

# Trust in the .nz domain name space

Transparency  
annual report  
2018/19

DOMAIN NAME  
COMMISSION 

# Trust in the .nz domain namespace

## Transparency annual report 2018/19

### Outline of the report

This transparency report details:

- Emerging privacy, safety and security trends in the .nz domain namespace
- The statistics
  - Number of .nz registrants who have chosen the individual registrant privacy option
  - Summary of enquiries
    - Government agency enquiries
    - New Zealand Police enquiries
    - MoU holder enquiries
    - Frequency
  - Push backs (local) and international (court orders from foreign jurisdictions)
- Requests for access to the zone file
- Releases to the individual concerned and individuals resolving disputes through the Domain Name Commission
- Domain name suspensions/ cancellations
  - Invalid details
  - Systemic investigations
  - Emergency or exceptional powers
  - Court orders
- Changes to our privacy policy/statement – General Data Protection Regulation (GDPR).

### Introduction

Privacy, trust, and security have been three themes keeping stakeholders in the .nz domain name space and staff at the Domain Name Commission busy this past year.

This is our first annual transparency report which we are committing to producing each May to coincide with Privacy Week - New Zealand's focus on privacy issues. Our first report outlines our activities for the past 14 months. The extra couple of months of reporting is because of responding to the Christchurch events and wanting to include some details of what we did in this report.

## Emerging privacy, safety, and security trends in the .nz domain namespace

### The individual registrant privacy option

In March 2018, we saw the introduction of our individual registrant privacy option. Registrants have embraced this option to not publish their phone number and address as part of a record from a .nz query search.

Registrars still collect these details, and the registry holds this, but their name and email addresses are not returned as part of a .nz query service. A separate process to access this withheld information from the Commission exists for our trusted notifier CERTNZ.

## The GDPR

The General Data Protection Regulation came into force on 25 May 2018. We updated our contracts with Registrars throughout the 2018/19 financial year. As both a controller and processor of European citizens data, the Commission and .nz authorised Registrars who sell .nz domain names to European citizens now have GDPR obligations.

## Domain Name Commission v Domain Tools

In a hard-fought action to protect the privacy rights of .nz registrants, we took on US company Domain Tools who had been collecting and storing registrant's personal information for years in defiance of our new individual registrant privacy option. In September 2018 we won a preliminary injunction in the Washington District Court for breach of contract. We are defending that case on appeal to the Washington Ninth Circuit which will be heard on 6 June 2019.

## Domain Name Abuse Forum

The Commission, together with InternetNZ convened New Zealand's first Domain Name Abuse forum in November 2018. A wide variety of stakeholders from across government, academia, civil society, and Member organisations contributed to discussions and working sessions that aimed to identify the issues surrounding domain name abuse. Many of the issues identified had a privacy flavour, including:

- bad actors using privacy to mask their contact details,
- anonymity and whether it should be permissible for domain name registration,
- data quality, in particular keeping contact details accurate and steps to validate details at the time of registration
- data retention around the history of domain name registration
- information matching and data sharing to assist law enforcement and
- transparency reporting for decision-making where registrant's privacy may be impacted.

The outcomes from the day have been captured in a series of [infographics](#), and several suggestions have formed the basis for internal continuous improvement projects. The ideas will also be shared with the independent Advisory panel that is reviewing .nz policy in the 2019/2020 financial year.

## Memorandum of Understandings regarding data sharing

In this reporting period, the Commission has signed two Memorandum of Understandings with government agencies. These MOUs are with the Cyber Emergency Response Team (CERTNZ) and the Digital Safety division of the Department of Internal Affairs (DIA).

Both MOUs feature provisions about what types of personal information will be shared and in what circumstances. In the case of CERTNZ, data may be shared in the public interest to minimise infrastructure abuse harms, including vital infrastructure such as the domain name system. When it comes, DIA, personal information may be exchanged to assist with an investigation, enforcement, and removal of objectionable material.

The MOUs include necessary provisions to ensure legally required safeguards such as compliance with the *Privacy Act 1993*. Copies of the MOUs are published on the Commission's [website](#).

## Christchurch terrorism events

On 15 March 2019, Christchurch suffered the worst terrorist attack in New Zealand. The Commission moved quickly to monitor the .nz domain name space on behalf of our MoU partner DIA, for the emergence of any terrorism-related objectionable material associated with the event and a .nz domain name space.

The Commission operated under a temporary policy arrangement ahead of interim changes to .nz policy. As part of that temporary arrangement, the Commissioner sought to act on any requests from Memorandum of Understanding partners CERTNZ and the DIA to take down .nz domain names linked to objectionable material about the Christchurch events.

The decision mentioned above slightly delayed the publication of our first annual transparency report, but in light of the circumstances was unavoidable. The decision has led to a complete summary of where we have taken action to balance the free flow of information to support the .nz domain space with respect for individual privacy and security.

We also intend to commit to a future publishing date during New Zealand privacy week in May of each year.

### Reform of the Privacy Act

This year saw the Privacy Bill head to the Select Committee.

We support the modernisation of the Privacy Act and are looking forward to the Bill becoming law. While we would have liked to have seen the Bill go further with harmonisation with GDPR requirements, we see no reason for further delays.

## The Stats

*The Number of .nz registrants who have chosen the individual registrant privacy option.*

As of 23 April 2019 there were 257,161 individuals, natural persons, who held a .nz domain name. Of these, 35,005 had chosen to flag their domains with privacy.

### Summary of enquiries

This report relates to requests for, or releases of, .nz registrant's personal information to third parties between 28 March 2018 and 9 May 2019. It also contains information about where we have exercised our discretion to cancel domain names either proactively or as a result of reports from the general public.

The total number of requests for access to personal information by agency type is set out in Table A below.

**Table A: No of requests from agencies for access to personal information**

Agency	Requests	Number of domains flagged with privacy	Disclosures
Commerce Commission	1	1	0
New Zealand Police	0	0	0
Ministry of Health	1	0	0
CERTNZ (MoU holder)	0	0	0
Department of Internal Affairs Digital Safety Branch (MoU holder)	1	0	1

### Push backs

We work with agencies with their requests for personal information related to current and historical domain name registration records.

We only disclose personal information under Principle 11 of the Privacy Act 1993 where in our judgment, an exception applies.

Where agencies ask for personal information, we consider whether the request can be met by helping the agency access already publicly available information contained in the search results of a .nz data query.

Where that does not satisfy a request, we check whether the information requested matches the reason for the request.

This year we discussed one request with the Commerce Commission and one with the Department of Health to understand their requirements.

We were able to assist them with their enquiries without the need to disclose any personal information.

#### *Requests for access to the zone file*

Sometimes individuals and organisations ask for access to the .nz zone files which contain information about domain names that are active in the .nz domain name space. The .nz zone file includes personal information contained in the current domain name registration record. Typically, these types of requests are by local and international researchers performing research into the .nz domain name space.

Principle 11(h) of the Privacy Act permits disclosures of information where information is to be used in a de-identifiable form, and the published format is not or cannot reasonably be expected to identify the individual concerned.

While we can rely on this exception, in the .nz domain name space under .nz policy framework, there is a prescribed process for gaining access to zone file data.

Access to the .nz zone data is only granted where it can be demonstrated that an exceptional reason exists and there is a "public good" aspect to the release of the information that outweighs the privacy concerns of .nz registrants.

Between 28 March 2018 and 10 May 2019, the Domain Name Commission received six requests for zone file data. The Commission granted none of these requests.

### **Warrants and court orders served on us**

We are required to share information with government agencies when:

- we are served with a court-issued warrant or production order
- the government agency is using a power given to them by law, for example, section 17 of the Tax Administration Act 1994 (which requires information to be disclosed when requested).

From 1 March 2018 to 31 May 2019, the Domain Name Commission was not served with any warrants or production orders.

The Ministry of Health did write to the Commission exercising its statutory powers concerning the enforcement of section 63 of the Medicines Act. However, upon further clarification with the Ministry, no disclosure of personal information was deemed necessary.

## Requests from overseas for domain name takedowns based on international jurisdictions

We are including in our transparency reporting the number of requests we push back from international jurisdictions to take down domain names based on overseas court orders that have not been localised.

While it creates work for Commission staff to respond to international customer requests, it is an integral part of what we do to uphold the rule of law and natural justice and procedural fairness for New Zealand based domain name holders.

In 2018/2019, we received two domain name takedown requests from the US and European jurisdictions.

No requestor from either of these international jurisdictions in the 2018/19 year localised their court orders.

## Domain name takedowns

Principle eight of the Privacy Act requires agencies that hold personal information to take steps, if any, to have regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant and not misleading.

An essential part of the domain name system is that people registering a domain name are who they say they are and are contactable at the details provided in the domain name registration record.

The Domain Name Commission this year took steps to validate registrant (domain name holders) contact details contained in the domain name registration record. Registrants are required to be contactable at their registration details on record.

This process involved contacting the registrant of a .nz domain name using the details listed on the registration record. The registrant was asked to validate the contact details, to prove they are contactable on the details listed.

As a result of our data quality efforts regarding fake contact details, 597 domain names were cancelled.

### *Systemic investigations*

We also saw an increase in domain name cancellations by .nz authorised Registrars as a result of two systemic investigations we conducted. Both investigations concerned the accuracy of the domain name registration record. A total of 4,979 number of domains were suspended from these initiatives.

### *Emergency or exceptional powers*

Following the Christchurch terrorist attacks, the Domain Name Commission took and explained emergency steps to allow for the suspension of .nz domains that are used to share or disseminate objectionable terrorist material.

As part of exercising those extraordinary powers, the Commissioner proposed that whenever those powers were to be used that the public is informed by way of transparency reporting.

The Commissioner did have to exercise this discretionary power and suspended one .nz domain during the period where the National Threat Level was at high.

That case involved liaising with a third-party provider, the registrant, the Department of Internal Affairs and New Zealand Police. It related to a request by the Department of Internal

Affairs to suspend a domain name that had been hijacked, and the domain name was displaying objectionable terrorism-related material. The domain name was suspended for less than 24 hours and was reinstated once that material had been removed. The domain name remains active, and the registrant of the domain name assisted throughout the process.

#### *Court ordered takedowns*

Sometimes members of the public or organisations name the Domain Name Commission as a second respondent in legal proceedings. Typically, the Domain Name Commission is named to assist with domain name takedowns and may have to disclose information to support the Court.

In April 2019, we were named as a second respondent about legal proceedings related to a Harmful Digital Communication Order. We filed a Memorandum agreeing to abide by any order of the Court.

#### **Changes to the DNCL privacy statement**

Our privacy statement is how we communicate with the public about the way we approach our privacy obligations.

In May 2018 and May 2019, we changed our privacy statement to incorporate requirements of the European General Data Protection Regulation.

Our revised privacy statement is available at <https://dnc.org.nz/privacy-statement>

#### **Privacy resources the Commission has authored over the period:**

Amended .nz Registrar authorisation agreement ( GDPR)

[https://dnc.org.nz/sites/default/files/2018-05/registrar\\_authorisation\\_agreement\\_v5.2\\_4.pdf](https://dnc.org.nz/sites/default/files/2018-05/registrar_authorisation_agreement_v5.2_4.pdf)

Being privacy conscious with domain name registrations, Joint publication with the Office of the Privacy Commissioner <https://dnc.org.nz/sites/default/files/2018-05/Domain%20Name%20Commission%20and%20Office%20of%20the%20Privacy%20Commissioner%20joint%20privacy%20fact%20sheet%20.pdf>

Safer Online shopping if it seems too good to be true, it probably is Joint publication with CERTNZ [https://dnc.org.nz/sites/default/files/2018-11/Safer\\_online\\_shopping.pdf](https://dnc.org.nz/sites/default/files/2018-11/Safer_online_shopping.pdf)

DNCL wins the first step in lawsuit against US Company <https://dnc.org.nz/index.php/the-commission/news/1738>

Emergency Response to the Christchurch terrorism attacks

<https://dnc.org.nz/index.php/christchurchterroristattackresponse>