Which Authors of ICANN Documentary Information Disclosure Policy Requests Are Likely to Receive Defined Conditions of Non-Disclosure in ICANN's Response?

Sarah Clayton

University of Southern California

Draft paper to be presented at XXXVI Sunbelt Social Networks Conference of the International Network for Social Network Analysis (INSNA),

5-10 April 2016, in Newport Beach, California.

Abstract

Most homophily studies have focused on individuals, rather than organisations. Research has demonstrated that homophily patterns increase as the number of distinct relationships between two individuals increase; hence, there's more homophily in multiplex networks than simplex networks. The Internet Corporation for Assigned Names and Numbers (ICANN) passed the Documentary Information Disclosure Policy (DIDP), its version of the the Freedom of Information Act, in February 2008, to "ensure that information contained in documents concerning ICANN's operational activities, and within ICANN's possession, custody, or control, are made available to the public unless there is a compelling reason for confidentiality" (ICANN, 2008). ICANN must respond to DIDP requests within 30 days and information and documents may be withheld if the requested information falls under one or more of ICANN-identified 12 Defined Conditions of Non-Disclosure (DCND). These essentially provide an administrative loophole for ICANN to restrict the free flow of information.

The present research examines status homophily in relation to DCND cited by ICANN in response to DIDP requests from organisations and individuals. It compares the 91 DIDP requests, submitted to ICANN between September 2008 and September 2015, to the DCND invoked in their responses in relation to the attributes of each request, including organisation type (e.g. internet non-profit) and word count. Shared DCND (edges) connect the 91 DIDP Request IDs (nodes). As it is not possible to fit an exponential random graph model (ERGM) to a multiplex network in R, undirected, unidimensional networks are constructed for four separate categories of DCND: Affect Individual, Burdensome, Compromise ICANN Integrity, and Confidential External Business Information. Statistical p* models demonstrate that lengthier DIDP requests tend to receive greater numbers of DCND, which implies that longer submissions ask for what ICANN considers as contentious

information. ICANN stakeholder groups/working groups are more likely to receive conditions in every condition category, except Affect Individual, which suggests they request quite sensitive and/or contentious information. It is rare for Burdensome conditions to be imposed on law firms, as they have a tendency to request precise information in relation to a specific case, rather than excessive or unreasonable quantities of information. Registrants are less likely to receive ICANN Integrity conditions as they are more concerned about their own domain name registrations than the inner-workings of ICANN. Further, Confidential External Business Information conditions are less likely to be imposed on internet non-profits, as they tend to be interested in ICANN's interface with internet governance and other related concerns, over third-party business interests. Altogether, the results support the idea that DIDP requests with a higher word count receive more DCND, and in many cases individuals and organisations that fall into the same category/industry sector receive similar DCND. The findings have implications for prospective DIDP requesters and enhancing ICANN's transparency and accountability processes.

Keywords: homophily, ICANN, DIDP, freedom of information

Introduction

The Internet Corporation for Assigned Names and Numbers (ICANN) passed the Documentary Information Disclosure Policy (DIDP), its version of the the Freedom of Information Act, in February 2008, to "ensure that information contained in documents concerning ICANN's operational activities, and within ICANN's possession, custody, or control, are made available to the public unless there is a compelling reason for confidentiality" (ICANN, 2008). It is one of ICANN's many mechanisms to meet accountability and transparency obligations set forth in Article 7 of the Affirmation of Commitments, Article 4 of its Articles of Incorporation, and Article 1, Section 2(7) of its Bylaws.

ICANN must respond to DIDP requests within 30 days and information and documents may be withheld if the requested information falls under one or more of ICANN-identified 12 Defined Conditions of Non-Disclosure (DCND). These essentially provide an administrative loophole for ICANN to restrict the free flow of information. Between September 2008 and September 2015, DCND have been invoked in 65 of the 91 [more than two-thirds of] DIDP request responses. By concealing information, ICANN can shield incompetence or misconduct, especially as there is inadequate means of independent appeal – only the ICANN reconsideration process, which is not independent of the ICANN Board. The DIDP is meant to enhance public transparency, in line with ICANN's commitment to accountability and transparency, which ICANN states as being paramount to "ensuring that its international, bottom-up and multi-stakeholder operating model remains effective" (ICANN, 2014). The DIDP, as it stands, it not providing proper transparency, as so many requests are partially or fully rejected - as evidenced by the number of DCND cited in ICANN's responses. It's therefore essential that the DIDP and its obstructive DCND are reformed to provide meaningful transparency within the organisation.

In lieu of literature concerning ICANN's DIDP specifically, I review access to information laws enacted by national governments. While ICANN is a private non-profit organisation and not an elected government, it does exercise ample regulatory authority over the technical management of the internet and protecting trademark rights in domain names. Further, in recent years, it has become a monolith for internet governance-related debates. Akin to a democratically elected government, ICANN owes stakeholders within the ICANN community the right to access a comparable degree of information, documents and records.

In this paper, I compare ICANN requests to the DCND invoked in their responses in relation to the attributes of each request, including organisation affiliation category (e.g. internet non-profit) and word count. I hypothesise that individuals and organisations that fall into the same category / industry sector will receive similar DCND. Further, DIDP requests with a higher word count will receive more DCND, than DIDP requests with a lower word count.

Background

In its seventeen-year history *Internet Corporation for Assigned Names and Numbers* (ICANN) has considerably grown in scope and size. Headquartered in Playa Vista, Los Angeles, California, it was selected by the US Department of Commerce and formed in 1998 to implement the guidelines issued in the *National Telecommunications and Information Administration* (NTIA) White Paper: *Management of Internet Names and Addresses* (1998). What was once a relatively small organisation for merely coordinating the technical management of the internet's naming and addressing system, and protecting trademark rights (via the Uniform Domain Name Dispute Resolution Policy: UDRP), has, in addition to the aforementioned duties, become a monolith for internet governance-related debates.

The United States is preparing to hand over the keys to the internet. In March 2014, the NTIA, which currently oversees ICANN's performance of the *Internet Assigned Numbers Authority* (IANA) functions, announced its intent to transition the management of the IANA functions to the global multi-stakeholder community (NTIA, 2014). These functions include IP address allocation, Domain Name System (DNS) root zone management, and protocol parameters registry maintenance. In addition, ICANN has been responsible for expanding the domain name system, adding hundreds of new Generic Top Level Domains (gTLDs) to the root zone. Organisations paid $185,000 to simply apply to launch a registry to operate a new gTLD, such as .google; .bank; and .london, and ICANN received 1,930 applications for a total of 1,409 unique strings. Auctions were held in instances where there were multiple applicants for the same string and through its "auction of last resort" ICANN made in excess of $58 million (ICANN, 2015). ICANN has been criticised for multiple failures over its handling of the process. For example, trademark owners have spoken out regarding the .sucks perceived predatory pricing model (IPC, 2015) and the .amazon objection lead by Brazil and Peru - especially as neither country holds any legally recognised rights, let alone trademark rights (Forbes & DelBene, 2015). Decisions concerning how the new gTLD cash should be spent, the management of the IANA transition process, and ICANN's increasingly important policy-making role, highlight the need for effective accountability within the organisation.

ICANN has multiple mechanisms to meet accountability and transparency obligations set forth in Article 7 of the Affirmation of Commitments, Article 4 of its Articles of Incorporation, and Article 1, Section 2(7) of its Bylaws, namely the: Independent Review Process (IRP); Request for Reconsideration (RR); Documentary Information Disclosure Policy (DIDP); and Ombudsman. These processes within the wider ICANN structure have been described as having "serious deficiencies" (Weber & Gunnarson, 2012).

While the DIDP was under development, ICANN community members criticised it, as being contrary to ICANN's Bylaws and for being published without a formal policy development process (Hasbrouck, 2007). Today, the process is under more scrutiny. After seven years of operation, the DIDP has not realised its advocates' modest objectives. Members of the Cross Community Working Group on Enhancing ICANN Accountability (CCWG-Accountability) are proposing DIDP reforms as part of Workstream 2 (WS2). WS2 is the second stage of the team's work on enhancing ICANN's transparency and accountability processes in preparation for transitioning the management of the IANA functions away from the U.S. Government, to the global multi-stakeholder community (NTIA, 2014). WS2 is "focused on addressing accountability topics for which a timeline for developing solutions and full implementation may extend beyond the IANA Stewardship Transition" (Rickert, et al., 2015).

It has been recommended that the DIDP should be brought into line with mechanisms found in comparable international organisations. Further, the DCND should be worded "as narrowly as possible"; however, as many of the conditions applied in the DIDP are overbroad, and ICANN has wide discretion to deny requests (Karanicolas, 2015).

A similar mechanism: The Freedom of Information Act

The existence of exemptions, or conditions of non-disclosure, is central to any freedom of information regime (Birkinshaw, 2010). A public interest test determines whether information is released or retained if an exemption applies. The Freedom of Information Act (FOIA) of 1966 afforded public access to information unless it fell into one of nine exemption categories. These exemptions protected three sets of interests: personal privacy interests, business interests, and government interests (Metcalfe, 2014). In response to the Watergate scandal (Congressional Quarterly, 1999), the FOIA was strengthened in 1974 and the scope of the exemptions narrowed.

Like ICANN's DIDP, the FOIA has faced harsh criticism over the years. Prior to its 1974 reform, the exemptions embodied within FOIA enabled reluctant federal officials to avoid disclosing information (Davis, 1967; Katz, 1970).In amending the act, the Senate Report explained that the exemptions were permissive rather than mandatory:

> *Congress did not intend the exemptions in the FOIA to be used either to prohibit disclosure of information or to justify automatic withholding of information. Rather, they are only permissive. They merely mark the outer limits of information that may be withheld where the agency makes a specific affirmative determination that the public interest and the specific circumstances presented dictate- as well as that the intent of the exemption allows- that the information should be withheld* (93rd Congress., 2nd Session).

Unfortunately, much of the critical commentary pertaining to ICANN's DIDP suggests that ICANN uses its DCND as mandatory, rather than permissive, exemptions (Karanicolas, 2015).

My Approach

Establishing which requests are most likely to receive any or specific categories of DCND requires statistical analysis. The 91 DIDP requests submitted to ICANN between September 2008 and September 2015 can be connected by their shared DCND provided in ICANN's response, in a multiplex network. Multiplex networks have one node type, but multiple types of relations (Wasserman & Faust, 1994). The homophily mechanism for producing a network tie principally relies on the correlation of characteristics or exogenous attributes of nodes in a network (Monge & Contractor, 2003, p. 303). Thus, homophily may be able to predict the likelihood of a DCND relation between requests. The more analogous one node is to another and the higher degree of the target node, the greater the probability of

forming a tie (Şimşek & Jensen, 2008). Lazarsfeld and Merton (1954) defined two homophily classifications: status homophily and value homophily. Status homophily concerns characteristics, such as occupation, values, attitudes, and beliefs, whereas value homophily is based on internal states which may shape future behaviour. Fischer (1982) demonstrated that homophily patterns increase as the number of distinct relationships between two individuals increase; hence, there's more homophily in multiplex networks than simplex networks. Most homophily studies focus on individuals, rather than organisations (McPherson, Smith-Lovin & Cook, 2001; Haas & Hansen, 2007). As this paper concerns requests for information, I will focus on status homophily, as the type of individual or organisation sending the request may influence both the content of the request and also the response to the request. Here, my argument assumes that DIDP requests from individuals and organisations in the same category, e.g. ICANN Working Group, are more likely to receive similar DCND, as they may ask for similar information, or equivalently complex information.

H1. Individuals and organisations that fall into the same category / industry sector, e.g. internet non-profit will receive similar DCND.

A higher word count may indicate that the request includes more detail and complexity. The requester may be seeking information about potentially contentious or sensitive topics, or simply requesting a greater quantity of information. Asking for more information may increase the probability of receiving DCND. Status homophily also applies here, as the characteristics of the request's word count (high/medium/low) may impact the number of DCND ICANN imposes.

H2. DIDP requests with a higher word count will receive more DCND, than DIDP requests with a lower word count.

Method

To test these hypotheses, I manually collected data from ICANN's Documentary Information Disclosure Policy requests and responses from September 24, 2008 to September 1, 2015. They are freely available on ICANN's website at: https://www.icann.org/resources/pages/governance/transparency-en. I collected Request IDs; Name of requester; Request Date; [ICANN's] Response Date; Affiliation in Request (organisation making the request); Category (type of organisation making the request); and Word Count [of request]. I also noted the Defined Conditions of Nondisclosure cited in ICANN's response to each request.

ICANN's defined conditions of non-disclosure are:

a. Information provided by or to a government or international organization, or any form of recitation of such information, in the expectation that the information will be kept confidential and/or would or likely would materially prejudice ICANN's relationship with that party.

b. Internal information that, if disclosed, would or would be likely to compromise the integrity of ICANN's deliberative and decision-making process by inhibiting the candid exchange of ideas and communications, including internal documents, memoranda, and other similar communications to or from ICANN Directors, ICANN Directors' Advisors, ICANN staff, ICANN consultants, ICANN contractors, and ICANN agents.

c. Information exchanged, prepared for, or derived from the deliberative and decision-making process between ICANN, its constituents, and/or other entities with which ICANN cooperates that, if disclosed, would or would be likely to compromise the integrity of the deliberative and decision-making process between and among

ICANN, its constituents, and/or other entities with which ICANN cooperates by inhibiting the candid exchange of ideas and communications.

d. Personnel, medical, contractual, remuneration, and similar records relating to an individual's personal information, when the disclosure of such information would or likely would constitute an invasion of personal privacy, as well as proceedings of internal appeal mechanisms and investigations.

e. Information provided to ICANN by a party that, if disclosed, would or would be likely to materially prejudice the commercial interests, financial interests, and/or competitive position of such party or was provided to ICANN pursuant to a nondisclosure agreement or nondisclosure provision within an agreement.

f. Confidential business information and/or internal policies and procedures.

g. Information that, if disclosed, would or would be likely to endanger the life, health, or safety of any individual or materially prejudice the administration of justice.

h. Information subject to the attorney– client, attorney work product privilege, or any other applicable privilege, or disclosure of which might prejudice any internal, governmental, or legal investigation.

i. Drafts of all correspondence, reports, documents, agreements, contracts, emails, or any other forms of communication.

j. Information that relates in any way to the security and stability of the Internet, including the operation of the L Root or any changes, modifications, or additions to the root zone.

k. Trade secrets and commercial and financial information not publicly disclosed by ICANN.

l. Information requests: (i) which are not reasonable; (ii) which are excessive or overly burdensome; (iii) complying with which is not feasible; or (iv) are made with an abusive or vexatious purpose or by a vexatious or querulous individual.

For simplicity's sake, I shortened the labels of the aforementioned DCND:

a. Confidential government information
b. Internal information
c. Compromise decision-making process between ICANN and others
d. Personal information
e. Prejudice commercial interests
f. Confidential business information
g. Endanger the life, health, or safety of any individual
h. Attorney-client / attorney-work product privilege
i. Drafts of all correspondence, reports, documents, etc.
j. Internet security and stability
k. Trade secrets
l. Not reasonable / excessive / not feasible / abusive

I recorded the data in two CSV files. One file contained the Request IDs (nodes) and their attributes. The second file contained the DCND (edges) for each Request ID. To visualise the data, I imported the CSV files to the igraph network analysis package in R. I first developed an undirected multiplex network, which comprised 91 Request IDs (nodes) that were connected by shared DCND (undirected edges). Name of Requester, Request Date, Response Date, Affiliation in Request, Category, and Word Count were attributes assigned to each request. As it is not possible to fit an exponential random graph model (ERGM) to a multiplex network in R, I next split the DCND into four categories, and created an undirected, unidimensional network for each category. Only eight requests from six

organisation types received “j. Internet security and stability” in ICANN’s response. Due to a large range of organisation types receiving the internet security DCND, and the fact that it did not easily fit into any group, no further analysis on the condition was conducted.

Grouped DCND were as follows:

1. Affect Individual
2. Burdensome
3. Compromise ICANN Integrity
4. Confidential External Business Information

Affect Individual included:

d. Personal information

g. Endanger the life, health, or safety of any individual

Burdensome included:

i. Drafts of all correspondence, reports, documents, etc.

l. Not reasonable / excessive / not feasible / abusive

Compromise ICANN Integrity included:

b. Internal information

c. Compromise decision-making process between ICANN and others

f. Confidential business information

Confidential External Business Information included:

a. Confidential government information

e. Prejudice commercial interests

h. Attorney-client / attorney-work product privilege

k. Trade secrets

I used the statnet statistical analysis package in R to fit ERGMs (p* models) to the dataset, to predict the likelihood of a condition existing between two DIDP requests. I used three different ERGM functions: absdiff, nodecov, and nodematch. Absdiff was used to see whether a DCND was expected to exist as the difference between word count increased between two requests. Nodecov was used to see whether a request was more or less likely to receive a DCND as word count increased. Nodematch was used to see whether requests made by similar individuals or organisations were likely to receive a DCND.

Results

The undirected multiplex network comprised 91 requests and 3453 edges. There were 26 isolates with no DCND from nine categories of request affiliation: 9x Internet Non-Profit (33%); 3x Law Firm / Plaintiff (23.8%); 4x Journalist (50%); 3x Registrant (37.5%); 1x ICANN Stockholder Group / Working Group (12.5%); 2x Trade Association (28.57%); 1x Registry / New gTLD Applicant (20%); 2x Internet Consultancy Firm (40%); and 1x Not Known (16.67%). Percentages are relative to the number of Request IDs in each affiliation category. Of the requests that received DCND, ten received condition a.; 38 received condition b.; 31 received condition c.; six received condition d.; 34 received condition e.; 36 received condition f.; one received condition g.; 22 received condition h.; 31 received condition i.; eight received condition j.; 12 received condition k.; and 18 received condition l.

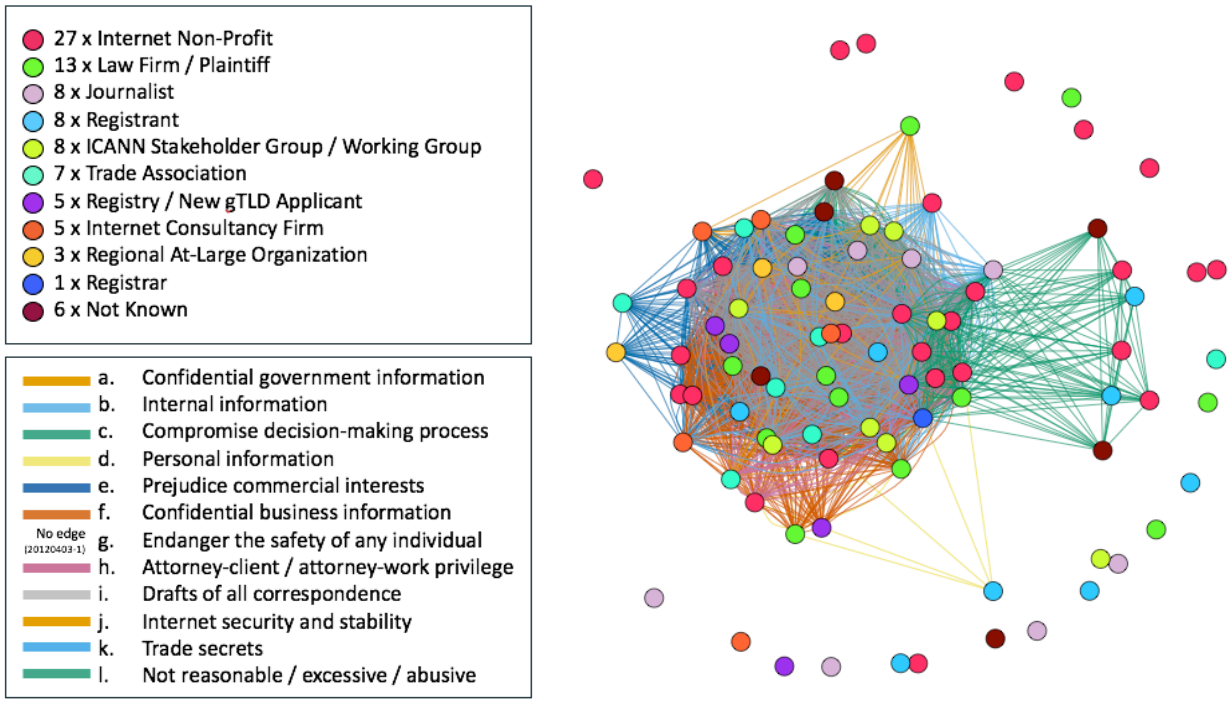

Figure 1 Visualisation of overall network.

A multiplex graph of the shared DCND between DIDP requests.

The individual, undirected, unidimensional networks for each DCND group facilitated hypothesis testing. I found some evidence for H1 that individuals and organisations, which fell into the same category/industry sector, would receive similar DCND. The hypothesis was proven for some affiliation categories, but not others. The affect individual DCND were not statistically significant for any affiliation category. ICANN Stakeholder Groups / Working Groups were more likely to receive Burdensome DCND, whereas law firms / plaintiffs were less likely to receive Burdensome DCND. The Burdensome DCND were not statistically significant for any other affiliation category. ICANN Stakeholder Groups / Working Groups were more likely to receive compromise ICANN Integrity DCND, whereas registrants were less likely to receive compromise ICANN Integrity DCND. The compromise ICANN Integrity DCND were not statistically significant for any other affiliation category. ICANN Stakeholder Groups / Working Groups were more likely to receive confidential, external

business information DCND, whereas internet non-profits were less likely to receive confidential, external business information DCND. The confidential, external business information DCND were not statistically significant for any other affiliation category.

I also found evidence for H2 that DIDP requests with a higher word count would receive more DCND, than DIDP requests with a lower word count. This hypothesis was proven as the nodecov test was statistically significant across all four networks. The absdiff test was statistically significant in all networks apart from the affect individual network. This meant that a DCND was expected to exist as the difference between word counts decreased between two requests in the Burdensome, Compromise ICANN Integrity, and Confidential External Business Information networks.

	Affect Individual		
	Estimate	**Std Error**	**P-value**
Edges	-5.8438381	0.3550127	<0.0001 ***
Absdiff.word.count	-0.0007214	0.0004766	0.1302
Nodecov.word.count	0.0007325	0.0002945	0.0129 *
Nodematch.category			
ICANN Stakeholder Group / Working Group	-Inf	0.0000000	<0.0001 ***
Internet Consultancy Firm	-Inf	0.0000000	<0.0001 ***
Internet Non-Profit	-0.2825324	1.0423642	0.7864
Journalist	-Inf	0.0000000	<0.0001 ***
Law Firm / Plaintiff	-Inf	0.0000000	<0.0001 ***
Not Known	-Inf	0.0000000	<0.0001 ***
Regional At-Large Organization	-Inf	0.0000000	<0.0001 ***
Registrant	-Inf	0.0000000	<0.0001 ***
Registrar	-Inf	0.0000000	<0.0001 ***
Registry / New gTLD Applicant	-Inf	0.0000000	<0.0001 ***
Trade Association	-Inf	0.0000000	<0.0001 ***

Table 1 p*/ERGM Results for network with Affect Individual DCND

	Burdensome		
	Estimate	**Std Error**	**P-value**
Edges	-2.3452261	0.0713213	< 0.0001 ***
Absdiff.word.count	-0.0004322	0.0001192	0.000291 ***
Nodecov.word.count	0.0008265	0.0001041	< 0.0001 ***
Nodematch.category			
ICANN Stakeholder Group / Working Group	2.0432571	0.3862606	< 0.0001 ***
Internet Consultancy Firm	-Inf	0.0000000	<0.0001 ***
Internet Non-Profit	0.1083298	0.1635329	0.507730
Journalist	-1.2803246	1.0198018	0.209382
Law Firm / Plaintiff	-0.9980504	0.3846324	0.009498 **
Not Known	0.3737011	0.7624666	0.624074
Regional At-Large Organization	1.3752830	1.2262259	0.262117
Registrant	-1.3037815	1.0198265	0.201169
Registrar	-Inf	0.0000000	<0.0001 ***
Registry / New gTLD Applicant	0.5951858	0.7300227	0.414950
Trade Association	-Inf	0.0000000	<0.0001 ***

Table 2 p*/ERGM Results for network with Burdensome DCND

	Compromise ICANN Integrity		
	Estimate	**Std Error**	**P-value**
Edges	-1.8008523	0.0648339	<0.0001 ***
Absdiff.word.count	-0.0016290	0.0001488	<0.0001 ***
Nodecov.word.count	0.0019364	0.0001381	<0.0001 ***
Nodematch.category			
ICANN Stakeholder Group / Working Group	1.8257309	0.4150773	<0.0001 ***
Internet Consultancy Firm	-Inf	0.0000000	<0.0001 ***
Internet Non-Profit	-0.1834905	0.1350003	0 0.1742
Journalist	-0.5928745	0.5440639	0.2759
Law Firm / Plaintiff	-0.0176856	0.2750424	0.9487
Not Known	0.2343428	0.6481665	0.7177
Regional At-Large Organization	0.4620778	1.2256604	0.7062
Registrant	-2.2317842	1.0223670	0.0291 *
Registrar	-Inf	0.0000000	<0.0001 ***
Registry / New gTLD Applicant	1.2582114	0.6875455	0 0.0673
Trade Association	-0.1024679	0.5417186	0.8500

Table 3 p*/ERGM Results for network with Compromise ICANN Integrity DCND

	Confidential External Biz Info		
	Estimate	**Std Error**	**P-value**
Edges	-1.8499771	0.0622953	< 0.0001 ***
Absdiff.word.count	-0.0007747	0.0001195	< 0.0001 ***
Nodecov.word.count	0.0010410	0.0001055	< 0.0001 ***
Nodematch.category			
ICANN Stakeholder Group / Working Group	1.8328875	0.3933300	< 0.0001 ***
Internet Consultancy Firm	0.6798189	0.6941035	0.32743
Internet Non-Profit	-0.4493622	0.1622915	0.00565 **
Journalist	-0.6179263	0.6134898	0.31388
Law Firm / Plaintiff	-0.5089013	0.3025035	0.09259
Not Known	-0.8946826	1.0366815	0.38817
Regional At-Large Organization	14.0685039	187.4908159	0.94019
Registrant	-1.8439802	1.0203126	0.07079
Registrar	-Inf	0.0000000	<0.0001 ***
Registry / New gTLD Applicant	0.1932237	0.7342138	0.79243
Trade Association	0.4992087	0.4930464	0.31136

Table 4 p*/ERGM Results for network with

Confidential External Business Information DCND

Discussion

I analysed ICANN's DIDP in relation to DCND assigned to each DIDP request. I hypothesised that individuals and organisations, which fell into the same category / industry sector, would receive similar DCND. I also postulated that DIDP requests with a higher word count would receive more DCND, than DIDP requests with a lower word count. I demonstrated that more DCND were received by requests with a larger word count, while the request affiliation category only had a partial effect on the type of DCND received. Thus, H1 was partially proven, and H2 was fully proven.

Compared to the other networks, the ERGM results from the Affect Individual network were not so enlightening, as the network was a maximum complete subgraph with 85 isolates. Six requests received d. Personal information and only one received g. Endanger the life, health, or safety of any individual. It would be worthwhile reanalysing this category, when more DIDP requests have been submitted to ICANN.

ICANN Stakeholder Groups / Working Groups were more likely to receive conditions in every condition category except Affect Individual. The fact that ICANN Stakeholder Groups / Working Groups were more likely to receive Burdensome, ICANN Integrity, and Confidential External Business Information [the majority of] conditions suggests that their requests were for what ICANN considers as sensitive and/or contentious information. ICANN Stakeholder Groups / Working Groups are heavily embedded within ICANN's day-to-day operations. Four [of the eight overall] requests came from members of the Cross Community Working Group to Develop an IANA Stewardship Transition Proposal on Naming Related Functions (CWG on Stewardship Transition), a group which has been a fundamental cog in the IANA transition wheel. Two requests came from the Non-Commercial Stakeholder Group (NCSG), which is part of the Generic Names Supporting Organisation (GNSO), the policy-making body for gTLDs. The GNSO is the overarching body responsible for the CWG on Stewardship Transition. As the stakeholders and working groups are dealing with the politically sensitive IANA stewardship transition process, they are more likely to be asking for complex and sensitive information pertaining to the transition. Thus, ICANN is more likely to enforce DCND in response to their requests.

Law firms / plaintiffs were less likely to receive Burdensome conditions. This may be because they requested precise information in relation to a specific case that they were working on, and therefore were less likely to ask for excessive or unreasonable quantities of information. As the New gTLD Program has rolled out over the past few years, attorneys of current or would-be registry operators have called some of ICANN's internal policies and procedures into question (e.g. requests 20140904-1; 20140917-1, among others). Rather than requesting burdensome quantities of information, they had a tendency to request specific contracts, agreements, policies, and reports.

Registrants were less likely to receive ICANN Integrity conditions. Registrants may be likely to ask for information pertaining to the inner-workings of ICANN as they may know little about the organisation or the domain name industry in general. Request 20130129-01 from Igor Petrenko exemplifies this observation, who ludicrously asked for "a list of all registered domains". If he had a general understanding of the DNS, he would have known that IANA retains a list of all TLDs, and domain name registrars hold information about second-level domains, through each registrar's WHOIS service. However, contacting each registrar would be an onerous process. Further, registrants were more likely to ask for information concerning their own domain name registrations (e.g. requests 20101108-1; 20150211-1). These requests concerned the application, rather than the development, of ICANN's procedures and policies. As a result, ICANN integrity was less likely to be called into question.

Internet non-profits were less likely to receive Confidential External Business Information conditions. This may be because internet non-profits are more interested in ICANN's interface with internet governance and other related concerns, over third-party business interests. Request 20141228-1 from Geetha Hariharan, on behalf of The Centre for Internet & Society (CIS) supports this suggestion. CIS requested information about several items pertaining to ICANN's interface with the NETmundial Initiative. In fact, CIS submitted two thirds [18 out of 27] of internet non-profit requests, which may have skewed the results. CIS conducts internet policy research and engages in and influences policy debates concerning privacy, freedom of expression, and other civil liberties. These are topics that may be less connected to business trade secrets, the attorney client privilege, commercial interests or government confidentiality.

As measured by word count, the length of a request had a considerable effect on the number and type of DCND received in relation to the request. Lengthier DIDP submissions

may have requested what ICANN would consider as contentious information, and therefore they received greater numbers of DCND. However, delving into the individual requests reveals some conflicting findings. The longest request (20140926-01, 3945 words) came from Bart Lieben, owner of law firm, Bart Lieben BV. The firm asked a number of questions in relation to a decision made by the Community Priority Evaluation panel, which essentially meant Donuts (Tin Dale, LLC), Afilias and BRS Media had to withdraw their gTLD applications to manage .radio. The request received five DCND: all of the DCND in the Compromise ICANN Integrity category, one in the Burdensome category, and one in the Confidential External Business Information category. Considering the length of the request, and the nature of the information sought, I would have expected more conditions from the Confidential External Business Information category. More interesting perhaps was that the Centre for Internet & Society's request (20150901-6) with a relatively low word count (93 words) had the most DCND (nine), obtaining a full house of DCND in every category apart from Affect Individual. They requested a document containing the contents of ICANN's internal website, accessible by ICANN staff. Therefore, even though word count does affect the number of DCND a DIDP request receives, it is not a good predictor for every DIDP request.

Limitations and Future Work

Since September 2015, ICANN has received and responded to six additional DIDP requests. As the network of 91 requests between September 2008 and September 2015 is relatively small, six new requests - an increase of almost 7% - could significantly alter the analysis. Thus, the ERGM tests should be re-run to take these requests into account.

Some requests fitted into multiple affiliation categories. For example, I assigned CORE, Internet Council of Registrars, the Trade Association category, but the organisation was also an Internet Non-Profit. As determining category of affiliation for each request was

not a cut and dry process, I could have assigned multiple affiliation categories to the individual or organisation making the request, rather than just one, so the results were not skewed in favour of one affiliation category over another.

ERGM methods require model specification controls or spurious relationships may be claimed. The ERGMs fit satisfactorily onto the original four networks as they had good geodesic distance. However, they exhibited degeneracy when the ERGMs took isolates into account. This was because the isolates in the actual, unmodeled networks were overrepresented compared to the ERGM simulated networks. Therefore, in order to get even more reasonable approximations of the networks, new models would be required, which take isolates into account.

As the remarkably high number of isolates in each network were ignored in my analysis, future research should consider why these isolates (or requests) did not receive DCND. Twenty-six requests did not receive any DCND whatsoever; 85 did not receive any Affect Individual DCND; 50 did not receive any Burdensome DCND; 40 did not receive any Compromise ICANN Integrity DCND; and 41 did not receive any Confidential External Business Information DCND. Perhaps requests were not subject to certain categories of DCND because they asked for information already made public. At a glance, this theory is certainly applicable to request 20110916-1, for example. Or another reason might be because they asked for DCND category-specific information, such as information about ICANN expenses, which falls into Compromise ICANN Integrity, but not Confidential External Business Information.

Finally, as word count was insufficient to account for the nature of information sought by DIDP requesters, future DIDP researchers should adopt detailed coding schemes to categorise information requested and information provided in ICANN's response in order to produce more generalisable results.

References

93rd Congress., 2nd Session. (1974). Rep. No. 93-854.

Birkinshaw, P. (2010). *Freedom of Information: The Law, the Practice and the Ideal.* New York: Cambridge University Press.

Congressional Quarterly. (1999). *Watergate: Chronology of A Crisis*. CQ Press.

Davis, K.C. (1967). The Information Act: A preliminary analysis. *University of Chicago Law Review, 34*. 761-816.

Fischer, C.S. (1982). *To Dwell among Friends*. Chicago: Univ. Chicago Press.

Forbes, J.R. & DelBene, S. (2015). Letter to ICANN from U.S. Congressional Trademark caucus representatives. Retrieved from: https://www.icann.org/en/system/files/correspondence/forbes-delbene-to-chehade-crocker-19jun15-en.pdf

Haas, M.R., and Hansen, M.T. (2007). Different knowledge, different benefits: Toward a productivity perspective on knowledge sharing in organizations. *Strategic Management Journal, 28*(11), 1133–1153.

Hasbrouck, E. (2007). Omissions from summary of comments, and request for independent review. *Email to ICANN.* Retrieved from: http://forum.icann.org/lists/draft-mop-2007/msg00011.html

ICANN. (2015). New gTLD Auction Proceeds. Retrieved from: http://newgtlds.icann.org/en/applicants/auctions/proceeds

ICANN. (2014). *Accountability.* Retrieved from: https://www.icann.org/resources/accountability

ICANN. (2008). ICANN Accountability and Transparency Frameworks and Principles. *ICANN Management Operating Principles.* Retrieved from: https://www.icann.org/en/system/files/files/acct-trans-frameworks-principles-10jan08-en.pdf

IPC. (2015). ICANN Requested to Immediately Halt .SUCKS Predatory Registration Scheme Designed to Exploit Trademark Owners. Letter to ICANN from the Intellectual Property Constituency. Retrieved from: https://www.icann.org/en/system/files/correspondence/shatan-to-atallah-27mar15-en.pdf

Katz, J.M. (1970). The games bureaucrats play: Hide and seek under the Freedom of Information Act. *Texas Law Review, 43*. 1047-1067.

Karanicolas, M. (2015). DIDP Statement Draft. Cross Community Working Group on Enhancing ICANN's Accountability (CCWG-ACCT). NCSG Email Comm.

Lazarsfeld, P. and Merton, R.K. (1954). Friendship as a social process: A substantive and methodological analysis. In *Freedom and control in modern society*, ed. Morroe Berger, Theodore Abel, and Charles H. Page, 18-66. New York: Van Nostrand.

McPherson, J.M., Smith-Lovin, L., and Cook, J. (2001). Birds of a feather: Homophily in social networks. *Annual Review of Sociology, 27*. 415-444.

Metcalfe, D.J. (2014). The history of government transparency. In P. Ala'a and R.G. Vaughn (Eds.), *Research Handbook on Transparency* (pp. 247-262). Northampton, MA: Edward Elgar.

Monge, P.R. and Contractor, N.S. (2003). *Theories of Communication Networks*. New York: Oxford University Press.

NTIA. (2014). NTIA Announces Intent to Transition Key Internet Domain Name Functions. Retrieved from: http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

NTIA. (1998). Statement of Policy on the Management of Internet Names and Addresses. Retrieved from: http://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-management-internet-names-and-addresses

Rickert, T., Sanchez, L., Weill M. (2015). Cross Community Working Group on Enhancing ICANN Accountability (CCWG-Accountability) | Chairs' Statement. *ICANN.* Retrieved from: https://www.icann.org/news/announcement-2015-01-23-en

Şimşek, Ö. and Jensen D. (2008). Navigating Networks by Using Homophily and Degree. *Proceedings of the National Academy of Sciences of the United States of America, 105*(35). 12758-12762.

Wasserman, S. and Faust, K. (1994). *Social network analysis: Methods and applications.* NewYork: Cambridge University Press.

Weber, R. H., & Gunnarson, R. S. (2012). A Constitutional Solution for Internet Governance. *Columbia Science and Technology Law Review*, 14(1), 1-71.