DS 593: Privacy in Practice

Privacy in Tension

Instructor: Alishah Chator

News?

CLIENT-SIDE ENCRYPTION

Gmail unveils end-to-end encrypted messages. Only thing is: It’s not true E2EE.

Yes, encryption/decryption occurs on end-user devices, but there's a catch.

DAN GOODIN – APR 3, 2025 5:16 PM | 66

Credit: Getty Images

https://arstechnica.com/security/2025/04/are-new-google-e2ee-emails-really-end-to-end-encrypted-kinda-but-not-really/

BurnBox: Self-Revocable Encryption in a World of Compelled Access

Nirvan Tyagi
Cornell University

Muhammad Haris Mughees
UIUC

Thomas Ristenpart
Cornell Tech

Ian Miers
Cornell Tech

https://eprint.iacr.org/2018/638.pdf

SocIoTy: Practical Cryptography in Smart Home Contexts

Tushar M. Jois
City College of New York
tjois@ccny.cuny.edu

Gabrielle Beck
Johns Hopkins University
becgabri@cs.jhu.edu

Sofia Belikovetsky
Johns Hopkins University
sofia.belikovetsky@gmail.com

Joseph Carrigan
Johns Hopkins University
joseph.carrigan@jhu.edu

Alishah Chator
Boston University
alishahc@bu.edu

Logan Kostick
Johns Hopkins University
lkostic1@jhu.edu

Maximilian Zinkus
Johns Hopkins University
zinkus@cs.jhu.edu

Gabriel Kaptchuk
Boston University
kaptchuk@bu.edu

Aviel D. Rubin
Johns Hopkins University
rubin@cs.jhu.edu

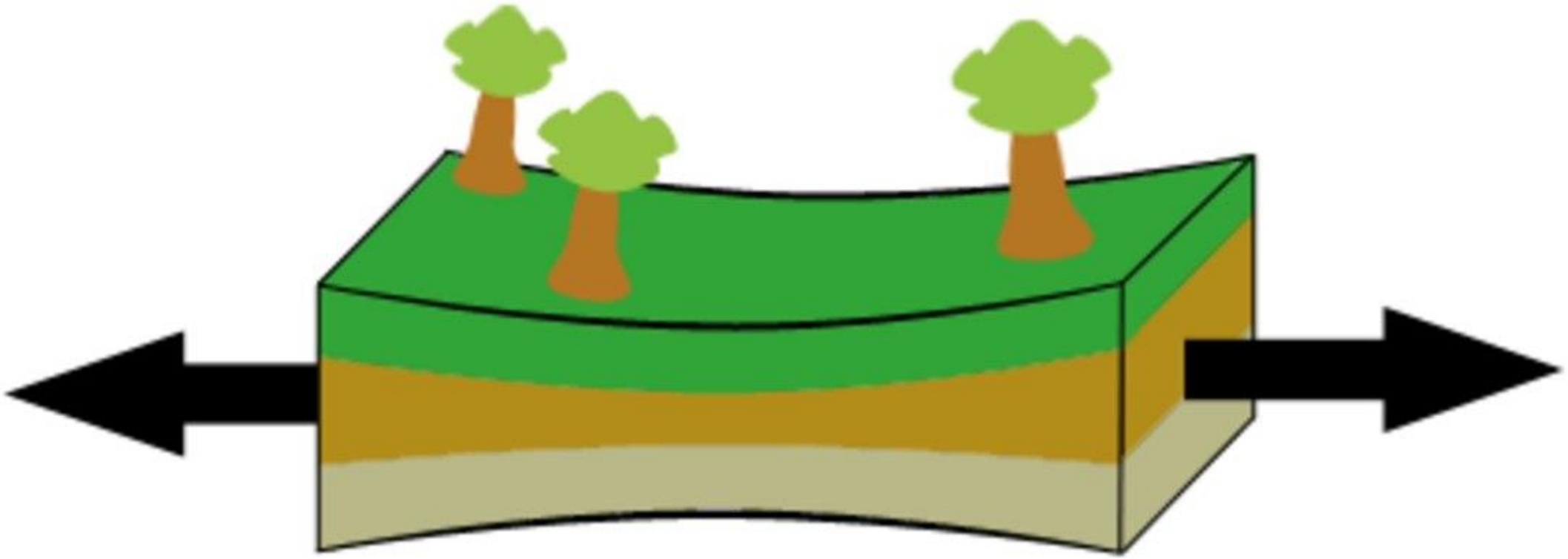
https://petsymposium.org/popets/2024/popets-2024-0026.pdf

Last time

- Exploring targeted and mass surveillance by the state, corporations and other actors

Today

- Exploring some of the tensions and trade-offs with regards to privacy



Tension

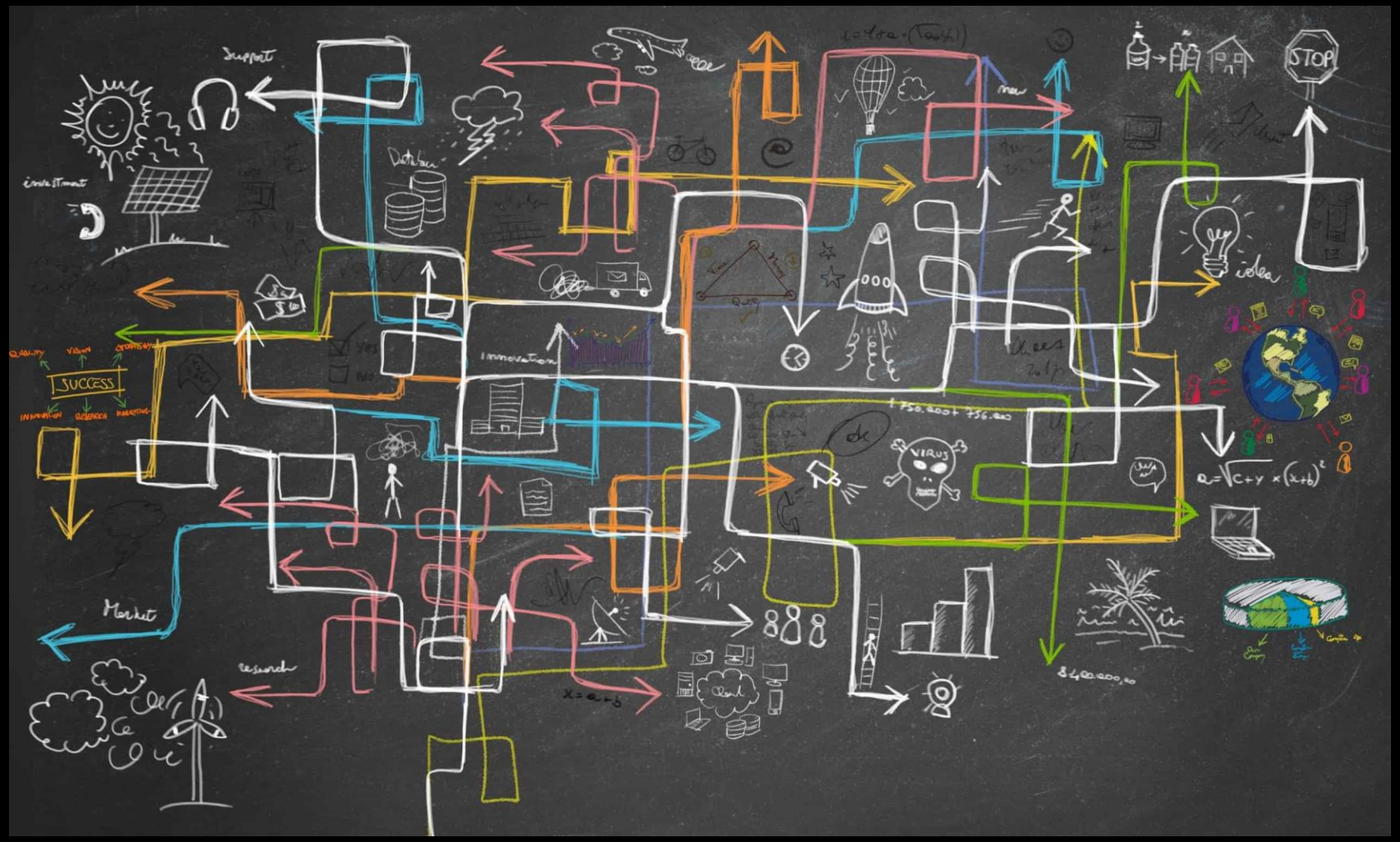
Valid concerns of negative impacts of privacy

- Safety impacts – Will this limit investigative capabilities?
  - “Going Dark”
- Business impacts – Will this limit what we can build and do?
- Societal impacts – What about the benefits of systems like contact tracing?
- Social impacts – Toxicity is correlated with anonymity

Valid concerns about consequences of surveillance

- Impacts of free expression
  - Privacy is understood as a necessary basis for other rights
- Dangers of misuse, hard to audit
- Can potentially decrease safety
- Limited evidence of efficacy
- Can have unintended consequences

It’s Complicated



Focus of today: Exceptional Access

- Most people on all sides of debate agree privacy is important
- Generally the request is for *Exceptional Access*
  - Privacy in most cases but can be undone in extreme cases
- Yet, privacy advocates often appear inflexible and reject even this idea
  - Why?

How to Build Exceptional Access

- The main privacy tool in these systems is encryption
  - Need to circumvent this somehow

- This is often referred to as a *backdoor*

Circumventing Encryption

- Weaken the standards
- Attack the cryptography
- Attack the implementation
- Attack everything outside the cryptography
  - The device
  - The metadata

What’s the worst that can happen?

The Clipper Chip (Early 1990s)

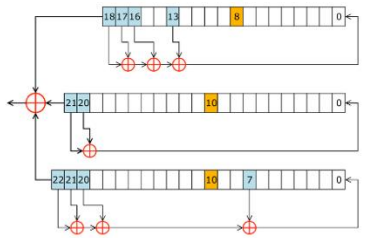
Export-Grade Encryption (1990s)

Primitives

- Practical Example: GSM encryption
  - A5/0: No encryption
  - A5/1: Based on LFSRs
  - A5/2: Weakened A5/1
  - A5/3 (KASUMI): New for 3G

GSM™
The wireless evolution

T-Mobile



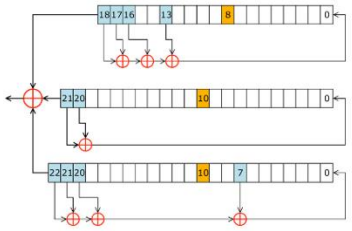
at&t

Primitives

- Practical Example: GSM encryption
  - A5/0: No encryption
  - A5/1: Broken
  - A5/2: Way Broken
  - A5/3 (KASUMI): Dented
    (and 3G vuln. to protocol attacks)
- Deliberately weak cipher design
  - Cost & politics

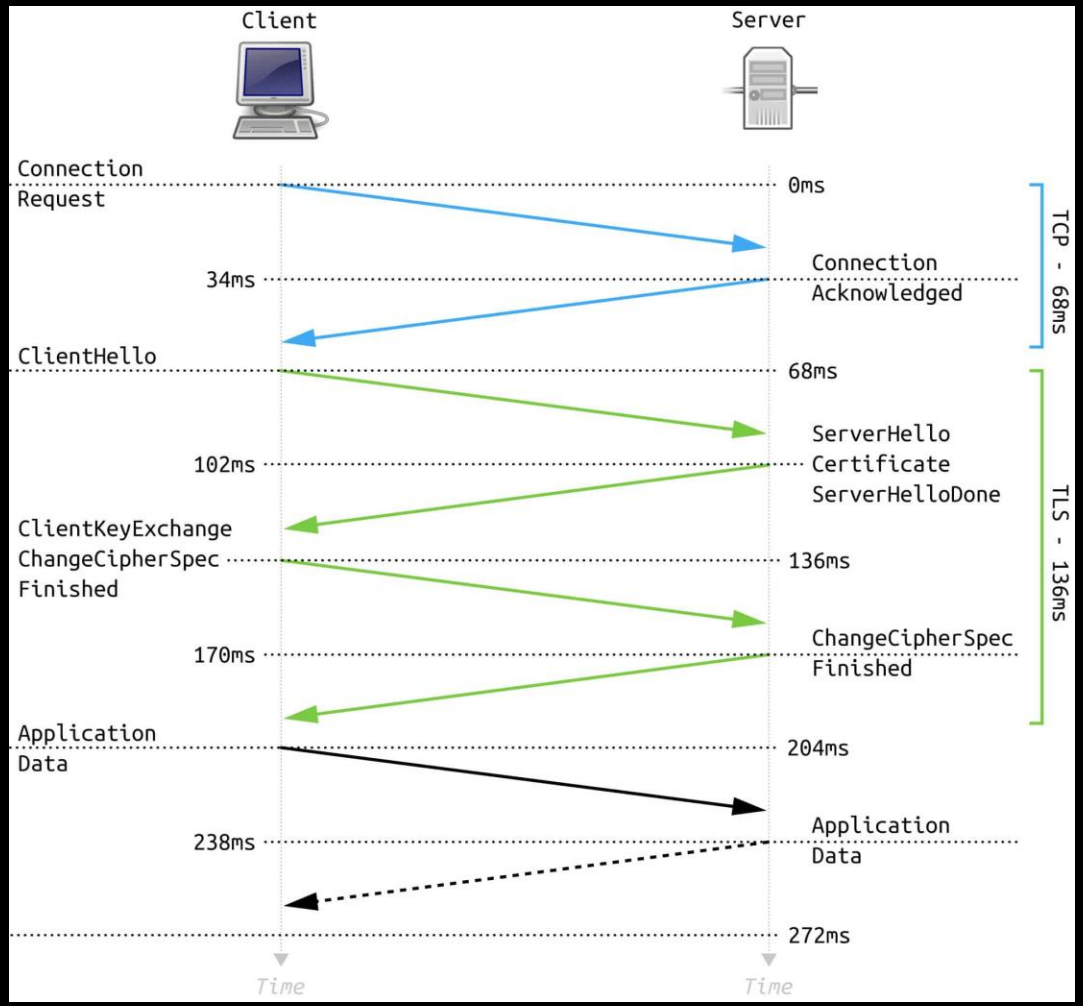
GSM
The wireless evolution

T · · Mobile



at&t

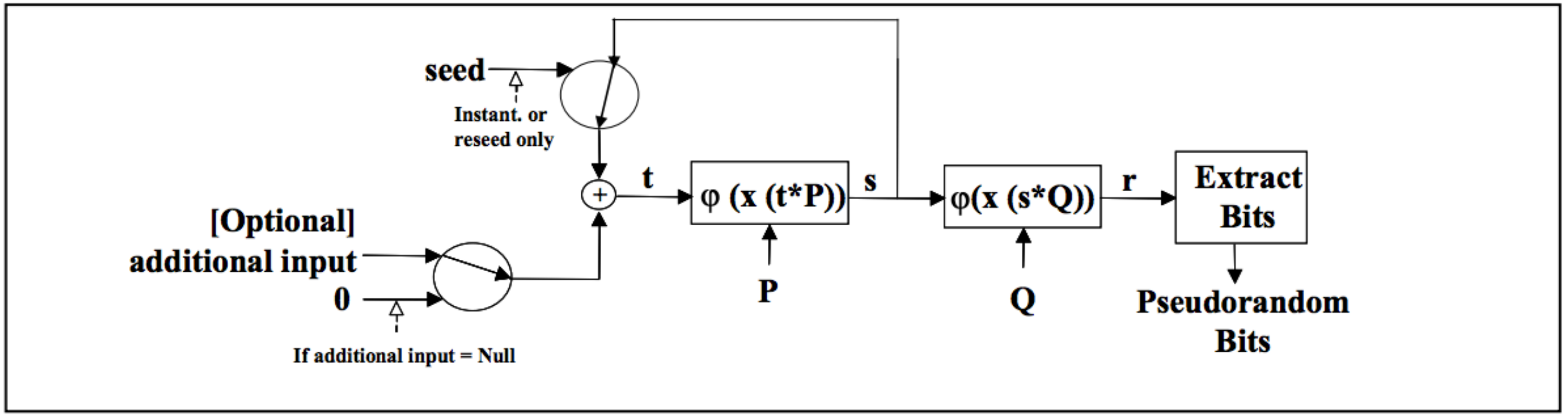
TLS/SSL (1990-???)


Client
Server
Connection
Request
0ms
Connection
Acknowledged
34ms
TCP - 68ms
ClientHello
68ms
ServerHello
Certificate
ServerHelloDone
102ms
ClientKeyExchange
ChangeCipherSpec
Finished
136ms
ChangeCipherSpec
Finished
170ms
TLS - 136ms
Application
Data
204ms
Application
Data
238ms
272ms
Time
Time

Rollback Attacks

- POODLE (2014)
- FREAK (2015)
- Logjam (2015)
- DROWN (2016)

Juniper and Dual EC (2015)



Ghost Users

Zero days and Device Vulnerabilities

- Recall from last class
- Pegasus
- Quantum-Turbine

On Metadata

- Do we really need to protect this too?

On Metadata

- Do we really need to protect this too?

- *“Metadata absolutely tells you everything about somebody’s life. If you have enough metadata you don’t really need content.”* - Stewart Baker, former general counsel for the NSA

- *“Baker is absolutely right. We kill people based on metadata.”* - Michael Hayden, former director of the NSA and CIA

Upshot

- Historically, any attempt towards exceptional access leads to a global weakening of security with lasting aftereffects
- Hard to control who can leverage a backdoor
  - NSA hacking Greece
  - China hacking Google
- No party is beyond compromise
- Many former national security officers support strong encryption

Next Time

Hate speech and content moderation challenges

Navigating this tension