

A Framework for Telephone Number Administration in the all-IP
Network
framework-for-webtn-00

Abstract

This document describes a framework for a telephone number administration system in the all-IP network. It outlines high-level service models for number administration and generic and high-level requirements. This document is offered as input to the first [FCC workshop](#) on the Numbering Testbed scheduled for March 25, 2014.

Table of Contents

1. [Introduction](#)
2. [Terminology and acronyms](#)
3. [Scope and structure of the document](#)
4. [Framework for webTN](#)
 - 4.1 [Registry](#)
 - 4.1.1 [Managing numbering resources](#)
 - 4.1.2 [Registrant registration](#)
 - 4.1.3 [Service provider registration](#)
 - 4.1.4 [Managing webTN service](#)
 - 4.2 [Certificate authority](#)
 - 4.3 [Addressing data](#)
 - 4.3.1 [Addressing protocol](#)
 - 4.3.2 [Master addressing database](#)
 - 4.3.3 [Slave addressing databases](#)
 - 4.4 [Whois data](#)
 - 4.5 [Identity provider \(IdP\)](#)
 - 4.6 [Social data](#)
5. [A proposed model for an operational testbed](#)
6. [Other considerations](#)
 - 6.1 [Anti-squatting and anti-speculation](#)
 - 6.2 [Integration with current number administration](#)
 - 6.3 [Interoperability with TDM/CS/SS7 networks](#)
 - 6.4 [Public safety](#)
 - 6.5 [National security](#)

- 6.6 [Access for persons with disabilities](#)
- 7. [Security considerations](#)
- 8. [Conclusions](#)
- 9. [Current numbering environment](#)
- 10. [Informative references](#)

1. Introduction

This document introduces the concept of webTN, which is our term for telephone numbers (TNs) in an all-IP environment. In this environment, we envision telephone numbers as identifiers, not network routing resources. They are registered to people and enterprises (registrants), much like domain names, and then associated with services provided by communications service providers. WebTNs have a credential associated with them which includes a public/private key pair. The database offers an Identity Provider (IdP) service using the webTN as the identity. The webTN credential can be used by any service to make authorization decisions based on webTNs as identifiers.

By registering webTNs to individuals and enterprises, we separate the webTN from a device identifier or address. This allows the webTN to serve as an identifier for many services, on many devices. Addressing mechanisms must be defined to enable using webTNs to place and receive communications from other users.

While many of the services associated with a webTN could be new services not even imagined today, we wish to continue to provide two-way, real-time communications services using voice, video and text within a traditional notion of a session. The services are provided in a manner that a user with a device that conforms to a specific set of protocols and parameters be able to call any other user with a device that also conforms. This retains the call anyone characteristic of today's public switched telephone network, but extended to video and text as well as audio.

2. Terminology and acronyms

- o Telephone number (TN) - Refers to the 10-digit telephone numbers used in the United States (U.S.) in the format of NXX-NXX-XXXX, where N=digits 2-9 and X=digits 0-9.
- o Area code - The first 3 digits of a TN assigned to a geographic area such as a city.

- Central office code (CO code) - The first 6 digits of a TN assigned to a service provider, a switch and a geographic area called a rate center. CO codes are used by existing U.S. communications networks to route calls to the assigned switch.
- webTN - A term used in this document that refers to a TN in the all-IP network that is registered in the webTN registry.
- Time division multiplex/circuit switched/signaling system 7 (TDM/CS/SS7) - Refers to the traditional technologies used in communications networks that are being replaced by IP.
- Calls - While the term session would be more accurate in an IP environment, this document uses the term call (as in phone call) to cover the establishment of communications between two or more individuals and covers the applications of at least voice, video, and text messaging.
- Caller - The originator of a call from or to a webTN, also calling party.
- Called party - The terminating individual for a call to a webTN.
- North American Numbering Plan Administrator (NANPA) - NANPA administers all area codes and geographic CO codes and some non-geographic CO codes in the U.S. It also administers various other numbering resources such as carrier identification codes (CICs). It does not administer toll free TNs.
- Registrant - The individual to whom a webTN is registered, also called a user or consumer. A registrant can be an individual or an enterprise that registers multiple TNs for multiple individuals.
- Service provider - An entity that provides communications services to webTN registrants for webTNs. A registrant requires a service provider to enable communication services.
- Secure Telephone Identity Revisited ([STIR](#)) - STIR refers to both the IETF working group and the protocol it is creating to provide mechanisms to verify a calling parties authority to use a specific TN.
- Certificate authority - An entity that issues digital certificates.

- o Digital certificate - A credential containing the keying material and scoping information necessary to validate secure communications.
- o ENUM - An IETF protocol to enable translation of TNS to Internet addresses.
- o Whois data - Contact data related to the registrant of Internet resources and webTNs.
- o Identity Provider (IdP) - A trust provider who can attest to a registered user's identity.

3. Scope and structure of the document

On January 31, 2014 the FCC released an Order, Report and FNPRM ([FCC 14-5](#)) on technology transitions, specifically the transition of the communications network to IP technology. The Order calls for research and development of a numbering testbed. In paragraph 152 the FCC states that, "[t]he testbed could facilitate the development of a future telephone numbering system by exploring what options are feasible without undue encumbrance by legacy notions and systems." Subsequent to this Order the FCC scheduled a workshop for March 25, 2014 to discuss the design of such a testbed. This document outlines one possible design and is intended to generate discussion both within and outside of the FCC workshop.

It describes the various elements that would enable a number administration system for the all-IP network. It addresses the end state all-IP network and does not address the transitional period where there will be coexistent TDM/CS/SS7 and IP networks. It does not address any aspects of a business model such as; the entities responsible for each function, business relationships among any entities involved in webTN service, and funding for any aspect of the webTN service. It also does not address any regulatory or policy issues related to number administration or changes that may be required to implement a webTN service.

This document only addresses geographic and non-geographic numbering resources (TNS, area codes, CO codes), it does not address toll free or other ancillary numbering resources (e.g., CICs).

This document has three major sections; the framework for webTN, a proposed model for an operational testbed, and other considerations. The framework section describes a vision for a set of functions that collectively comprise a possible number administration system for the all-IP network. The operational testbed section describes how

this framework could be used to enable an operational testbed. The other considerations section covers issues related to communications service but not necessarily addressed in the operational testbed.

There is a security considerations section, a conclusion and a description of the current numbering environment. The current numbering environment section also addresses the changing environment and how those changes have influenced webTN. It is not necessary to read the current numbering environment section to understand our proposed model for the future numbering system.

4. Framework for webTN

This section describes the six major elements of the webTN service.

1. Registry - At the core of webTN is the registry that manages the numbering resources and enables the registration of webTNs by registrants and the activation of communication service by service providers.
2. Certificate authority - The certificate authority provides digital certificates to authorize registrants and service providers to use the webTN.
3. Whois data - Is collected from registrants and service providers, and potentially disclosed to approved entities.
4. Addressing data - Is collected and propagated.
5. IdP - The registry could act as an IdP.
6. Social data - The registry could collect and disclose social data if the registrant provides explicit approval to do so.

4.1. Registry

The webTN registry is very similar to a domain name registry. It manages the namespace (the webTNs) and enables the registration of webTNs by registrants and service providers.

4.1.1. Managing numbering resources

WebTN numbering resources are managed at the individual TN level. They are registered to consumers, either directly to the consumer or to a service provider on behalf of the consumer. There is no concept of a CO code or a thousands block, other than the fact that they are a block of ten thousand or one thousand individual TNs.

The registry works directly with federal and state regulators to activate area codes (approximately eight million TNs) in the registry. Area codes may be non-geographic (cover the entire U.S.), state-wide (cover an entire state), or regional (cover a region that is associated with an existing area code region). Many area codes will be activated to give registrants a wide choice of TNs. There will also be some reserved area codes to account for state-wide or region-specific growth and other potential future functions.

Registrants can choose a TN from any area code category; non-geographic, state-wide, or regional. The only nexus requirement is that the registrant has a verifiable location in the U.S.

4.1.2. Registrant registration

There are two methods for a registrant to register a webTN; either directly through the registry website or via a service provider. A registrant can be either an individual consumer or an enterprise. The registrant creates an account with the registry. A webTN can be designated as personal or business. They can choose to select a specific webTN or have one randomly assigned from a chosen area code. As an anti-squatting measure, there should be a limit to the number of webTNs an individual registrant can register. This limit is subject to further industry discussion.

Registrant verification is a key component of ensuring a reliable STIR solution and an accurate whois. The registrant will provide identifying information such as name, address, phone numbers, and e-mail addresses. This information will be used to verify the registrant in the same way that is done with existing commercial services. After the initial verification, there will be a second verification process where an e-mail or text message is sent to the registrant and the registrant will take an action on that text or e-mail, such as enter a provided code, to complete the process. After this verification, the registrant's account is created and they can register webTNs.

Further work needs to be done to address those that fail the verification process.

Upon registration, the registrant will receive a digital certificate that authorizes them for the webTN.

4.1.3. Service provider registration

Service providers that wish to provide communications services for webTNs will also be required to register. This will be a similar

process to registrant verification, e.g., name, address, phone numbers, e-mail addresses, etc. Ideally this would be the only registration/certification process for service providers, so they would not need to also go through a regulatory registration/certification as well.

4.1.4. Managing webTN service

Unlike traditional telephone numbers, webTNs are not directly tied to a service. Services can be associated with a webTN but; multiple services can be associated with a single webTN and multiple webTNs can be associated with a single service.

The simplest form of associating multiple services with a single TN is where the services involve different media. This would permit, for example, text service for a webTN to be provided by a different provider than voice service. However, we envision more complex situations where multiple services with the same media may be provided on a single webTN. So, for example, a mobile service and a cable-based home service may be associated with a webTN. Outgoing calls in such a situation would be straightforward. Incoming calls could be handled by webTN registrant selection of one of several strategies (sequential ring, parallel ring, geofence, etc). A simple situation, where one service provider supplies all services, is also supported.

The digital certificate is used to activate, change, transfer, or cancel webTN service. It requires collaboration between the consumer, the service provider, and the registry. The consumer provides their certificate to the service provider. The service provider submits the certificate to the registry to enable service by, at least, provisioning addressing information for terminating calls to the webTN.

To change service providers, the consumer would provide their certificate to the new service provider. The new service provider would provide their addressing data to the registry with the certificate. The change in service is immediate. There is no interaction between the old and new service providers. The registry would notify the old service provider that their service was terminated for that webTN.

To transfer the webTN, the registrant would delegate the certificate to another webTN registrant. It cannot be transferred to a person that does not have an active account with the webTN registry.

To cancel the service, the consumer would submit their certificate to the existing service provider or registry and cancel their service. If the service were cancelled through the service provider, then the service provider would notify the registry. If the service were cancelled with the registry then the registry would notify the service provider.

4.2. Certificate authority

The registry will also serve as a credential authority to distribute certificates to consumers and service providers and verify signatures that use the certificate.

Since the certificates are distributed to consumers, there needs to be a consumer friendly method for distributing the certificates to the registrants and for the registrant to provide the certificate to the service provider or the registry.

The credential is used to; manage the registration, manage the association of services to the webTN, assert authority over the webTN (including signing outgoing calls), and prove possession of the webTN.

Any entity can obtain the public key of a webTN, which it can use to verify operations purportedly made by the registrant. For example, the public key is used in the STIR verification to prevent spoofing of webTNs. A service provider associated with a webTN can also sign outgoing calls using its service on behalf of the registrant, using a credential issued to it by the registry for this purpose.

4.3. Addressing data

Since IP networks cannot use telephone numbers for addressing purposes, there must be a way to translate webTNs to Internet addressing resources to enable terminating calls to webTNs. This is particularly critical in the case of automatic callback from a public safety answering point (PSAP). In the event that a consumer with a webTN calls a PSAP and the call is disconnected, there must be a way for the PSAP to use that webTN to call back the consumer.

The addressing data itself should be in the form of an Internet-based resource. This could be a uniform resource identifier (URI) that connects directly to the consumer's application or it could be a domain that identifies a service on the service provider's network that will, in turn, terminate the call (similar to an ENUM Tier 2 address).

4.3.1. Addressing protocol

Many would think that ENUM is the obvious solution for addressing in an all-IP network. [ENUM](#) is a protocol created by the IETF. In summary, it converts a telephone number into a domain name and queries the DNS to find addressing information. The ENUM working group was created in 1999 and closed down in 2011. While a version of ENUM has been used in privately managed IP networks for call routing, it was never deployed as originally envisioned and is rarely used between managed IP networks.

ENUM's reliance on DNS is one of its shortcomings. The DNS is an integral part of the Internet and IP networks that translates domain names into IP addresses. Like many foundational protocols, it does something limited in scope and therefore does it very well. However, over time, the scope of proposed applications DNS is used for has expanded. This expansion of DNS applications creates tension with the original limited scope of DNS, especially when the DNS has been extrapolated to identifiers other than domain names, such as TNs. In fact, DNS can be a poor fit for some of its proposed applications. This is documented in IETF [RFC 6950](#) issued by the Internet Architecture Board (IAB) titled Architectural Considerations on Application Features in the DNS.

The original intent for ENUM was that it would be part of the public DNS. But operational, organizational, and political problems associated with integrating international and national numbering management into the public DNS proved too great to overcome. Eventually, entities decided ENUM would be a good protocol for privately managed IP networks. It was also proposed to expand ENUM's role to include applications that were used in existing communications networks such as calling name service.

The needs of the industry to have a secure protocol that accesses rich information about telephone numbers will go beyond what ENUM and DNS can meet. This will only become more pronounced in the webTN environment where there will be a need to access rich data related to the registrant, the service provider, addressing, security, and other information. While ENUM/DNS would be a good near-term solution, it will not likely be a good long-term solution. The need for a query-response capability that allows for richer expression of both questions and answers related to TNs is documented in the IETF draft titled A Framework and Information Model for Telephone-Related Queries ([TeRQ](#)).

Rather than being DNS-based, a protocol consistent with the TeRQ framework would leverage protocols used in web services such as

RESTful HTTP and JSON. These are widely deployed, well understood, and have the capability to be secure and support complex queries and answers.

The FCC workshop should develop requirements and a data model for implementing a query/response protocol that uses web services technology and is consistent with the TeRQ framework.

4.3.2. Master addressing database

The registry will maintain the master addressing database (master). This is the authoritative addressing database used to create slave addressing databases (slaves). The master is an administrative database and is not queried during call processing. It must be secure and redundant to protect against loss of data.

4.3.3. Slave addressing databases

Ideally, there would be hundreds or even thousands of slaves that would be available to be queried during call processing. Any entity would be able to host one or more slaves and receive updates from the registry. This would ensure the highest quality of service for consumers by pushing the data closer to them as well as provide continuity of service in the event of one or more slaves being out of service.

However, this ideal solution must be balanced against the need for addressing accuracy and timeliness and the need for consumer privacy. The address can change at anytime and service changes are immediate at the registry. These changes need to be propagated to the slaves rapidly. In a 911 callback, or other emergency situation, it would not be acceptable for some slaves to have outdated addressing information.

The slaves contain bulk information that could be exploited for nefarious purposes. To combat this, data within the slave must be encrypted and can only be accessed by a query for addressing data. It may be appropriate to require any entity that queries the slave do so with a webTN as their source identifier. This way, the registry would be able to identify abusers and revoke their webTN privileges.

The FCC workshop should consider a solution where slaves are distributed freely. However, they also need to consider the possibility of doing so in an environment where the data must be accurate, timely, and secure from potential abusers. An alternative

to freely distributed slaves could be slaves distributed to verified service providers only.

4.4. Whois data

Whois is the term for a service that provides information about the registrant of a domain name or IP address. Domain name and IP address registries provide a whois service to the public. This is in the event that there is a problem or issue with the domain name. WebTN should have a whois service.

Some of the information in a domain name whois record includes; registrant name and contact, administrative contact, technical contact, and billing contact. There is an existing protocol used by most registries, [RFC 3912](#), which defines the query and response process. The IETF Web Extensible Internet Registration Data Services working group ([WEIRDS](#)) is currently working on an updated protocol for whois data.

There must be controls on the webTN whois because it provides contact information that could be abused. Some possible controls could be:

- o access to contact information is strictly limited to approved entities, not the public;
- o no contact information is ever disclosed for consumers, only for service providers;
- o a trouble ticket process that goes through the registry and never discloses contact information; and/or
- o a webTN is required as an identifier for accessing whois.

The FCC workshop should develop a recommendation for what information is stored in the whois, how it is protected, who can access it, and how they can access it. The workshop should evaluate the benefits of using WEIRDS as the query/response protocol or whether something new should be created using the TeRQ framework.

4.5. Identity provider (IdP)

The webTN is used as an identifier for a consumer. The webTN registry will verify the consumer, i.e., verify he/she is who he/she claims to be. As such, the webTN service can be used as an identity provider (IdP), an entity that can assert the identity of an

individual. Consumers can use their webTN credentials to sign on to sites that choose to rely on the webTN service as an IdP.

Existing IdPs include Google, Facebook, AOL, Yahoo, PayPal, and Microsoft. OpenID is the most widely used protocol; it provides a framework for the communications that must take place between the IdP and the relying party (a website or entity that uses an IdP to authenticate a user).

The FCC workshop should address the possibility of the webTN provider being an IdP.

4.6. Social data

Communications patterns are an excellent way to create a social graph. Social networking applications such as Facebook, LinkedIn, and Google+ have shown that many people like to understand their social graph, i.e., relationships among them and their acquaintances and their acquaintances' relationships.

WebTN service will be in a position to track webTN users' social graph, i.e., who they call, who calls them, and how often. WebTN registrants would always need to opt-in to share their social data. WebTN call data could be collected from the slaves and service providers. The service could provide an application programming interface (API) to access the social data to applications authorized by webTN registrants. Like addressing data, the social data could be accessed using a protocol created from the TeRQ framework. Other social networking sites can access this data to enhance their services with the permission of the webTN owner.

The FCC workshop could evaluate the possibility of the webTN platform collecting and providing access to users' social data.

5. A proposed model for an operational testbed

The framework section of this document describes a vision for the future number administration system in the all-IP network. Once the workshop develops a consensus design for the testbed based on this vision and visions provided by others, we can then develop working versions of the various aspects of it to test in a real-world environment. We should reserve at least one non-geographic area code for testing. Perhaps we could also reserve a state-wide and a regional area code for testing too. These would be reserved from NANPA's existing area code inventory.

We can allow consumers and service providers to register webTNs to enable services. We need to be explicit that this is a trial and the service will be turned down within approximately 12 months. We need to let them know they will not necessarily receive calls from non-webTN numbers, nor originate calls to non-webTN numbers. Ideally some trial participants would be able to enable calls between webTNs and non-webTNs, but we'd have to communicate to the public that this may not be the case. Most importantly, the public needs to know that they cannot call 911.

We can gather data about usage of such a system including registration, verification, call processing, whois, incident management, IdP, and social data. This will help us better understand the future all-IP numbering system

6. Other considerations

This section is intended to raise issues that will eventually need to be addressed but don't necessarily need to be addressed to have a successful testbed.

6.1. Anti-squatting and anti-speculation

Some phone numbers could be more desirable than others. For example some consumers may want numbers that have repeating digits, or others may prefer numbers with 0s. Further, some area codes could be more desirable than others. In the future, a non-geographic code such as 777 could be more desirable than others.

However, TNs are a limited resource. In the current format, there are 6.4B telephone numbers in the NANP—of those TNs, approximately 1.5B are already allocated, and of those, there are approximately 750M assigned to consumers.

Because TNs are a limited resource, there must be strong anti-speculation and anti-squatting measures in place for webTNs. We've discussed a couple of possible measures so far. First, the fact that the registrant is verified provides the ability to identify abusive behavior. Second, we could put a limit on the number of webTNs any one registrant can register without getting further permission to register more.

While we should support the process of transferring webTNs, we also need to ensure this is not being used to create a business for selling webTNs. Perhaps there should be a limit on transfers for an individual registrant.

There has been a lot of experience in these issues in the domain name environment. The FCC workshop should leverage this experience to help develop further measures to combat these abuses.

6.2. Integration with current number administration

As stated previously, there are 1.5B allocated and 750M assigned TNs. How would webTN integrate these numbers into the new system? Are there two namespaces; one legacy and one all-IP? Would unassigned numbers in existing area codes become webTNs? How do we transition from the current administration regime to webTN? These are just some of the questions that will ultimately need to be addressed.

These types of issues need to be addressed after the FCC testbed process. In fact, the testbed will help inform these types of issues and decisions.

6.3. Interoperability with TDM/CS/SS7 networks

There are only two methods for integrating TDM/CS/SS7 networks with IP networks. Either the TDM/CS/SS7 network recognizes a call as destined to IP and hands it off to an IP network for call processing. Or the IP networks maintain interfaces to the TDM/CS/SS7 network.

This trial is not necessarily going to test those methods, but it is an issue that needs to be addressed as we transition to the all-IP network.

6.4. Public safety

There has been significant work done in standards groups to prepare the 911 systems for the all-IP network. This comes under the broad heading of [NG911](#). In addition, there is work going on at the IETF to be able to provide more accurate location information. For example, current technologies cannot provide location to a specific floor in a large building. These future enhancements will use the IP address of the caller, not the TN. For webTN we should assume that TNs will not be used as an identifier to access location information.

Currently, PSAP callback still plans to use the TN to call the consumer. We should assume that this is still the case for webTN.

6.5. National security

We should assume wiretapping and data gathering with regard to webTNs will still be a requirement from local and national security agencies. The current model, however, would still seem to work in the webTN world. Agencies identify the service provider, likely through whois, and then submit a request to the service provider to access the webTN user's communications.

It doesn't seem that the webTN environment changes the current process. However this should be evaluated as part of the testbed research.

6.6. Access for persons with disabilities

It does not seem that there would be any special handling of webTNs required for persons with disabilities. The website would need to be accessible. But there would be no need to distinguish a webTN assigned to a person with disabilities from one assigned to anyone else. The service providers will be able to associate the webTN with any services necessary.

This should be kept in mind as we go through the testbed research.

7. Security considerations

This framework is based on allocating identifiers to verified registrants. It describes an administrative model for associating digital certificates with the identifier. It discusses the need to protect contact information about the registrant and an opt-in model for the registrant to participate in processes that would disclose information about them.

8. Conclusions

The FCC's numbering testbed offers the industry a unique opportunity to research number administration in an all-IP environment. This document is offered as input to that process to assist in focusing the effort to gain the greatest benefit.

9. Current numbering environment

Communications networks are undergoing a transformation from the traditional TDM/CS/SS7 technologies to IP technology. As this occurs, TNs are evolving from network routing resources to user identifiers. TNs are not a natively routable resource on IP networks and therefore need to be translated into an address that is

routable. When they are no longer used as routing resources, they will solely be used as user identifiers. In addition, as mobile and IP become more dominant forms of communication; geography, which is built into geographic TNs, is becoming less relevant.

TN administration consists of a number of entities that allocate: area codes to states, routing resources (e.g., CO codes, CICs) to service providers, TN inventory to service providers (CO codes and thousands blocks), toll free TNs to service providers and manage the porting of TNs, as well as a number of other functions.

The structure of a U.S. TN is NXX-NXX-XXXX, where N=digits 2-9 and X=digits 0-9. The first three digits of the TN are called an area code. These are assigned to specific regions within a state. There are approximately 8M TNs in an area code. Typically more populated regions have more area codes.

The combination of the first three digits and the next three digits is called the CO code. The CO code is used by communications networks to route calls. They are uniquely assigned to a service provider and switch. Therefore, they identify the terminating service provider and switch for call routing purposes. With the advent of number portability (NP) and thousands-block number pooling, networks often must translate the dialed TN to a routing TN called a location routing number (LRN). Networks use the CO code of the LRN to route calls.

CO codes are assigned to a service provider, to a switch, and to a specific region called a rate center within a larger region called a LATA. Service providers are entitled to a CO code for each switch and each LATA. There are approximately 200 LATAs in the country. There are 800 CO codes in an area code. Once all CO codes are assigned, a new area code needs to be introduced to the region; a disruptive process for consumers, regulators, and service providers. This practice has resulted in new area codes being introduced when there are a large percentage of the 8M TNs unassigned to users.

TN inventory is allocated in blocks of a 1,000 TNs to a service provider, to a switch, and to a specific region called a rate center. There are almost 20,000 rate centers in the country. According to the last FCC [Number Resource Utilization in the United States](#) report for the year 2010, utilization rates are less than 50% for all allocated TNs. This is due, in large part, to how numbers are allocated to specific geographies.

This strong linkage between TNs and geography is rapidly becoming irrelevant. Many people now have billing plans that are not

affected by the distance a call travels in the U.S. Consumers are moving away from traditional wireline service and adopting mobile or IP service. Mobile and IP service are not dependent on where the consumer lives or where they originate calls. While many people like to have their TN indicate something about a region they are associated with, it is becoming more important to retain a TN even if you move. It is now common for people to have mobile TNs associated with a place they lived or worked many years ago.

The transition to IP is also having a negative affect. It is becoming easier for entities to spoof TNs as their callerID. It is less expensive to operate IP communications infrastructure than TDM/CS/SS7 infrastructure. This has resulted in an increase of abusive practices on the communications network. Robocalling, swatting, TDoS, (telephone denial of service) and vishing (VoIP phishing) are some of the abusive practices on the increase. There is an IETF effort underway in the STIR working group to develop technology to combat this problem by authenticating TNs and the entities using them. These solutions should be part of the future number administration processes.

WebTN attempts to take into account all of these issues; the TN as solely a consumer identifier, the decoupling of TNs from geography, a more efficient utilization regime, and a more trusted environment. In addition to these changes that need to be taken into account, there are a few things that need to, at least, remain the same such as; numbering's role (if any) in NG911, national security, interconnection, enabling communications for persons with disabilities, and portability.

10. Informative references

[I-D.draft-iab-dns-applications-07]

Peterson, J., Kolkman, O., Tschofenig, H., Aboba, B.,
"Architectural Considerations for Application Features in the
DNS", [draft-iab-dns-applications-07](#), February 2013

[I-D.draft-peterson-terq-03]

Peterson, J., "A Framework and Informational Model for Queries
About Telephone-Related Queries", [draft-peterson-terq-03](#),
February 2013

[I-D.draft-jennings-stir-rfc4474bis-01]

Peterson, J., Jennings, C., Rescorla, E., "Authenticated Identity Management in the Session Initiation Protocol", [draft-jennings-stir-rfc4474bis-01](#), February 2014

[I-D.draft-peterson-stir-certificates-00]

Peterson, J., "Secure Telephone Identity Credentials: Certifictes", [draft-peteerson-stir-certificates-00](#), February 2014

Authors' Address

Tom McGarry
Neustar
Email: tom.mcgarry@neustar.biz

Jon Peterson
Neustar
Email: jon.peterson@neustar.biz

Brian Rosen
Neustar
Email: brian.rosen@neustar.biz