Trusted Notifiers: Making Domain Takedowns Work

ICANN84 Session Summary and emerging topics | ccNSO & GAC

Bottom Line Up Front

Trusted notifier systems work—and they're surprisingly straightforward. The UK's .uk registry (Nominet) shared how they manage 2-3 thousand domain takedowns yearly using three tiers of trusted relationships. The key insight? **Don't try to become experts in everything.** Partner with people who already are—like law enforcement, child safety organizations, and specialized watchdogs. Speed varies by severity: child abuse content gets suspended immediately, while other cases get 48 hours to appeal. No lawsuits yet, which suggests the system's working.

How Trusted Notifiers Actually Work

Think of it as a VIP lane at airport security. Most abuse reports go through standard channels, but trusted notifiers get expedited handling because they've proven themselves reliable. Here's the UK system:

Three Tiers of Trust

1. Internet Watch Foundation - The Fast Lane

When the Internet Watch Foundation reports child abuse content, domains get suspended *immediately*. No questions, no delays. The trust level is absolute because the stakes are highest.

2. MOU Partners - Jump the Queue

Organizations like TWNIC and DotAsia have formal agreements (MOUs) with Nominet. Their reports don't get immediate suspension, but they jump to the front of the investigation queue. Think of it as priority processing.

3. Criminal Practices Policy - The Law Enforcement Channel

Nominet has arrangements with 14 UK law enforcement agencies. When they flag criminal activity (phishing, fraud, illegal gambling), the registry investigates and typically gives domain owners 48 hours to respond or prove legitimacy before suspension.

Real-World Example

One participant mentioned the UK Environment Agency case: a company was illegally dumping waste. The domain got suspended not because it violated ICANN rules, but because UK law enforcement requested action under the Criminal Practices Policy. The domain wasn't hosting abuse content—it was just being used by someone breaking environmental laws.

Scale and Process Details

By the Numbers:

- 2,000-3,000 domain takedowns per year
- Immediate suspension for child abuse content
- 48-hour notice period for most law enforcement cases
- Quick appeal process if mistakes happen

Cost-effective approach: Multiple participants emphasized this is actually cheaper and easier than building in-house expertise. It's described as "low maintenance" and "well-run." You're not hiring forensic analysts—you're trusting people whose full-time job is identifying specific types of abuse.

No lawsuits yet: Despite thousands of takedowns, Nominet hasn't faced legal challenges. This suggests the combination of trusted sources, clear terms and conditions, and appeal processes provides adequate protection.

Emerging Topics and Questions

Who Should Decide?

Strong consensus emerged: domain registries and registrars should *not* try to become experts in everything. As one participant put it, "We are not experts—there are experts that are very competent and have national and legal obligations." Partner with specialists rather than making judgment calls on unfamiliar territory.

The Jurisdiction Question

This got interesting. The UK system operates under UK law and jurisdiction. What happens when something isn't clearly illegal under UK law but might be elsewhere? The discussion touched on this but didn't resolve it. It's a clear tension point—especially for ccTLDs serving international audiences.

How to Get Started

Registries interested in setting up trusted notifier systems asked about implementation. The process seems to involve introductions and relationship-building with established organizations. There wasn't detailed discussion of formal requirements, but the implication is that trust must be earned and verified—it's not just paperwork.

Contracts and Consequences

Participants asked about what happens to domain owners: immediate cancellation or warning first? The answer depends on severity. Child abuse = immediate suspension. Other violations might trigger warnings or notice periods depending on terms and conditions. The trust level of the notifier influences the response speed.

Data Release and Privacy

Someone asked about data requests. Nominet confirmed they have a formal process for releasing data after proper review. It's not routine, but there's a structured approach when law enforcement needs information.

Registration Restrictions

Interesting note: .uk domains have no citizenship requirements. Anyone can register. This makes the trusted notifier system even more important since you can't rely on geographic or legal barriers to prevent abuse.

Key Takeaways for Registries

- **Start simple:** Don't build everything at once. Begin with one or two trusted partners with clear mandates (like child safety organizations).
- **Document everything:** Clear terms and conditions plus transparent appeal processes seem to prevent legal challenges.
- **Tier your responses:** Different types of abuse need different response speeds. Child safety = immediate. Other issues = notice periods.
- **Trust, but verify:** Even trusted notifiers get reviewed. Law enforcement tips go to investigators; MOUs don't mean blind acceptance.
- **Keep costs in mind:** This approach is described as cheaper and lower maintenance than trying to be experts in everything.
- **Plan for appeals:** Mistakes happen. Quick appeal processes help mitigate risks when the system gets it wrong.

The Bigger Picture

What's interesting about this session is what it reveals about internet governance. Trusted notifier systems work because they acknowledge that no single entity can be expert in everything. Child safety experts handle child safety. Law enforcement handles criminal activity. Environmental regulators handle environmental violations. The domain registry's role is facilitating action based on trusted expertise, not making impossible judgment calls across dozens of specialized domains.

The unresolved questions—especially around jurisdiction and international coordination—suggest this model still has room to evolve. But the core principle seems solid: build relationships with legitimate authorities, create clear processes, and don't pretend to know more than you do.

For registries considering implementing similar systems, the UK example provides a proven template. Three tiers, clear processes, manageable scale, and so far, no legal problems. Not bad for handling thousands of abusive domains per year.