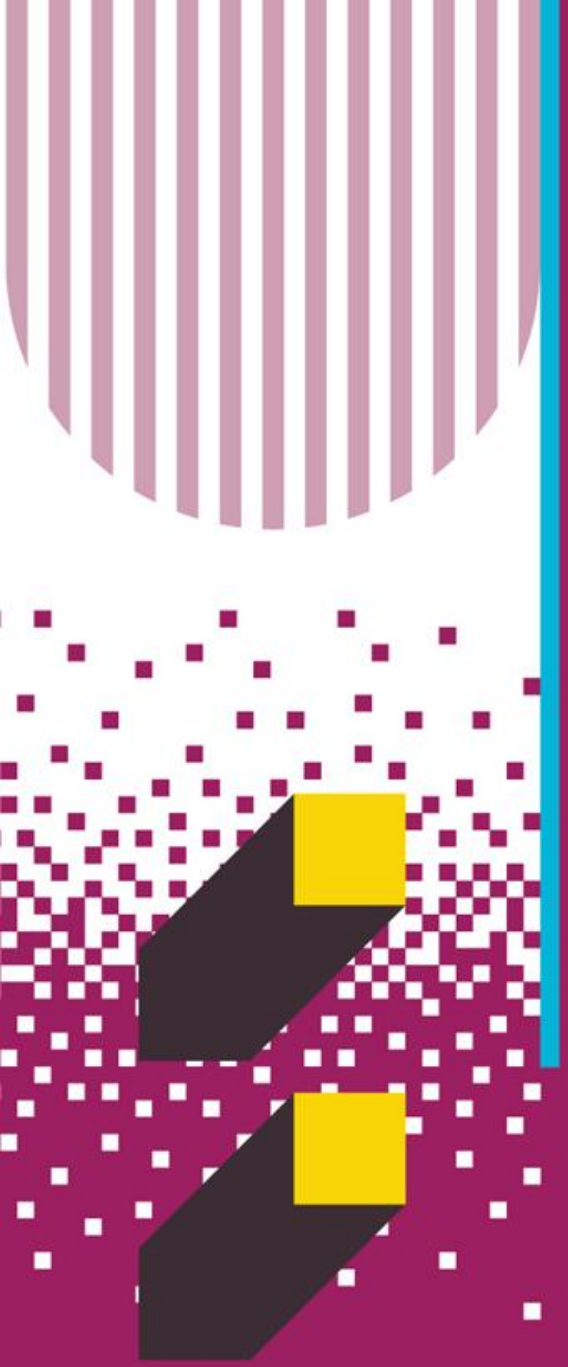


# IAPP **Canada Symposium 2026**

## Privacy | AI governance | Cybersecurity law

**Conference 4-5 May**
Workshops 6 May
Training 6-7 May
**TORONTO**

**#IAPPSymposium26**

# QUANTUM SHIFT: PRIVACY PERILS & PROMISES

## A Family Perspective, on Star Wars Day

# WELCOME & INTRODUCTIONS

**Patrick Hayden**
Quantum Physicist & Professor
Stanford University

**Anne-Marie Hayden**
Privacy and Comms Consultant
nNovation LLP, Hayden PR

# WHAT WE'LL COVER TODAY

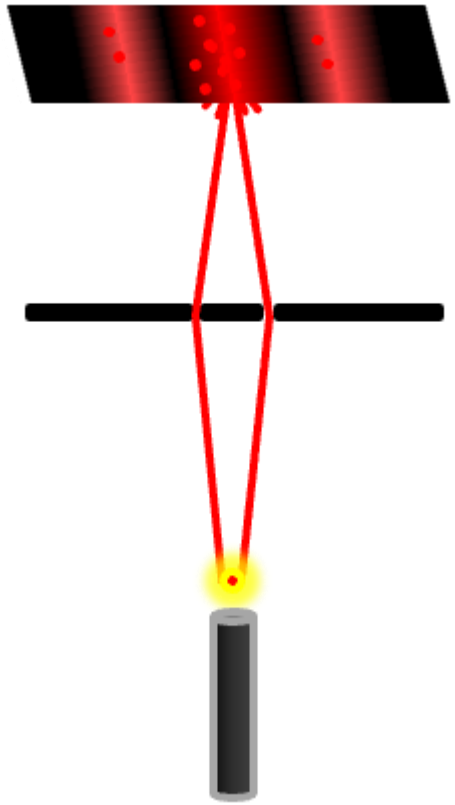
- ✅ Why quantum computing is now on our profession's radar
- ✅ Quantum Computing 101
- ✅ Why quantum matters for people working in data protection
- ✅ Risks for privacy and digital trust
- ✅ Benefits of quantum for data protection
- ✅ Top tips to prepare
- ✅ What quantum does *not* change
- ✅ Helpful resources
- ✅ A few little Star Wars references (can't help it; it's in our DNA)

# WHY QUANTUM IS ON THE RADAR:
# RULES OF THE GALAXY ARE CHANGING

Three main reasons:

1. Quantum capability is advancing beyond theory, and the tech is becoming real: <5 years to Q-day
2. The sensitive information we're collecting and producing now will outlast today's encryption
3. Post-quantum standards are emerging

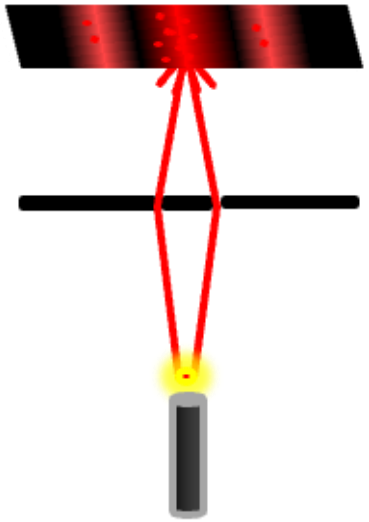
# QUANTUM COMPUTING FUNDAMENTALS:
# NO SCIENCE FICTION!

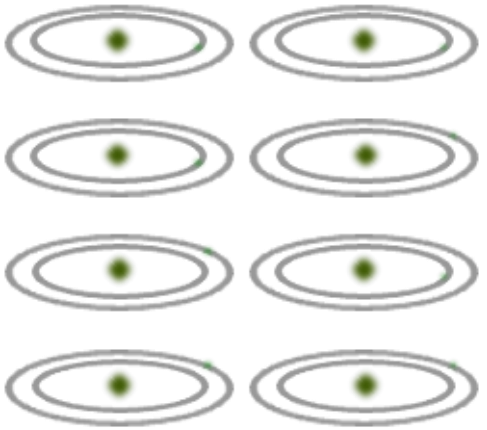


**Fact 1:** Everything is wavy in quantum mechanics

**Fact 2:** Mutually exclusive states can coexist

# QUANTUM COMPUTING FUNDAMENTALS:
# NO SCIENCE FICTION!





All the usual computing we know and love

Interference and superposition

Exponential growth

GOOD FOR DETECTING EXPONENTIALLY LONG PATTERNS

# WHY IT MATTERS:
# PROTECTING THE REPUBLIC

- There is **no privacy** in a digital world without secure cryptography
- Encryption protects confidentiality, identity and integrity
- If cryptography weakens, so do digital trust and safety

# RISKS TO PRIVACY & DIGITAL TRUST:

## THE DARK SIDE

- Widely deployed public-key systems can fail at scale
- Encryption and digital signature protocols would be compromised
- Previously encrypted long-term data could become readable
- Global digital trust infrastructure depends on these systems
- The systematic impact would be profound
- This is a *known* vulnerability that cannot be understated

# BENEFITS FOR DATA PROTECTION: A NEW HOPE

- Cryptographic agility improves future-proofing
- Migration planning can modernize security architecture
- Proactive governance reinforces digital trust
- *Bonus:* Post-quantum cryptography strengthens long-term resilience – you don’t need to trust your cloud

# TIPS TO PREPARE:
# THE RESISTANCE STRATEGY

- Very simple in most cases
- Understand where encryption underpins your data protection program
- Monitor for reference implementations of post-crytographic protocols and guidance
- Ensure your organizations migrate to them
- Migration should also apply retroactively
- Pressure vendors to get in line
- Strengthen data minimization and retention discipline

# WHAT QUANTUM DOES *NOT* CHANGE


- Quantum will not revolutionize technology on the scale of AI - don't believe all the hype
- It remains a specialized capability
- Quantum does not change:
  - Privacy principles and obligations endure
  - Accountability, risk assessments, data minimization and governance remain essential
  - Episode 5 is still the best of the saga

# HELPFUL RESOURCES TO STAY CURRENT

NIST Post-Quantum Cryptography Resource Center

What makes quantum computers so hard to explain? [article] [video]

Major platform updates:

i. Google
ii. Apple
iii. AWS

Mandalorian and Grogu trailer

# THANK YOU

# How Did Things Go?
# (We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Symposium 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!