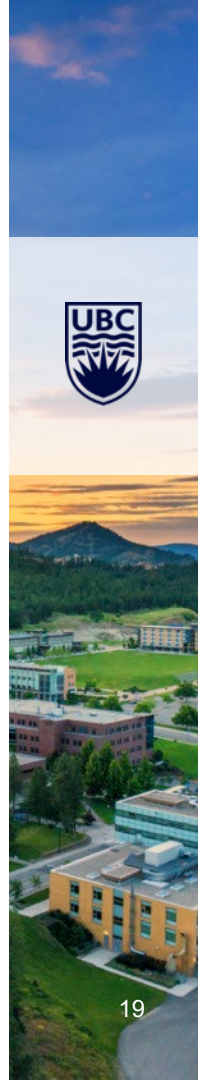
Do not download or possess leaked/classified materials for coursework; use vetted secondary sources.

Minimize harm: avoid PII, do not name individuals; focus on systems/governance.

Purpose limitation & minimization: state retention TTLs; document access and roles.

Reciprocity: return value safely (transparency/notice; responsible disclosure patterns).

Comparative lens: analyze state, platform, infrastructure without country-bashing.



Legal Realities: Who Can Handle Leaked Data?

A Case Study in the Real-World Rules of Data Privacy

✓ Legal, technical, and ethical risks for academics downloading leaked data

✓ "Chilling effect" = rational response to asymmetric risk

⚠️ **But... does EVERYONE follow these rules?**

The "Geedge" leak case study - Three key players:

1. The Government
(CSIS)

2. The Media
(Globe & Mail)

3. Academics
(Us)

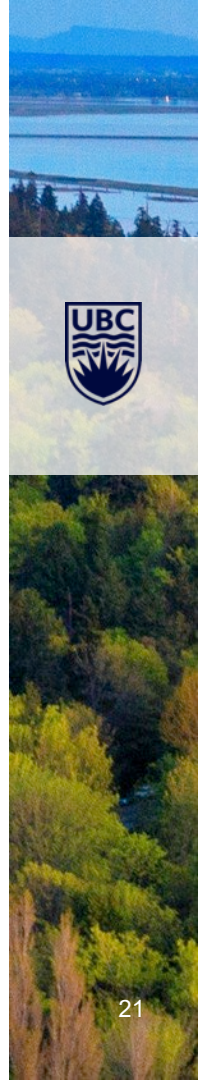
The Rules Aren’t the Same for Everyone

Rules depend on role, mandate, and legal protections

Actor	Primary Mandate	Key Question
🏛️ **The State** (CSIS)	National Security	*"Is this a threat?"*
📰 **The Media** (Globe & Mail)	Public Interest	*"Should the public know?"*
🎓 **Academics** (Us)	Legal Compliance	*"Is this legal & ethical?"*

📌 **KEY INSIGHT:**

Journalists have legal protections (Journalist Sources Protection Act) and institutional support (lawyers, editors, infosec teams) that academics lack.



The Accelerator Layer: Wealth & Power

The "meta-layer" that bends the rules for all tiers

💡 **Wealth doesn't change the law, but changes your ability to navigate, influence, and withstand its consequences**

How Wealth Changes the Game:

⚖️

Legal Resources

Top-tier legal teams
to fight or settle

🛡️

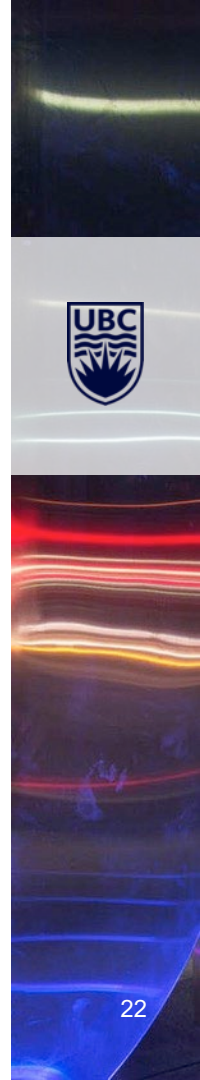
Outsourcing Risk

Private security firms
under attorney privilege

📢

Managing Fallout

PR & financial resources
to survive damage



So What? Why This Matters to You

CPSC 436C TAKEAWAYS

1

Cloud systems are NOT neutral

They exist in a world where power, law, and ethics are in constant, unequal conflict.

2

Technical ≠ Complete

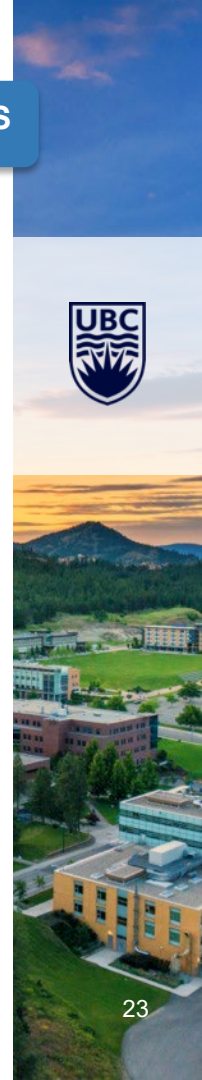
Encryption, access control, IAM are just one layer. Human and political layers are equally important.

3

Technician vs. Professional

Understanding this landscape is what separates a good technician from a wise professional.

🎯 **Build with awareness. Deploy with wisdom. Lead with integrity.**



So What? Why This Matters to You 🧠

CPSC 436C TAKEAWAYS

1

Cloud systems are NOT neutral

They exist in a world where power, law, and ethics are in constant, unequal conflict.

2

Technical ≠ Complete

Encryption, access control, IAM are just one layer. Human and political layers are equally important.

3

Technician vs. Professional

Understanding this landscape is what separates a good technician from a wise professional.

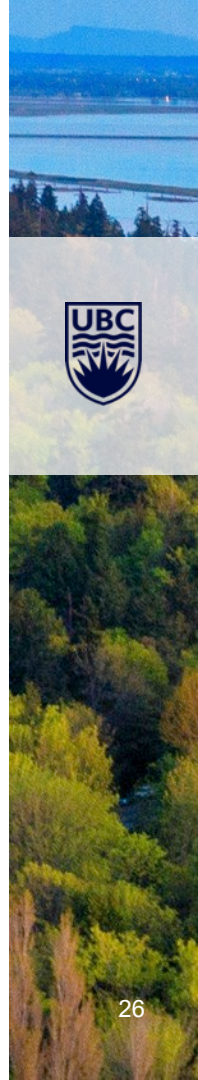
🎯 **Build with awareness. Deploy with wisdom. Lead with integrity.**

Question

Quick poll: how many students would appreciate a discussion of *ethical models* that are relevant to cloud computing?

Context: the goal isn't to teach you right from wrong, it is to *evaluate the ethical implications of what you are doing or being asked to do.*

Discussion



RENT SEEKING