Mitigating the Risk of DNS Namespace Collisions

WPNC 2014

March 8-10, London

Thanks!

Background

- October 2013: ICANN approved the New gTLD Collision Occurrence Management Plan
- As a part of this plan, ICANN committed to "commission a study to develop a name collision occurrence management framework"
- JAS Global Advisors LLC was selected in November to lead the development of the framework
- Phase I of the JAS report was released for public comment on 26 Feb

Where This Project Fits

ICANN has identified several phases of the broad DNS Name Collision Mitigation Strategy:

1. SLD Block List Strategy/Publication
2. Creation of the Collision Occurrence Management Framework
3. Applying the Framework

JAS has been engaged to complete (2)

Scope

- Initial Evaluation “DNS Stability String Review” focused on a string’s potential impact on the global DNS
- JAS research performed from the perspective of end-systems as “consumers” of the global DNS
- JAS found no evidence to suggest that the security and stability of the global Internet DNS itself is at risk

Risk Assessment Objectives

- The frequency of possible collisions has received substantial attention; JAS primary objective is to advance discussion of the possible consequences from the theoretical to the concrete
- Not all potential for collision results in collision
- Not all collisions are problematic
- Not all problematic collisions are equal
- Evaluate mitigation options

Definition

- Interisle: *Name collision occurs when name resolution takes place in a semantic domain other than the one that was expected by a user.*
- SAC062: *The term "name collision" refers to the situation in which a name that is properly defined in one operational domain or naming scope may appear in another domain (in which it is also syntactically valid), where users, software, or other functions in that domain may misinterpret it as if it correctly belonged there.*

Core Questions

Is this a new occurrence?

No

Is the occurrence limited to [new] TLDs?

No

Is it serious?

In some circumstances, yes

Core Questions

Why does it happen?

What do we do about it?

Stay Tuned!

Summary Findings

- DNS namespace collisions occur routinely throughout the entire DNS namespace
- Collisions have occurred prior to delegation of every TLD since (at least) 2007

TLD	Registration Date	# SLDs in theoretical block list
.post	2012-08-07	58,133
.xxx	2011-04-15	49,399
.me	**2007-09-24**	12,754
.cw	2010-12-20	10,030
.asia	**2007-05-02**	7,451
.sx	2010-12-20	5,244
.rs	2007-09-24	5,109
.tel	2007-03-01	3,954
. xn--mgba3a4f16a	2013-09-13	135

Summary Findings

- Collisions have caused “issues” in the past
  - 1987-ish: .cs/JANET
  - 1993: edu.com (RFC 1535)
  - 2008-9: MSFT Windows XP SP2 -> SP3 -> Vista changes
- Collisions are pervasive at the TLD and 2LD
  - Corp.com theoretical “3LD Block list” count > 175,000
  - Based on a 50 hour period in January 2013
  - All other parameters the same
  - Observed ample 2LD collisions in other delegated space

Why is this happening?

- Lack of appreciation/understanding of DNS
  - Architect at design time
  - Engineer at development time
  - Operator/user at configuration time
- DNS search list processing
  - Application layer
  - OS layer
- Intentional use of a namespace that is not under the control of the using party
- Retirement/expiration of hostnames/2LD registrations

Why is this happening?

- Lack of appreciation/understanding of DNS
  - **Architect at design time**
  - **Engineer at development time**
  - Operator/user at configuration time
- DNS search list processing
  - Application layer
  - OS layer
- Intentional use of a namespace that is not under the control of the using party
- Retirement/expiration of hostnames/2LD registrations

Why is this happening?

- Inconsistent/changing software behavior
- Inconsistent/changing DNS service provider behavior
  - Or changing DNS service providers!
- Colliding DNS namespaces are often purchased
  - squatting, investing, domaining, drop-catching…
- Typos, miscommunications, etc.
- Buggy code
- “Bit-flips” in DNS queries
  - (Robert Stucke DEFCON 2013)

Misuse of DNS for Authentication

- DNS is intended for identification
- Problems arise when it is also used for authentication (intentionally or unintentionally)
- DNS queries may be resolved by a different administrative party than expected by the querier
- DNSSEC doesn’t solve this
- (DANE might, depending)

Problems with DNS Resource Location

- Predominately driven by issues related to DNS search list processing
- Kumari/McPherson Paper
- SAC064
- Dependence on technical happenstance
- Intermittent DNS issues often tolerated

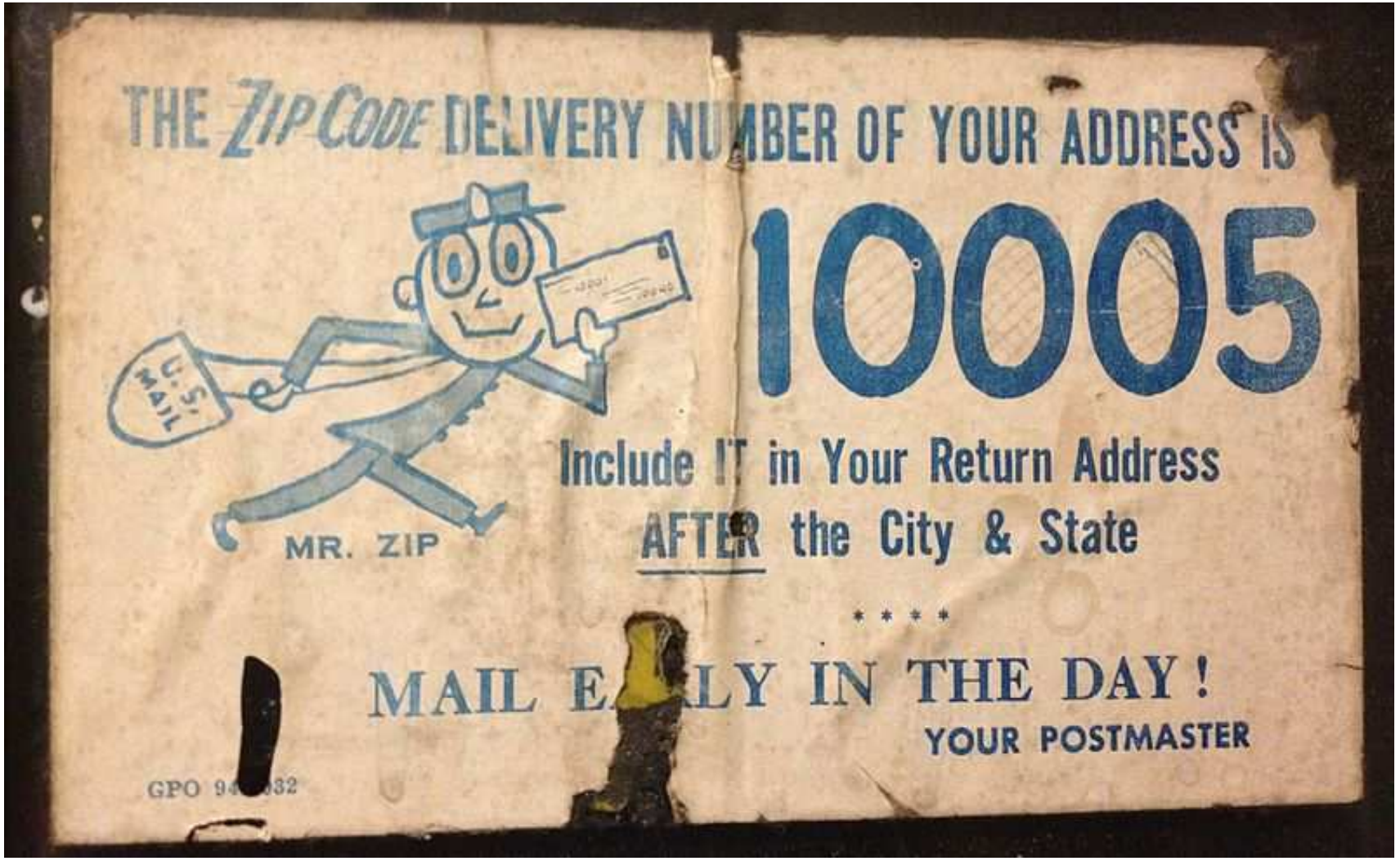
What to do?


RETURN
TO
SENDER
For Better Address


UNITED STATES POSTAL SERVICE
THIS MAIL IS ADDRESSED INCORRECTLY.
SOON YOUR MAIL WILL BE PROCESSED
BY COMPUTERS. TO AVOID
DELAY AND POSSIBLE RETURN OF YOUR
MAIL, PLEASE NOTIFY SENDER OF
YOUR CORRECT ADDRESS OR PO BOX.
WE CARE!


061219 19:26 KOA JOX 097
Santa HOHOHO Père Noël
Père Noël HOHOHO Santa
89 CANADA
Matt Groening
The Guy Who Created
The Simpsons
Los Angeles
California
USA
NIXIE 900 1 72 12/29/06
RETURN TO SENDER
UNKNOWN REASON
UNABLE TO FORWARD
BC: 00101000000 *2262-04624-29-29
00101@0000


DECEASED


THE ZIP CODE DELIVERY NUMBER OF YOUR ADDRESS IS
10005
U.S. MAIL
MR. ZIP
Include IT in Your Return Address
AFTER the City & State
* * * *
MAIL EARLY IN THE DAY!
YOUR POSTMASTER

PARTY LINES

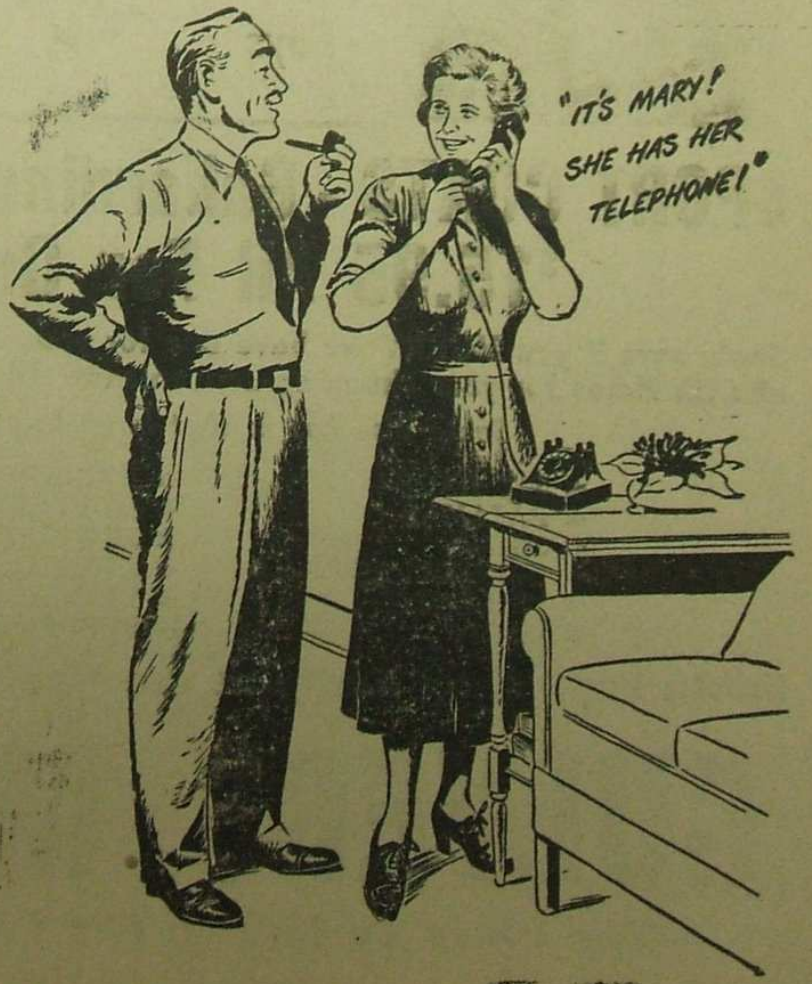
help bring telephone service sooner

WE'RE ADDING TELEPHONE EQUIPMENT... switchboards and wire, poles and cable ... at a record-breaking pace.

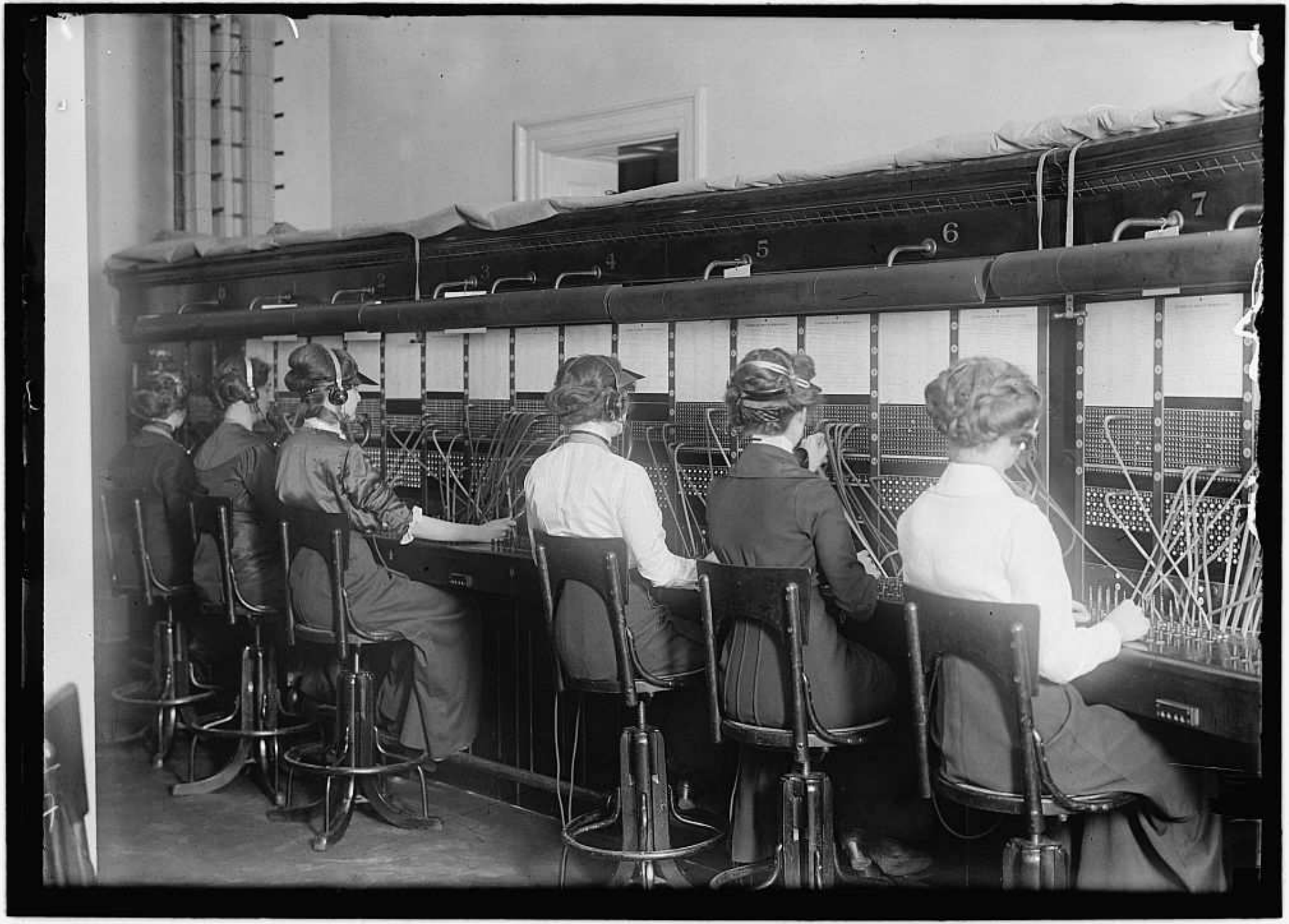
Party-line service . . . sharing the line . . . makes it possible for this new equipment to serve the greatest number of people.

That's why, in most communities, we're installing new residence telephones on party lines only.

Party-line service is *good* service, too, especially when party-line neighbors share the line with courtesy and consideration for others.



THE DIAMOND STATE TELEPHONE COMPANY


2
3
4
5
6
7


GALLOZZO
M.W.2114

The following is the complete list of Chicago and Evanston central office names and their corresponding prefixes, adopted in 1948. This system allowed for additional prefix equivalents without the invention of new exchange names.

Aberdeen.....AB 4
Albany .....AL 2
Ambassador .....AM 2
Andover .....AN 3
Ardmore.....AR 1
Armitage .....AR 6
Atlantic .....AT 5
Austin.....AU 7
Avenue.....AV 3

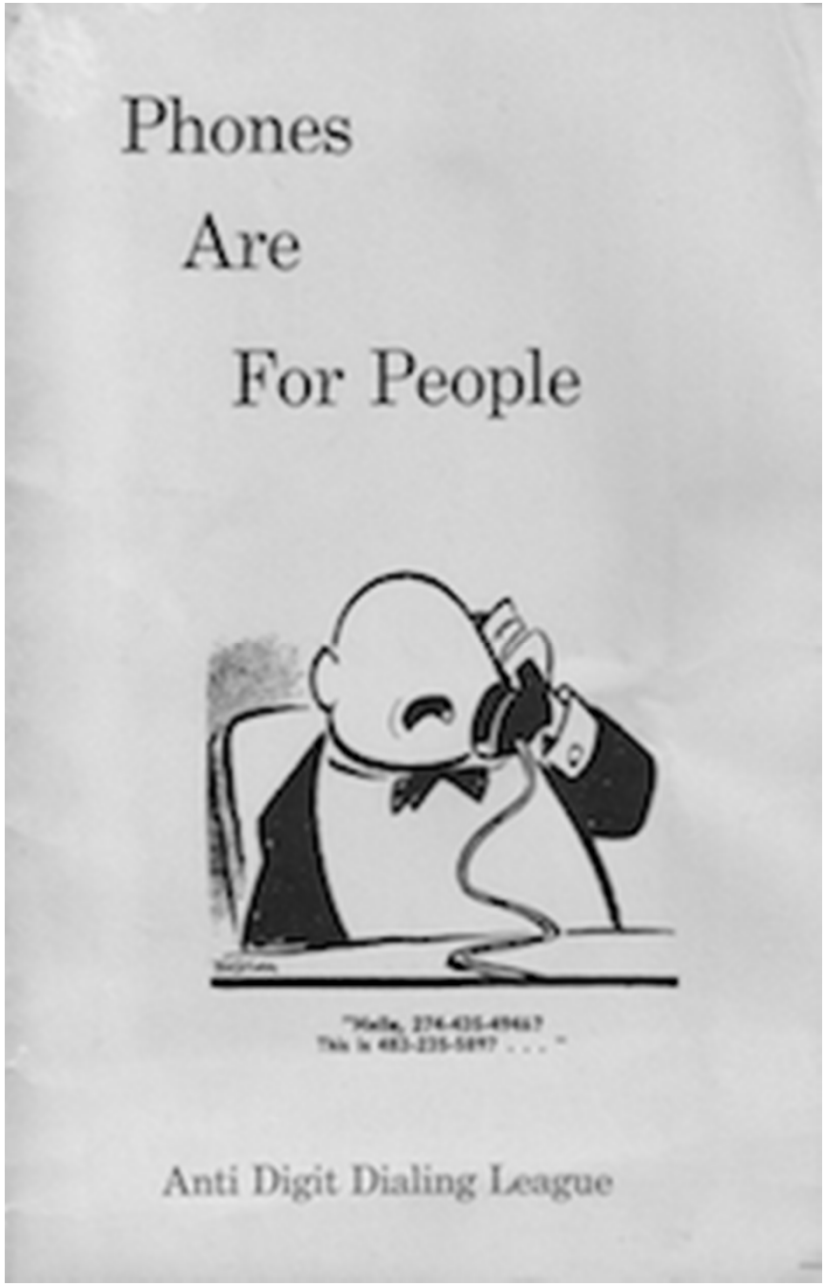
Capitol..... CA 7
Cathedral ..... CA 8
Cedarcrest..... CE 3
Central..... CE 6
Chesapeake..... CH 3
Cliffside..... CL 4
Columbus ..... CO 1
Commodore.....CO 4
Cornelia ..... CO 7
Crawford ..... CR 7

Essex.....ES 5
Estebrook.....ES 8
Everglade .....EV 4

Fairfax.....FA 4
Financial .....FI 6
Fire.....FI 7
Franklin.....FR 2
Frontier .....FR 6

ANTI-DIGIT-DIALING LEAGUE. San Francisco Bay Area residents, befuddled at memory frenzies entailed in the new, all-numeral telephoning system, are battling to make the Pacific Telephone Company revert to old exchange names—YUKON, SUTTER. Formed last May, the A.D.D.L. had an instant membership, is drawing moral support from fellow warriors across the nation. To get connected: P.O. Box 966, Sausalito, Calif. Dues, none; donations sought.

[Life, February 8, 1963]



Excerpt:

Most people, and certainly the members of ADDL, welcome constructive change. However, the telephone is an extremely important part of everyday life, and major changes in its use will have widespread effects.

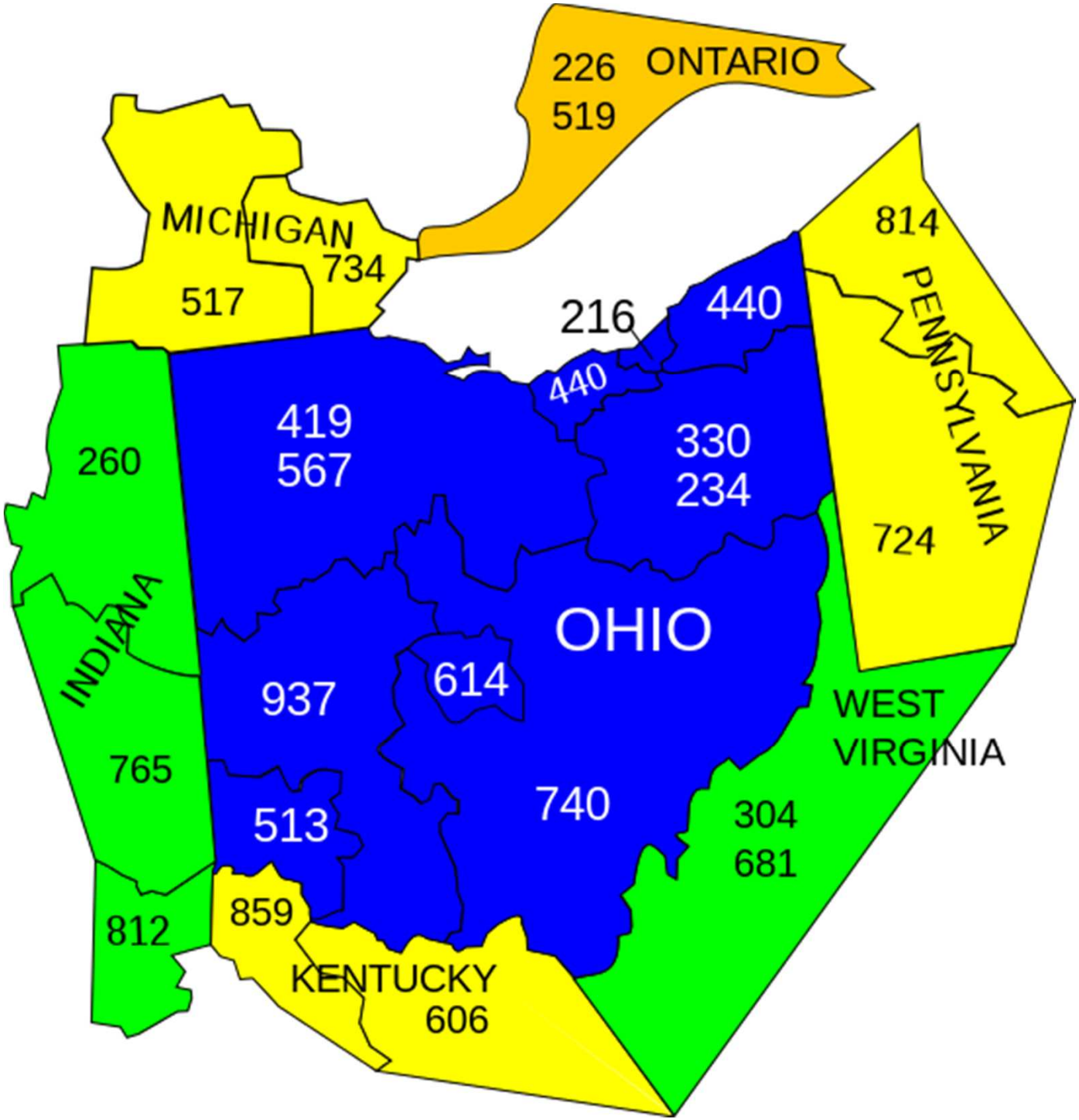
[ADDL Publication c. 1962]

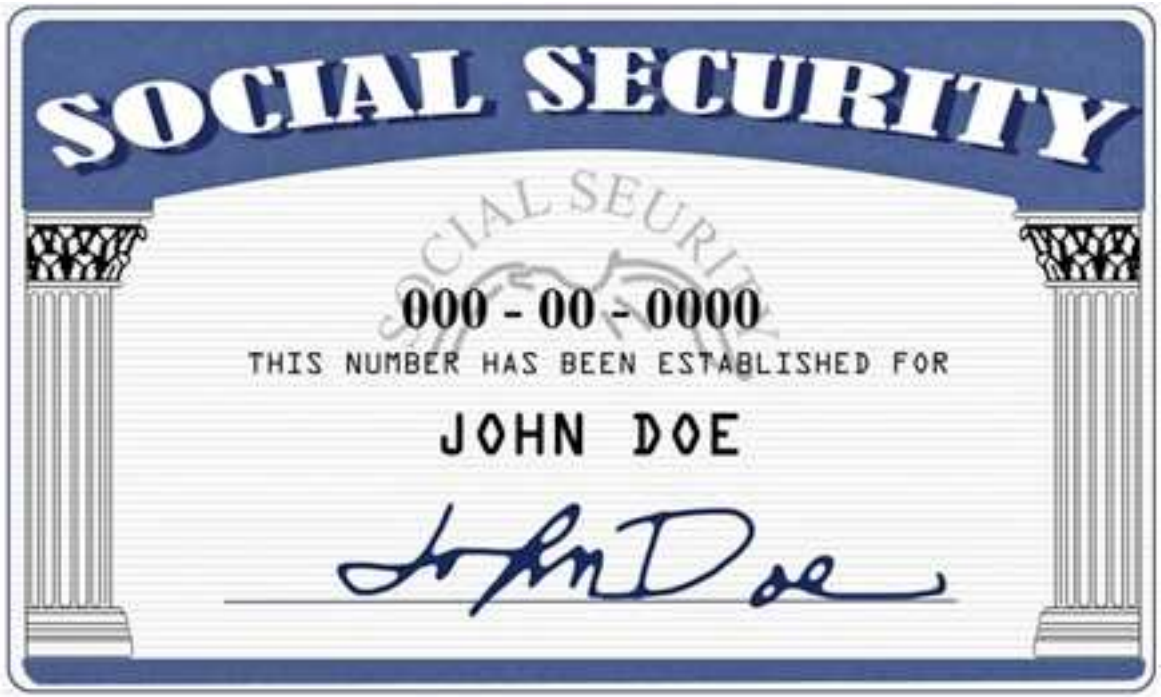

Don’t Forget!
Ten-digit dialing starts September 8, 2008


Get ready!
GREG
610-2121
204


Don’t Forget!
Eleven-digit dialing starts 10/20/12


NEW Area Code
919/984
336
252
828
704/980
910


226
519
ONTARIO
MICHIGAN
734
517
814
PENNSYLVANIA
216
440
440
419
567
330
234
260
724
INDIANA
OHIO
614
937
WEST
VIRGINIA
765
740
513
304
681
859
812
KENTUCKY
606


SOCIAL SECURITY
000 - 00 - 0000
THIS NUMBER HAS BEEN ESTABLISHED FOR
JOHN DOE
John Doe

What are the lessons for us?

- Other (important) namespaces have collisions
- Other (important) namespaces have changed
- Use notification/transition periods
  - Advance notification
  - Temporary grace/NACK period highly desirable
- 30-90 days typical
- There will be resistance to change
- In the end people and systems will adapt

JAS Recommendations

- The TLDs .corp, .home and .mail should be permanently reserved
- “Controlled Interruption” zone (127.0.53.53) immediately upon delegation and extending for 120 days
- ICANN maintain emergency response processes to act upon reported problems that present “clear and present danger to human life”
- Don’t de-delegate at root level; use EBERO

Bind Response Policy Zones

IP Trigger

The IP policy trigger is based on target data (RDATA). It matches IP addresses that would otherwise appear in A and AAAA records in the "answer" section of a DNS response.

A single resource record (RR) consisting of a CNAME whose target is the root domain (.) will cause a response of NXDOMAIN to be returned.

```
; IP policy record restores NXDOMAIN
32.53.53.0.127.rpz-ip      CNAME   .

$ dig +short corp.com @8.8.8.8
127.0.53.53

$ dig corp.com @localhost
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 11926
```

Bind Response Policy Zones

…any other RRset … specifies local overriding data which will be used to generate synthetic DNS responses.

; IP policy record redirecting to local RFC 1918 honeypot

32.53.53.0.127.rpz-ip A 10.53.53.53

$ dig +short corp.com @8.8.8.8

127.0.53.53

$ dig +short corp.com @localhost

10.53.53.53

Pretty handy, eh?

Questions?
Comments?
Discussion?