

ICANN
ANNUAL GENERAL

63

BARCELONA

20–25 October 2018



Whatis Whois

A Brief Introduction

David Conrad

ICANN 63 Barcelona

21 October 2018



A Sample of Email

• Please verify your email address for 913288

• **GoDaddy <info@godaddy.com-verify.name>**

Dear GoDaddy Customer,

ICANN has implemented a new Transfer Policy which aff... email is in response to ICANN's requirement that registr... can read more about this requirement on ICANN's site at <http://www.icann.org/whois/w...>

You have registered one or more domains from Godaddy Inc. and verification of the Reg... to remain active. Please click the link below to verify the email address. If you don't verify... website on hold until verification is complete.*

Please cut-and-paste the following URL into an open web browser to complete the verifi... <http://www.godaddy-verification.com/domains/contact-validation/mailverify/Verification...>

Please remember that under the terms of the registration agreement, providing false WH... domain name registration.

Thanks for your attention to this matter, Please do not reply to this email. Emails sent to... Thanks for being a GoDaddy customer.

Copyright (C)1999-2017 GoDaddy Operating Company, LLC. 14455 N. Hayden Rd, Ste. 2

NETFLIX

Please Update Your Payment Method,

Sorry for the interruption, but we are having trouble authorising your Credit Card.

Please click the link below ↴

Click Here

to enter your payment information again or to use a different payment method.

When you have finished, we will try to verify your account again. If it still does not work, you will want to contact your credit card company.

If you have any questions, we are happy to help. Simply call us at any time on 0800 096 6380.

Questions? [Call 0800 096 6380](tel:08000966380)

This account email has been sent to you as part of your Netflix membership. To change your email preferences at any time, please visit the [Email Preferences](#) page for your account. Please do not reply to this email, as we are unable to respond from this email address. If you need help or would like to contact us, please visit our [Help Centre](#) at help.netflix.com.

-The Netflix Team

SRC: 4304.2.GB.en-GB

From: Amazon <management@amazoncanada.ca> on behalf of Amazon <management@amazoncanada.ca> 5/01/2014 7:55 PM
To: @sheridanc.on.ca
Cc:
Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

amazon.com®

Dear Client, ← Generic non-personalized greeting


We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:

<https://www.amazon.com/exec/obidos/sign-in.html>

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,
The Amazon Associates Team



© 1996-2013, Amazon.com, Inc. or its affiliates

Whois: A Tool to *Help* in Origin Identification

- ⊙ Identifiers on the Internet
 - “Domain Names”: used by people
 - IP Addresses: used by computers
- ⊙ Internet Identifiers are obtained from “Registries”
 - Domain Names via ~2500 *Registrars*
 - GoDaddy, NameCheap, Tucows, etc.
 - Addresses via the 5 *Regional Internet Registries*
 - AfriNIC, APNIC, ARIN, LACNIC, RIPE-NCC
- ⊙ **Registries maintain registration data for Internet Identifiers**

```
Domain Name: BADDAIRY.US
Domain ID: D36067773-US
Sponsoring Registrar: MARKMONITOR, INC.
Registrar URL (registration services): whois.markmonitor.com
Domain Status: clientDeleteProhibited
Domain Status: clientTransferProhibited
Domain Status: clientUpdateProhibited
Registrant ID: MMR-85997
Registrant Name: Domain Administrator
Registrant Organization: DNStination Inc.
Registrant Address1: 303 Second Street
Registrant Address2: Suite 800N
Registrant City: San Francisco
Registrant State/Province: CA
Registrant Postal Code: 94107
Registrant Country: United States
Registrant Country Code: US
Registrant Phone Number: +1.4155319335
Registrant Email: admin@dnstinations.com
Registrant Application Purpose: P1
Registrant Nexus Category: C11
Administrative Contact ID: MMR-85997
```

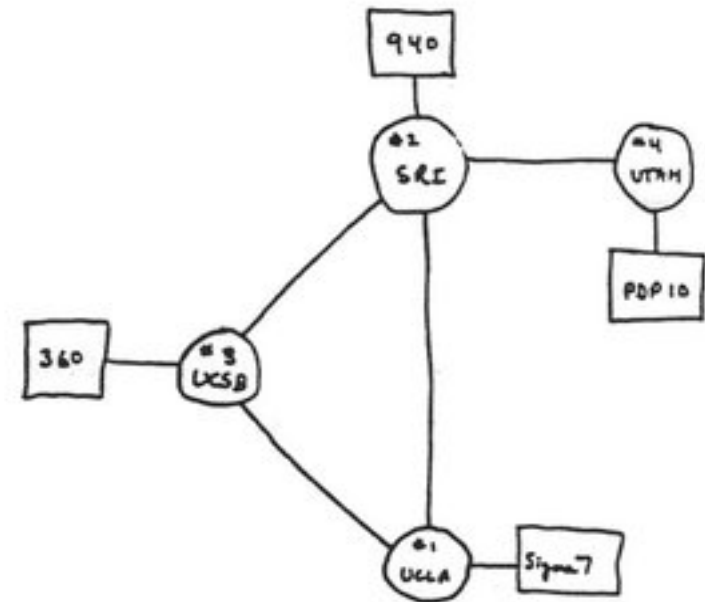
Comparing Registration Data Pre- and Post-GDPR

Domain ID:D2234962-LROR
Domain Name:EFF.ORG
Created On:10-Oct-1990 04:00:00 UTC
Last Updated On:17-Sep-2008 02:53:03 UTC
Expiration Date:09-Oct-2010 04:00:00 UTC
Sponsoring Registrar:Tucows Inc. (R11-LROR)
Status:OK
Registrant ID:tuBWGAuuFhoayNud
Registrant Name:Shari Steele
Registrant Organization:Electronic Frontier Foundation
Registrant Street1:454 Shotwell St.
Registrant Street2:
Registrant Street3:
Registrant City:San Francisco
Registrant State/Province:CA
Registrant Postal Code:94110
Registrant Country:US
Registrant Phone:+141.54369333
Registrant Phone Ext.:
Registrant FAX:
Registrant FAX Ext.:
Registrant Email:whois@eff.org
Admin ID:tuUmXIR7vM5YEXD2
Admin Name:Shari Steele
Admin Organization:Electronic Frontier Foundation
Admin Street1:454 Shotwell St.

Domain Name: EFF.ORG
Registry Domain ID: D2234962-LROR
Registrar WHOIS Server: whois.gandi.net
Registrar URL: http://www.gandi.net
Updated Date: 2018-03-08T02:19:58Z
Creation Date: 1990-10-10T04:00:00Z
Registry Expiry Date: 2022-10-09T04:00:00Z
Registrar Registration Expiration Date:
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Reseller:
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Registrant Organization: Electronic Frontier Foundation
Registrant State/Province: CA
Registrant Country: US
Name Server: NS1.EFF.ORG
Name Server: NS2.EFF.ORG
Name Server: NS4.EFF.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form <https://www.icann.org/wicf/>
Last update of WHOIS database: 2018-09-18T09:01:45Z

Backing up a Bit: Ancient History

- Multi-user mainframes or mini-computers operated by Universities or research institutions interconnected with dedicated telecom lines
 - Researchers all knew each other
 - Knew their telephone numbers and postal addresses
 - Email addresses? What's email?
- Connectivity issues were extremely common
 - Computers, networks, services, etc., all would fall down frequently
 - The fact they were up at all was often a surprise
- “Out of band” communication was a necessity, but easily managed
 - <Ring>
 - “Hi Jon, why is your Sigma 7 system down?”



THE ARPA NETWORK

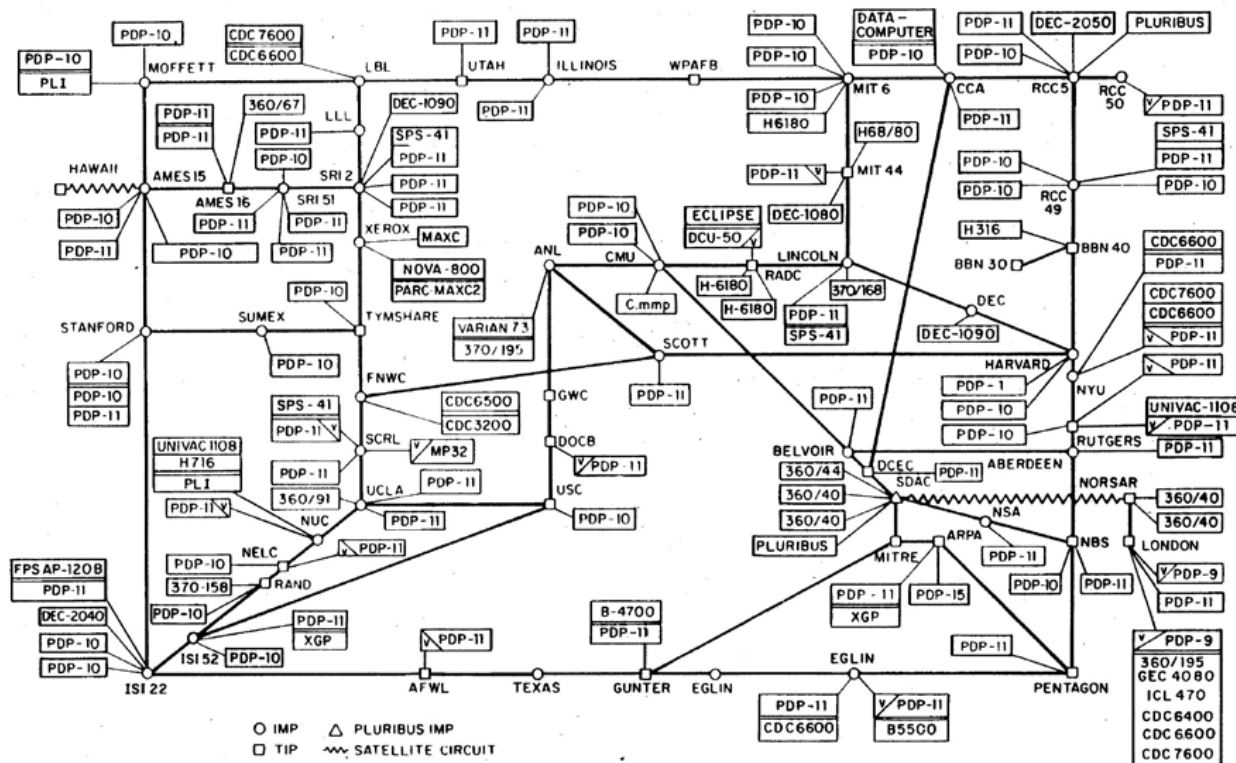
DEC 1969

4 NODES

Slightly Less Ancient History

- Network grows, more nodes
 - Universal knowledge of researchers on the network breaks down
- Connectivity issues still a problem
 - Systems up and down for various reasons
- Devices on the network are numbered with IP addresses and named with “host names”
- Creation of a centralized registry
 - Stanford Research International Network Information Center (SRI-NIC)
- **SRI-NIC created/maintained a “reverse telephone book” that translated IP addresses and host names into the people responsible for the devices named/numbered**
- Network access to this reverse telephone book is via a (extremely simple) protocol named **Whois**

ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

The Internet Becomes a More Annoying Place

- ⊙ Early Internet was largely researchers and academics
 - Most problems were due to bugs, misconfiguration, or other errors
- ⊙ Morris Worm: 1988
 - First large scale exploitation of software vulnerabilities
 - Proof of concept that escaped
- ⊙ Green Card Spam: 1994
 - First large scale "unsolicited commercial email"
 - Canter & Siegel law firm
- ⊙ **Whois** used to identify and contact sources of unwanted network traffic

```
Path: gmd.de:xlk.net!rz.uni-karlsruhe.de!news.uni-st
From: nike@indirect.com (Laurence Canter)
Newsgroups: rec.juggling,us.legal
Subject: Green Card Lottery- Final One?
Date: 12 Apr 1994 08:12:17 GMT
Organization: Canter & Siegel
Lines: 34
Message-ID: <2od151$45t@herald.indirect.com>
NNTP-Posting-Host: idl.indirect.com

Green Card Lottery 1994 May Be The Last One!
THE DEADLINE HAS BEEN ANNOUNCED.

The Green Card Lottery is a completely legal program g
certain annual allotment of Green Cards to persons bor
countries. The lottery program was scheduled to contin
permanent basis. However, recently, Senator Alan J Si
introduced a bill into the U. S. Congress which could
lotteries. THE 1994 LOTTERY IS SCHEDULED TO TAKE PLACE
SOON, BUT IT MAY BE THE VERY LAST ONE.

PERSONS BORN IN MOST COUNTRIES QUALIFY, MANY FOR
FIRST TIME.

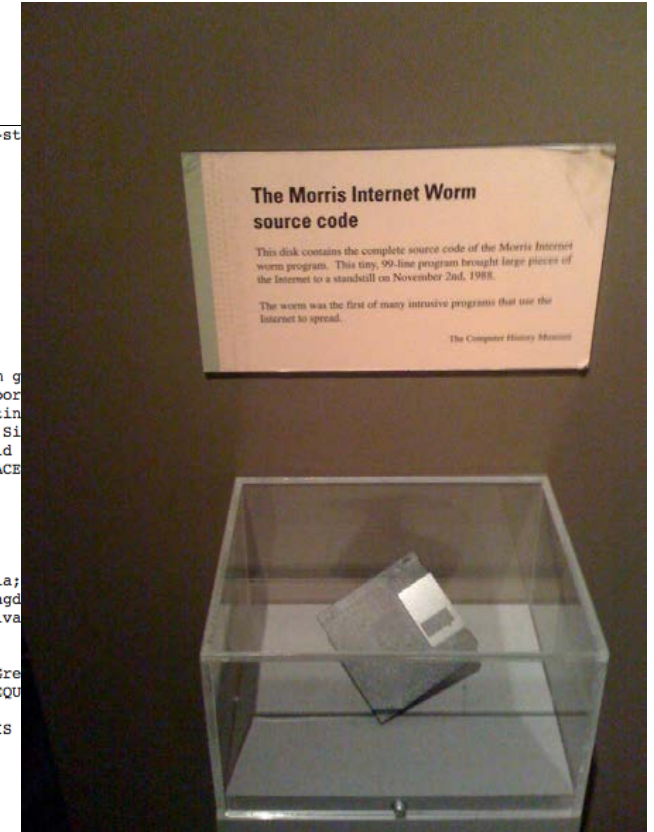
The only countries NOT qualifying are: Mexico; India;
Taiwan, Philippines, North Korea, Canada, United Kingd
Northern Ireland), Jamaica, Dominican Republic, El Salva
Vietnam.

Lottery registration will take place soon. 55,000 Gre
given to those who register correctly. NO JOB IS REQU

THERE IS A STRICT JUNE DEADLINE. THE TIME TO START IS
NOW!!

For FREE information via Email, send request to
cslaw@indirect.com

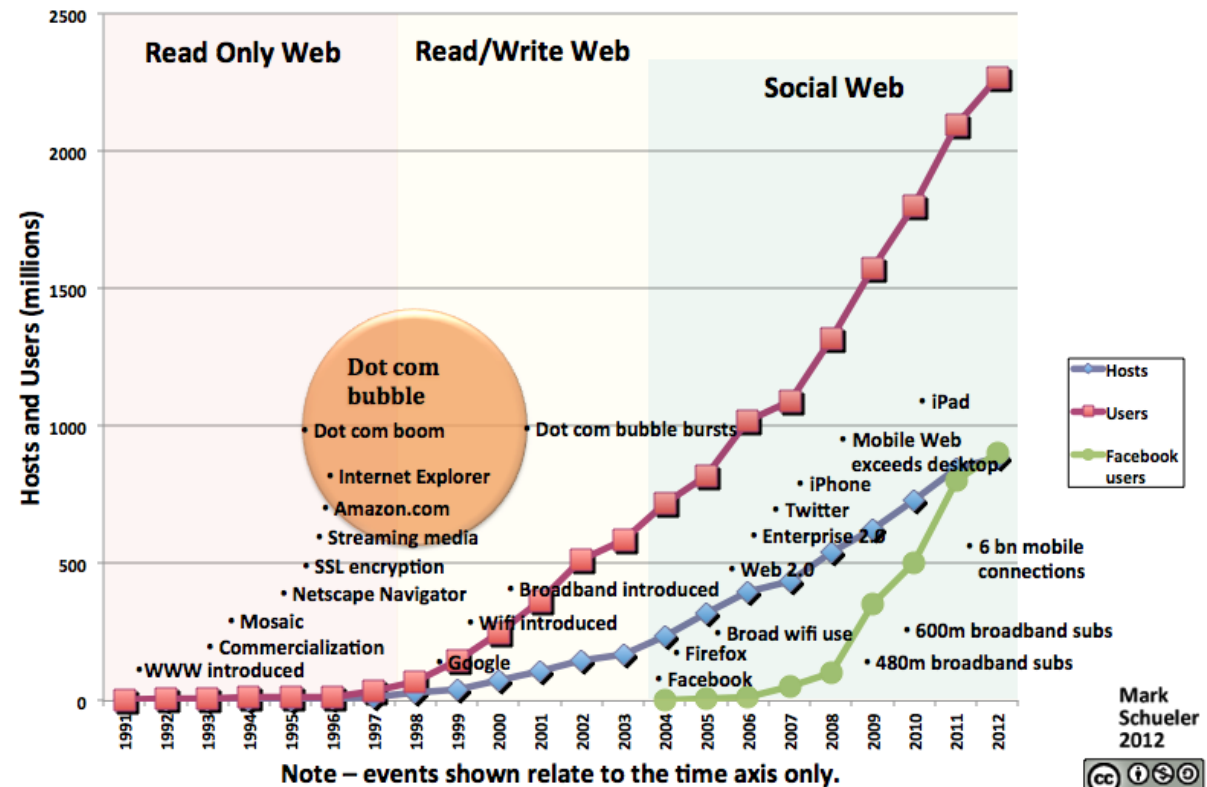
--
*****
Canter & Siegel, Immigration Attorneys
3333 E Camelback Road, Ste 250, Phoenix AZ 85018 USA
cslaw@indirect.com telephone (602)661-3911 Fax (602) 451-7617
```



Internet goes Mainstream

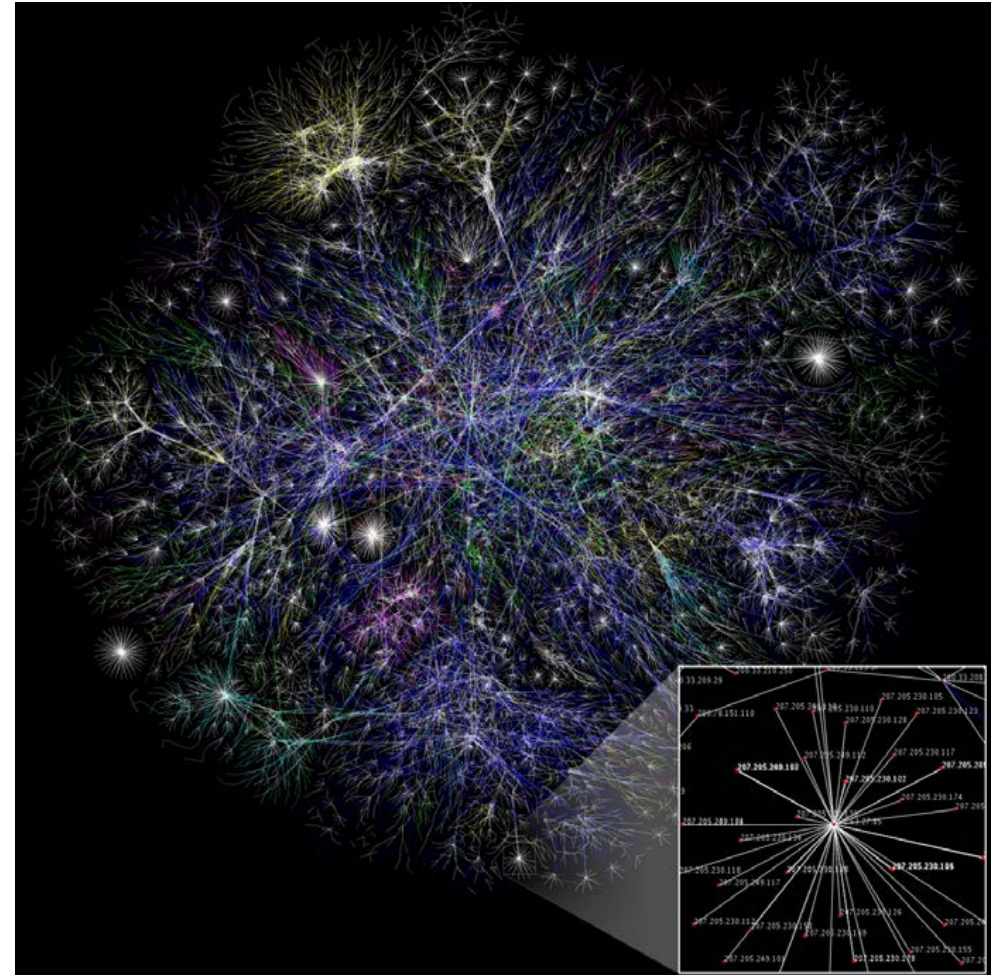
- ⊙ Invention of the World Wide Web (1991) opens the Internet up to everyone
 - Internet grows rapidly
- ⊙ Centralized allocation of names and addresses can't keep up
 - Creation of multiple address registries (1993)
 - Creation of multiple name registries (1994)
- ⊙ Whois database now distributed across multiple independent organizations
 - Single point of entry: Internet Assigned Numbers Authority (IANA)
 - Operated by ICANN
 - Only maintains referral information

Internet Growth - Usage Phases - Tech Events



The Internet Today

- ◎ Over 700,000 individual networks
 - Connecting 4.1 billion end users
- ◎ Over 350,000,000 names
 - Over 2,500 "top-level domains"
 - E.g., COM, EU, BE, INFO, etc.
- ◎ The Internet remains **peer-to-peer**
 - Every endpoint on the Internet can offer services
 - Websites, databases, games, etc.
 - Every endpoint on the Internet can initiate connections
 - Home PCs, IOT devices, etc.
- ◎ Identifying whether an incoming connection is "friend or foe" increasingly difficult
 - And increasingly important (e.g. "fake news")



Whatis Whois

- ⊙ *Whois* is an umbrella term meaning:
 - **A protocol:** defined by the Internet Engineering Task Force
 - Defined (post facto) in RFC 3912 (<https://tools.ietf.org/html/rfc3912>)
 - **A database of registration records:** defined by ICANN and the RIRs
 - Contains information about who “owns” names and addresses used on the Internet
 - Prior to 25 May 2018, publicly accessible
- ⊙ Uses of Whois:
 - Providing contact information for identifiers/resources used on the Internet
 - By analogy, a land ownership registry or a registry of companies.
 - Used in tracking down connectivity problems and abuse
 - Helping to verify resources on the Internet are legitimate
 - Mapping sources of network information to its real world sources
 - Helping to identify trademark/copyright violations
- ⊙ Historically, privacy offered as an “add on” service by some registries and registrars

Future of Whois

- ⊙ The demand for functionality provided by Whois is increasing
 - Growing with use of (and threats from) the Internet
- ⊙ Protocol being (thankfully) replaced with “Registration Data Access Protocol” (RDAP)
 - Allows for “differentiated access”
 - What you get back in response to queries depends on who you are (your credentials)
 - Allows for automatic referrals
 - Point of entry still IANA
- ⊙ Policy Changes
 - Database is no longer fully public
 - Access to full data by authorized entities being discussed
 - What is in the database will evolve
 - New fields will be added based on demands of naming (ICANN) and addressing (RIR) communities.
 - In conformance with legislation from various jurisdictions



Thank You and Questions

Visit us at icann.org

gdpr@icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



slideshare/icannpresentations



soundcloud/icann