Law enforcement and the .nz domain name space
What I’ll cover

• Who we are
• Compliance Philosophy
• Typical Process
• Domain Name Cancellation process
• Case Studies
• Future Plans
• Resources
By way of a Memorandum of Understanding with Government we operate the registry in accordance with .nz policies, procedures and formal agreements.
Activities that concern the abuse of domain names is of concern to the Commission and the community.

It’s important that people are who they say they are online.

We cannot police the whole Internet but we want to play our part in cooperating with law enforcement to make it difficult for criminals to operate in the .nz domain name space.
## Law enforcement – trusted notifiers

<table>
<thead>
<tr>
<th>Cyber Emergency Response Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Memorandum of Understanding</td>
</tr>
<tr>
<td>• Referrals of enquirers</td>
</tr>
<tr>
<td>• Quarterly operational meetings</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New Zealand Police</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identification of registrants</td>
</tr>
<tr>
<td>• Evidence for further investigation</td>
</tr>
<tr>
<td>• Source of reporting for fake registration details</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other: Court Orders and Statutory powers to conduct [criminal/consumer] investigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Authorised or required by law to disclose [statutory or court compulsion powers]</td>
</tr>
<tr>
<td>• Principle 11(e) of the Privacy Act 1993 - law enforcement exception</td>
</tr>
</tbody>
</table>
Typical process - considerations

- **Informal Intelligence Enquiry**
- **Formal email request for help**
- **Request for further information to support enquiry**
- **Managed through enquiry management workflows**

**Notice**

- Is it a cross border court order? If yes, must localise. Send legal proforma
- Is it content related? Refer to TLD principles and .nz policy no jurisdiction re criminal behaviour liaise with Hi Tech Crime Unit in New Zealand Police, CERT or Netsafe
- Is it local law enforcement about infrastructure or registration abuse closely related to the security and quality of the DNS and the register?
- Authority to assist local law enforcement - either Court imposed or disclosure permitted under Principle 11 (e) of Privacy Act

**Due process & due diligence**

- Notification to registrant where outcome may be cancellation process
- If request is for withheld registrant (email and phone number) then Registrant will be notified of disclosure unless disclosure would prejudice an investigation & subject to transparency reporting

**Transparency & procedural guarantees**
Specific process for domain name cancellations

Contact the current registrant of the .nz domain name via the .nz data query service. The registrant information can be searched via the following link: https://dns.org.nz/whois

If the registrant is unable to be contacted at the details on the registration record let the Domain Name Commission know what details require updating.

The Domain Name Commission will follow up with the Registrant and the .nz Authorised Registrar to have the details updated.

If the registration details are not updated, then the domain name may be cancelled.

If the issue is not resolved, then the Domain Name Commission may be able to provide further assistance, or provide information about an organisation that can

Domain Cancellations

103 domain names for incorrect or invalid registration details

In the six month period between October and March 2018, the Domain Name Commission cancelled 103 domain names for incorrect or invalid registration details. These cancellations are in contrast to 2 domain name registration cancellations between April 2017 and September 2017.

2 domain name registration cancellations between April 2017 and September 2017.

We have also commenced a program of work to follow up domain names we are made aware of by CERT NZ or other trusted notifying bodies, and those brought to our attention by members of the public.

Trends

Over the last year, we have seen a steady upward trend in cancellations of non-compliant domain names for having invalid contact details, and as we solidify our thinking of processes when it comes to poor registration details, this number will only increase.

These cancellations occurred in the context of a broadening public debate around illegal and offensive content and infrastructure abuse involving increased cyber criminality and cyber warfare.
Example two Case Studies – this year

Case study 1

• Batches of domains referred by law enforcement agency allegedly registered with fake details.

• Due diligence undertaken by Commission and various notices sent to registrant. Registrant provided with opportunities to correct the registration record.

• Of those referred X number updated their record. The rest were either:
  • Made up details - no response OR
  • Real details - but never registered a domain

• In both scenarios domain names cancelled.

Case study 2

• Compliance check following referral by law enforcement resulted in systemic investigation in to more than 3000 .nz domains.

• Notification of systemic investigation to .nz authorised Registrars.

Outcome

• .nz authorised registrars working with the Commission to identify where there might be a problem in their reseller network.

• One .nz registrar immediately quarantined domain names in a holding account pending data validation checks
What we have planned

• **Strategic priority** tackling fakeness in the .nz domain name space

• **Issuing joint consumer factsheets with other experts** to educate consumers about online issues in the .nz domain name space. For example, we have a fact sheet on privacy and domains with the Privacy Commissioner

• Monitoring and improving our **threat intelligence feeds** from trusted notifiers

• Engaging with the **New Zealand Government’s 2018 review of its Cyber Security strategy** and the Commerce Commission of New Zealand’s **review in to online shopping**.

• An InternetNZ group-convoked multi-stakeholder **one day domain name abuse forum held on Tuesday 27 November 2018 in Wellington**. Key theme approaches to domain name takedowns, in what circumstances and with what protections.

• Working with the local Internet community and InternetNZ to **modernise the way domain name disputes are dealt with in the .nz domain name space**, to ensure effective and efficient access to justice.

• **Sponsor and member of Internet and Jurisdiction Domains and Jurisdiction Track - participants of Working groups on Taxonomies and Transparency reporting - tackling cross jurisdictional domain name abuse**
## Resources – happy to share

<table>
<thead>
<tr>
<th>Process/Form/Document</th>
<th>Description: Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memorandum of Understanding template</td>
<td>Used for strategic partnerships, for example, agreement with Cyber Emergency Response Team</td>
</tr>
<tr>
<td>Invalid Registration Details Process - process map</td>
<td>Process for cancelling domain names under .nz policy</td>
</tr>
<tr>
<td>Request for Disclosure under one of the exceptions in the Privacy Act 1993 Principle 11</td>
<td>Types and level of information law enforcement need to demonstrate to permit the Domain Name Commission to make an authorised disclosure of registrant personal information</td>
</tr>
<tr>
<td>Named second defendant in High Court Court Order - template</td>
<td>Draft Order where in disputes involving domains in the High Court of New Zealand the Commission can be named as a second defendant and ordered to lock, cancel or transfer a domain name</td>
</tr>
<tr>
<td>Member of Fraud Investigators and Dispute Investigators Group</td>
<td>Government, Industry, technical operators, law enforcement, consumer protection Information sharing network locally in relation to fraud prevention, consumer protection, compliance and dispute matters.</td>
</tr>
<tr>
<td>Domestication of international court orders - letters</td>
<td>Legal proforma letter explaining process in New Zealand to domesticate international court orders</td>
</tr>
<tr>
<td>Transparency Reporting - template</td>
<td>Information required to report publicly when withheld data accessed eg. Number of push backs, types of enquiry, time taken to notify registrant</td>
</tr>
<tr>
<td>Whitelisting agreement</td>
<td>Agreement to whitelist limited IP addresses to perform WHOIS searches without the need to enter a RECAPTCHA on the .nz data query service on the Commission’s website.</td>
</tr>
</tbody>
</table>


Finally...call to action

• The more CCTLD operators take seriously their data quality obligations — the better their space and the spaces around them will become.

• Remember opening philosophy — CCTLD operators can’t police the whole Internet but in a multi-stakeholder model have a part to play in ensuring the quality, security and stability of the domain name system.
Questions?

0800 101 151
info@dnc.org.nz