

Rebuilding Digital Trust: A Measured Path Through Quantum and AI

Recent reporting from the WSJ and NYT points to two shifts in how we secure data and verify media. Neither calls for alarm. Both call for a plan.

By Parker Dunning, Managing Principal & Founding Architect · Oct 11, 2026 · 6 min read

Two recent pieces of reporting are worth reading side by side.

The Wall Street Journal examined how much data sits exposed on the public internet, including internet-connected cameras that have been compromised and used for intelligence gathering. The New York Times tested a dozen AI-detection tools and found they are reliable in some situations and inconsistent in others.

On the surface these are separate topics: one about keeping data **confidential**, one about knowing whether media is **authentic**. They call for different tools, but they share a lesson: trust holds up best when it is **established at the source**, rather than inspected after the fact.

The good news is that the path forward is well understood, the standards are maturing, and organizations that start now can move at a deliberate pace.

Shift One: How We Protect Data Over Time

Start with the basics

Much of the exposure the WSJ described comes from familiar, fixable issues: devices still running factory-default passwords, firmware that hasn't been updated and settings that were never changed after installation. Intelligence agencies in Europe and elsewhere have noted that many of the compromised cameras had exactly these weaknesses.

These are not exotic problems, and they have straightforward solutions: inventory, update, segment.

Plan for the quantum transition

The longer-horizon consideration is encryption itself. Today's public-key encryption is expected to become vulnerable once sufficiently capable quantum computers exist. Because some adversaries collect encrypted traffic now in hopes of decrypting it later — a practice known as **Harvest-Now-Decrypt-Later** — the question to ask is simple: *how long does this data need to stay confidential?*

For most day-to-day information, the answer is short and the risk is modest. For long-lived assets such as intellectual property, health records, financial data and sensitive communications, it makes sense to prioritize a move to post-quantum protection.

This is a well-charted transition. NIST finalized its first post-quantum cryptography standards in August 2024, and federal guidance — including National Security Memorandum 10 and the Quantum

Computing Cybersecurity Preparedness Act — already lays out a phased migration path that the private sector can follow.

Shift Two: How We Know What's Real

What the NYT found

The Times generated images and videos with leading AI models and ran them, along with real photographs, through twelve detection services.

- **Real photos were recognized reliably.** Genuine camera images were consistently identified as real.
- **Sophisticated fakes were harder.** On the more complex AI-generated images, only a few tools flagged them correctly.
- **Video support varies.** Many services don't yet analyze video, and some AI clips were judged authentic.

The Times' sensible conclusion: treat a detector's verdict as one input and corroborate it with other evidence.

A more durable approach

Detection tools will keep improving, and so will image generators. A more durable approach is to record provenance when content is created. Industry standards such as C2PA Content Credentials do this by attaching a cryptographically signed record of the device or tool that produced a file and how it was edited — including a clear label when content is AI-generated.

The Common Thread: Attestation Over Inspection

Both shifts move trust away from inspecting things after the fact and toward establishing it at the source. They solve different problems, and both rest on modern cryptography.

	Data protection	Media authenticity
What it protects	Confidentiality: who can read the data	Authenticity and integrity: where content came from and whether it changed
Old approach	Assume classical encryption and perimeter firewalls will hold	Inspect pixels and hope fakes leave traces
Modern approach	Post-quantum encryption, authenticated devices, crypto-agility	Signed provenance at capture or creation
Depends on	Encryption that resists quantum attack	Digital signatures that resist quantum attack

The two are complementary, not interchangeable. Provenance shows that a file is genuine; it does not keep sensitive data private. Confidentiality still depends on strong encryption, and provenance depends on strong signatures — which is why post-quantum migration matters on both fronts.

It also helps to be precise about *whose* origin is being verified. Most legitimate enterprise traffic comes from machines — services, APIs and sensors — and is verified through device attestation and mutual TLS. For the smaller set of actions where a person's decision matters most, organizations can add one more layer: confirming that a real human authorized it.

A Practical Roadmap

None of this needs to happen overnight. A steady, phased approach works well:

1. **Take inventory.** Note where your systems rely on classical encryption, and which internet-connected devices you operate.
2. **Cover the fundamentals.** Change default credentials, keep firmware current and place IoT devices on their own network segment.
3. **Prioritize by data lifetime.** Plan post-quantum protection first for information that must stay confidential well into the next decade.
4. **Use detection as one signal.** Pair AI-detection results with other verification before acting on them.
5. **Ask for provenance.** Where possible, favor tools and partners that support signed content credentials.
6. **Build crypto-agility.** Build systems so cryptographic algorithms can be updated as standards evolve, without a full rebuild.
7. **Add human verification where it matters most.** Reserve human-verified authorization for your highest-value access, approvals and decisions.

Looking Ahead

Quantum computing and generative AI are both creating real opportunity, and the security practices that accompany them are maturing quickly. Organizations that approach these changes calmly and methodically — starting with the fundamentals and building toward modern encryption and trusted provenance — will be well positioned for what comes next.

Secure Your Access.

Safe. Secure. Simple.

secure@routerandrouter.com

[Explore Services](#) · [Get in Touch](#)
