CENTER FOR
DEMOCRACY
&
TECHNOLOGY

# ENUM: MAPPING TELEPHONE NUMBERS ONTO THE INTERNET

## Potential Benefits with Public Policy Risks

**April 2003**

**Standards, Technology & Policy Project**
**Center for Democracy & Technology**
**1634 I Street, NW, Suite 1100**
**Washington, D.C. 20006**
**+1-202-637-9800**

# Table of Contents

# Executive Summary

ENUM is a technology "protocol" that allows the translation of normal telephone numbers into a format that can be used to store and retrieve Internet addressing information, which can in turn be used to route communications over the Internet. As such, ENUM can help bridge the gap between the traditional telephone network and the Internet. With ENUM and "Voice over Internet Protocol" ("VoIP") technology, an increasing amount of voice communications can be carried over the Internet instead of over the telephone network. Initially, ENUM is likely to be deployed by corporations and other large institutions that seek to reduce their use of traditional telephone services. This technology has the potential to allow large and small users to save money and increase control over and flexibility in their communications.

But ENUM's potential benefits also bring risks in terms of privacy and other public policy concerns. The simplest implementation of ENUM envisions that individuals' personal contact information (such as telephone numbers and e-mail addresses) will be stored in special records located in the Domain Name System (or DNS) of the global Internet. Because the DNS is publicly available, the use of ENUM could significantly compromise the privacy of its users.

A more complex use of ENUM (in conjunction with a "proxy server"), however, offers the opportunity to gain the benefits of ENUM without sacrificing control over personal information. To promote the availability of this approach, any implementation of ENUM should follow a number of important guidelines to ensure that there is a diversity of ENUM service providers and that those providers are able to offer privacy-protecting ENUM options. This paper lists 14 specific policy recommendations, found in Section II.C below.

One critical aspect of the global public policy issues surrounding ENUM is the fact that ENUM will, to a large extent, be implemented within each country by the telephone authorities or companies that operate within that country. Thus, many critical decisions (for example, about how much information will be required to obtain an ENUM number) may be made on a country-by-country basis. Because there are important potential privacy and policy risks raised by ENUM, it is vital that within each country, the relevant authorities must closely consult with the public interest and civil society sector, the communications industry, and the computer industry.

ENUM does offer important potential benefits, and if implemented correctly it can enhance rather than harm individual privacy. But any country seeking to implement ENUM should pay close attention to the important issues of public concern that it raises.

**For more information, contact John Morris**
**at jmorris@cdt.org or +1-202-637-9800**

# ENUM: MAPPING TELEPHONE NUMBERS ONTO THE INTERNET

## Potential Benefits with Public Policy Risks

**Center for Democracy & Technology**

**April 2003**

ENUM is a technology "protocol" to convert traditional telephone numbers into a format that can be used to store and retrieve Internet addressing information (such as "voice over the Internet" and e-mail addresses), which can in turn be used to route communications on the Internet.

According to its proponents, ENUM[1] promises to bridge the gap between the main communications network of the end of the Twentieth Century (the telephone system) and the network of the beginning of the Twenty-First Century (the Internet). ENUM can assist users in making "voice" calls over the Internet in a seamless manner, without having to change how they place a phone call. By using ENUM (and "voice over the Internet" services more generally), users may be able to save money on local and long distance phone service, exercise new options for structuring the communications services they purchase, and benefit from new service offerings. But, along with this potential, ENUM also poses some serious threats to privacy and other public policy concerns, threats that must be considered in any implementation of ENUM.

This paper first introduces ENUM and the "voice over Internet Protocol" service (which is one of the enabling technologies that has motivated the creation of ENUM). It then reviews a range of privacy and public policy issues raised by ENUM, and concludes with a series of specific policy recommendations that the Center for Democracy & Technology believes should be followed in any ENUM implementation.

[1] The word "ENUM" had its origins in the phrases "*e*lectronic *num*bering" and "t*e*lephone *nu*mber *m*apping," but today, "ENUM" is generally used as a word unto itself.

# I. ENUM Fundamentals

At its broadest, ENUM is a technology protocol created by the Internet Engineering Task Force that will be used to tie the traditional telephone network with the new communications network, the Internet.[2] As such, ENUM may prove to be an important component of the communications industry's transition away from the traditional telephone network to the Internet as the primary carrier of communications, both voice and data. Although the dedicated telephone system will likely continue to exist for years to come, voice communications will increasingly be carried over the Internet. ENUM has a variety of potential uses, but its first significant use will likely be to facilitate the carrying of voice phone calls over the Internet. In supporting this and other services, it will be important to implement ENUM so that – at a minimum – it does not *reduce* the level of privacy and personal control available in the regular phone system. If properly implemented, ENUM may in fact ultimately be able to *enhance* privacy and personal control.

## A. Telephone and "Voice Over IP" Basics

Before considering ENUM, it is important to first understand some basic terminology of the traditional telephone system and the new technology to carry voice telephone calls over the Internet:

The "Public Switched Telephone Network" (or "PSTN") is a common term for the traditional telephone system as it has developed through the twentieth century. A key word in PSTN is "switched" – the traditional telephone network is called a "circuit switched" network. When a telephone call is placed in a circuit switched network, a single dedicated electrical connection (a "circuit") is created (using "switches") between the calling party and the called party.[3] That dedicated channel is maintained until the call ends.

In contrast to a circuit switched network like the PSTN, the Internet is a "packet-switched" network that sends communications in small digital packets over shared electrical connections (which themselves use wired, wireless, optic, or other technologies). A communication (such as an e-mail or a web page) is divided into small packets that are sent over the shared connection (the Internet) and then reassembled at the receiving end. The most common rules for the handling of packets are contained in a pair of "protocols" that are referred to together as the "Transmission Control Protocol/Internet Protocol" (or "TCP/IP").[4]

[2] The core standard, as articulated by the IETF, is found in RFC 2916, "E.164 number and DNS," http://www.ietf.org/rfc/rfc2916.txt.

[3] Historically, a dedicated electrical channel was created to carry telephone calls over the PSTN. As a technical matter today, however, even the PSTN uses "virtual circuits" and other techniques to make communications more efficient. Nevertheless, the concept of a dedicated communications channel is still applicable to telephone calls made over the PSTN.

[4] Increasingly, the PSTN in incorporating TCP/IP technology into the core of the existing telephone network. This use is invisible to end users, and does not raise the same issues as are discussed below.

"Voice over IP" (or "VoIP") is the process of transmitting a voice call over the Internet using the "Internet Protocol."[5] The sound to be transmitted in a voice call is converted into digital form and divided up into small "packets," which are sent over the Internet (sharing the links with other packets, which might contain e-mail, web pages, or other types of communication) and then reassembled at the receiving end and converted back into sound. All of this can happen quickly enough that one can have a clear voice telephone call over the Internet (using VoIP), with no discernable difference in quality between it and a phone call over a traditional voice network (although heavy traffic on the Internet could result in delayed or lost packets, which could degrade the sound quality of a VoIP phone call). Over the past few years, the quality of VoIP calls has significantly improved, and the cost of VoIP equipment is continuing to decline.

Although ENUM will help facilitate VoIP telephone calls, it is important to understand that VoIP phone calls do *not* require ENUM, and such calls can be made wholly without ENUM. In other words, one can take advantage of a variety of "Voice over the Internet" services without using ENUM. There are commercial services today that support VoIP to allow phone calling over the Internet, and none of those services currently uses ENUM.

Moreover, one can place VoIP calls directly to someone else who has VoIP capability, without using ENUM or any commercial VoIP provider. A common (but not exclusive) way to initiate a VoIP call is to use the "Session Initiation Protocol" (or "SIP").[6] Essentially, SIP performs the function of establishing a connection and "ringing" someone else's VoIP telephone over the Internet. Sending a SIP message is effectively the same as dialing someone's telephone number in the PSTN: both actions can start a phone call. One would use a "SIP" address that looks similar to an e-mail address. For example, a SIP address might look like: "sip:john@tele.cdt.org," and that address could be used to start a telephone call (if both parties have the correct software and VoIP equipment).

One key point to understand about VoIP communications is that in many instances they can be much less expensive than placing a normal telephone call. Assume, for example, that someone has a high-speed connection to the Internet in Washington, D.C., (such as a DSL circuit, a cable modem, or a high speed office connection), and that person wants to talk to a colleague in Hong Kong who also has a high-speed connection to the Internet. If both parties have the proper VoIP equipment,[7] they can today talk to each other over the Internet without incurring *any* additional telephone charges for the phone call.

[5] For background on VoIP technology and the public policy concerns it raises, see "Voice-over-IP: The Future of Communications," Global Internet Policy Initiative, April 29, 2002, http://www.internetpolicy.net/practices/voip.pdf.

[6] As with the ENUM protocol, SIP was developed by the Internet Engineering Task Force, and is described in RFC 2543, "SIP: Session Initiation Protocol," http://www.ietf.org/rfc/rfc2543.txt.

[7] At its simplest, "VoIP equipment" can consist of only a personal computer equipped with speakers, a microphone, and VoIP software. One can also purchase telephone handsets that plug directly into personal computers. On the other end of the spectrum, there are sophisticated VoIP "gateways" that can link large corporate or institutional telephone networks to the Internet.

### B. What Is ENUM?

At its simplest, ENUM is a protocol that defines a method to convert an ordinary telephone number (such as, for CDT, +1-202-637-9800) into a format that can be used on the Internet to look up Internet addressing information (such as, for example, VoIP or e-mail addresses). To accommodate a different convention used in Internet domain names,[8] the ENUM protocol *reverses* the sequence of the digits in an ordinary telephone number (and also assigns a special domain name, "e164.arpa"[9]). Thus, the ENUM format of CDT's telephone number +1-202-637-9800 would be "0.0.8.9.7.3.6.2.0.2.1.e164.arpa." In the remainder of this paper, the term "ENUM number" will refer to a regular telephone number that has been expressed using this inverted ENUM format.[10]

The second key element of ENUM is that the Internet addressing information associated with an ENUM number is stored within the "domain name system" (or "DNS"),[11] providing instructions on how to reach the device associated with a particular ENUM number (which in turn is associated with a particular telephone number). In the remainder of this paper, the terms "ENUM record" and "ENUM DNS record" will refer to records stored in the DNS system according to the format specified in the ENUM protocol.

For example, if CDT's offices used ENUM and were set up to receive "VoIP" calls, then CDT's "ENUM DNS record" would be stored at "0.0.8.9.7.3.6.2.0.2.1.e164.arpa" in the Domain Name System and would point to CDT's VoIP address (say,

[8] In a regular telephone number, the most "significant" numbers appear first – for the United States, the country code "1" is followed by an area code (e.g., 202). In Internet domain names, however, the most significant information appears last – for example, to locate the "www.cdt.org" web site, a computer would first determine the location of the "top level domain" (".org"), then the domain itself ("cdt"), and then the particular server in that domain ("www").

[9] The "e164" refers to the global telephone numbering system established by the International Telecommunications Union. The ".arpa" represents to a top-level domain on the Internet. Historically, it refers to the U.S. Government agency that funded the initial development of Internet technology, and is currently used for certain domain name mapping functions on the Internet. The use of ".arpa" within the ENUM protocol is a point of contention among some non-U.S. countries and providers. *See* Craig McTaggart, "The ENUM Protocol, Telecommunications Numbering, and Internet Governance," Mar. 2003, http://www.innovationlaw.org/cm/ writing/cm-enum-cardozo.pdf.

[10] To be clear, in its basic form there is no separate number that is an "ENUM number" – instead a standard telephone number is converted into a new format using the ENUM protocol. Section II.B.6 below discusses the possibility of ENUM numbers that are *not* related to any existing normal telephone number, but except in that unusual case, "ENUM numbers" are simple normal telephone numbers expressed using the ENUM protocol.

[11] The Domain Name System, or DNS, is the system used to translate a familiar Internet domain name like "www.cdt.org" into a numeric "Internet Protocol" (or "IP") address like 206.112.85.61. As detailed below, the ENUM system grafts wholly new functions onto the DNS, but because of the distributed nature of the DNS system, it is expected that the extra ENUM functions will not significantly degrade the performance of the DNS.

sip:main@tele.cdt.org). Thus, if someone has CDT's telephone number and the appropriate VoIP equipment, they could place a voice call over the Internet by

1. dialing CDT's ordinary phone number, +1-202-637-9800 using a regular phone or a phone-like device,
2. having their computer (or phone system) convert the telephone number into CDT's ENUM number,
3. looking up the ENUM record in the Domain Name System, and then
4. placing a VoIP phone call to sip:main@tele.cdt.org.

With the right software and hardware, these steps happen quickly and seamlessly.

A third key – but optional – element of the ENUM protocol is that *more than one* piece of contact information can be stored in the DNS record that is associated with a particular ENUM number. Thus, an ENUM record associated with CDT might contain instructions for (1) a VoIP voice call (e.g., sip:main@tele.cdt.org), (2) a facsimile call (e.g., mailto:fax@cdt.org or fax:mainfax@fax.cdt.org), and (3) an e-mail communication (mailto:postmaster@cdt.org). Under some conceptions of ENUM, this ability to include multiple contact methods in an ENUM record would allow an ENUM number to be a single contact number that could be given out to support, in theory, any type of communication (voice, fax, e-mail, cellular, SMS text messaging, etc.).

Thus, the ENUM protocol provides, first, a method to use a regular phone number to look up a special type of record in the public Domain Name System, or DNS, and then second, a format to store one or more pieces of Internet contact information associated with that phone number in the DNS. A factor that is crucial to the privacy concerns discussed below is that any information stored in the DNS is completely public and accessible worldwide.[12]

### C. What ENUM Is Not

It is important to recognize what ENUM does *not* do. ENUM does not in any way replace the numeric IP (or Internet Protocol) address that one uses (usually invisibly) to interact with the Internet. Generally speaking, whenever you use the Internet you have an "IP address," which today is most commonly formatted with four numbers separated by dots (such as 206.112.85.61). Depending on your specific type of connection to the Internet, this IP address might never change (a "static IP address"), or might change at regular intervals or whenever an Internet connection in initiated (a "dynamic IP address"). ENUM will alter *none* of this – ENUM users will still connect to the Internet using their normal IP addressing scheme (static or dynamic), and the ENUM protocol will have no affect on what specific IP addresses are used.

[12] It is technically possible to create a "split-brained" DNS server that returns different information depending on the source of the query (and thus some information may not be public), but for the most part all information in the global DNS system is unprotected and publicly available.

Similarly, ENUM does not alter the internal mechanics of how one sends an e-mail, surfs the World Wide Web, or even places a VoIP call over the Internet. Fundamentally, what ENUM does is to provide another way to determine the desired destination to be used to initiate a communication over the Internet. Critically, it does this in a way that bridges – through steps that can be made seamless to the end user – the gap between telephone numbers and, ultimately, IP addresses.

To illustrate this point, consider the mechanics of the transmission of a simple e-mail message. Sending an e-mail over the Internet is – behind the scenes – a two-step process. Assuming that one wants to send e-mail to jmorris@cdt.org, the following two steps would be taken (by the outgoing mail server):

| Step | Basic Process | Detailed Action |
|---|---|---|
| 1 | Look up the destination address ("cdt.org") in the Domain Name System (DNS) | Through one or more requests to the DNS, determine that mail for "cdt.org" is handled by a mail server named "mail.cdt.org," which is located at Internet Protocol address 206.112.85.61 |
| 2 | Transmit the e-mail message directly to the destination mail server | Send the e-mail message to IP address 206.112.85.61 (addressed to user "jmorris" on server "mail.cdt.org") |

The process to initiate a Voice-over-Internet-Protocol (VoIP) telephone call is virtually identical. Assuming that one wants to place a VoIP call using SIP (the Session Initiation Protocol) to jmorris@tele.cdt.org, the following two steps would be taken (by the outgoing VoIP software):

| Step | Basic Process | Detailed Action |
|---|---|---|
| 1 | Look up the destination address ("tele.cdt.org") in the Domain Name System (DNS) | Through one or more requests to the DNS, determine that the SIP server named "tele.cdt.org" is located at Internet Protocol address 206.112.85.61 |
| 2 | Initiate a call directly to the destination SIP server | Send a SIP query to IP address 206.112.85.61, requesting a voice connection to user "jmorris" on server "tele.cdt.org" |

Using ENUM to initiate a VoIP call simply adds one additional step *prior* to Step 1 above. Note that Steps 2 and 3 below are *identical* to steps 1 and 2 above. Assuming that (a) one wants to place a VoIP call to John Morris, (b) one does *not* know John's SIP address, but (c) one does know John's phone number, +1-202-637-9800, the following three steps would be taken (by the outgoing VoIP software):

| Step | Basic Process | Detailed Action |
|---|---|---|
| 1 | Using ENUM, look up the VoIP address in the Domain Name System (DNS) | Retrieve from the DNS the ENUM record for 0.0.8.9.7.3.6.2.0.2.1.e164.arpa and determine that the associated SIP address is "jmorris@tele.cdt.org" |
| 2 | Look up the destination address ("tele.cdt.org") in the Domain Name System (DNS) | Through one or more requests to the DNS, determine that the SIP server named "tele.cdt.org" is located at Internet Protocol address 206.112.85.61 |
| 3 | Initiate a call directly to the destination SIP server | Send a SIP query to IP address 206.112.85.61, requesting a voice connection to user "jmorris" on server "tele.cdt.org" |

The critical point to note is with or without ENUM, the ultimate communication is a direct communication from the calling party's computer to the destination computer. Using ENUM does not change the fundamental mechanics of the communication. Instead, what ENUM provides is (in its simplest form) a way to look up the correct Internet destination using a traditional telephone number.

## D. How Might ENUM Be Used?

ENUM is capable of being used in a number of different ways. The usage that has received the most attention, from the media as well as from the International Telecommunications Union – allowing a single ENUM number to provide access to voice, fax, cellular, and other channels of communication[13] – may well not be the most important initial usage of ENUM. More important might be the second usage described below, facilitating the ability to route telephone calls over the Internet instead of over the regular telephone system.

### 1. Single Number Point of Contact

As noted above, one element of ENUM permits an ENUM DNS record to include multiple methods of contact. Some companies (and perhaps some individuals) are likely to take advantage of this capability. For example, in the United States many real estate agents advertise numerous different contact telephone numbers (such as office, home, mobile, and fax). ENUM would allow a real estate agent to provide VoIP-capable clients with one ENUM number that could reach all of those different points of contact.

[13] For example, see "Consumers could get one number for phone, faxes, Net access," USAToday.com, Feb. 12, 2003, available at http://www.usatoday.com/tech/news/techpolicy/2003-02-13-numbers_x.htm; "Internet Telephone Numbering System (ENUM) offers promise of a single point of contact for all communication devices," Press Release, International Telecommunications Union, May 31, 2002, available at http://www.itu.int/newsarchive/press_releases/2002/NP05.html.

Similarly, some companies may choose to set up ENUM numbers – with multiple contact methods – for the companies' sales forces. Using ENUM, the companies can maximize the possibility that a customer will be able reach a sales person.

This use of ENUM, however, is unlikely to be widespread until VoIP usage becomes widespread – few phones today can take advantage of a single-point-of-contact ENUM number. Even after VoIP usage is widespread, it is far from clear whether this use of ENUM will be popular among individuals. Historically, "find me/follow me" services (which provide similar functionality to this approach to ENUM) offered by telephone companies have not been very successful.

### 2. Transitioning Away from the Traditional Telephone System

The first broad use of ENUM will more likely be to facilitate the transition away from the PSTN and to the Internet as the primary carrier of voice communications. This transition will likely occur first with large corporations and institutions that operate large internal telephone networks, as well as "early adopting" smaller companies and individuals. If this initial deployment of ENUM proves to be both technically successful and economically beneficial, the use of ENUM may move to smaller companies and a broader range of individuals.

#### a) Corporate Bypass of the PSTN

ENUM may initially see widespread adoption with large- and medium-sized corporations (and other institutions) seeking to reduce telephone costs by using VoIP for voice calls (and thereby bypassing local and long distance telephone companies). Corporations could implement ENUM entirely behind the scenes, and route some (but not all) phone calls over the Internet instead of the normal telephone network (the PSTN). A typical corporate implementation of ENUM would allow seamless routing of phone calls along the following lines:

1. An employee picks up an ordinary office phone and dials a number, using the familiar PSTN dialing format (e.g., "12026379800").
2. The call is first routed to a switch in the internal corporate phone system that operates as a "gateway" to the Internet.
3. The internal gateway switch does an ENUM lookup in the Domain Name System on the public Internet.
4. If an ENUM record is found, the internal switch initiates a VoIP call to the destination using the Internet (entirely bypassing the PSTN).
5. If no ENUM record is found, the internal switch connects the call to the local telephone company for completion over the PSTN.

All of this could take place in milliseconds, and be completely invisible to the employee placing the call. As more and more branch offices, customers, suppliers, and other corporate partners establish gateways between the Internet and their internal telephone systems, a company would be able to push more and more voice traffic over the Internet, thereby lowering the volume and cost of service the company must obtain from traditional phone carriers.

#### b) Individual Bypass of the PSTN

Just as corporations may use internal telephone systems to bypass the local telephone service, individuals will likely be able to install Internet-to-telephone equipment in their homes and, in conjunction with VoIP and ENUM-based technology, may be able to reduce their usage of traditional telephone services. As with corporations, the more of an individual's friends, family, and colleagues who use similar Internet-based voice services, the more potential that the individual can save money.

Some currently available commercial services work by routing *all* voice traffic from a home over the Internet to a central switching facility, which in turn routes the call to completion over the Internet or over the PSTN. In this scenario, an ENUM lookup would likely take place from the central facility rather than from the customer's home.

### 3. Internal Routing of Calls Within a Telephone Company's Network

Similar to the "bypass" uses discussed above, another use of ENUM may take place entirely behind the scenes within a traditional telephone company's network.[14] Increasingly, the leading long distance companies in the United States are converting over to carry voice calls using VoIP. These companies may use the ENUM specification to create their own *wholly internal* version of the Domain Name System (DNS), and then use ENUM to assist in routing telephone calls with their own networks.

### 4. Dialed Access to New Internet Services

ENUM may also be used as a convenient way to access new Internet services from cellular telephones and other devices that lack a full computer keyboard. For cellular telephones that also have access to Internet services, users may have to use cumbersome methods to enter an Internet URL (like www.cdt.org). Service providers that are targeting wireless uses may offer an alternative method of access, by allowing users simply to dial a telephone number that can be translated – using ENUM – into the desired Internet address.

[14] In strict technical terms, any use of the ENUM protocol that does *not* use the public DNS system is not in fact an implementation of ENUM. The focus of the public policy concerns below is on the use of ENUM in conjunction with the public DNS system. If the ENUM protocol is being used for purely internal purposes within a single communications service provider, the provider must ensure that personally identifiable information remains confidential.

## E. Two Technical Approaches to ENUM Implementation

For any of the anticipated public uses of ENUM (but most importantly for the "bypass" uses), there is a critical choice to be made about how ENUM will be implemented – a choice that directly affects the privacy issues discussed below. There are two fundamentally different conceptions of how ENUM might be implemented, where one approach allows the "calling party" (the person placing a call) to control how the call will be connected, and a second approach that places the control with the "called party" (the person being called). These two models are not mutually exclusive – both can be used at the same time – but they do have important differences from the perspective of privacy.

### 1. Calling Party Control Model – Using ENUM Alone

In the Calling Party Control model, the amount of data entered into an ENUM record is maximized – all available forms of contact (such as voice, mobile, fax, e-mail, etc.) are placed in the Domain Name System (DNS) record. This allows the person initiating the contact (the "calling" party) to choose which of the forms of contact to use. This approach to ENUM is illustrated in Figure 1 below:

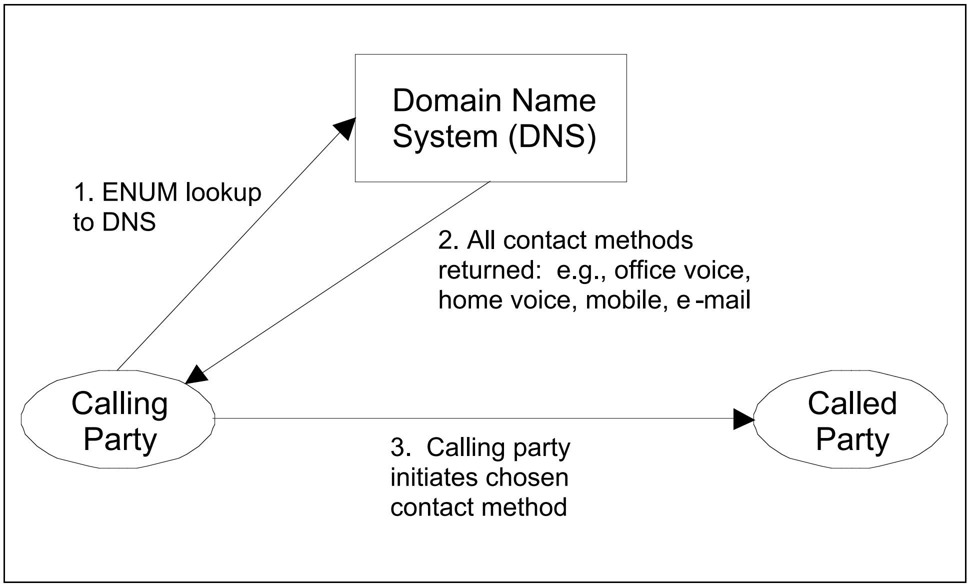
Domain Name System (DNS)
1. ENUM lookup to DNS
2. All contact methods returned: e.g., office voice, home voice, mobile, e -mail
Calling Party
Called Party
3. Calling party initiates chosen contact method

**Figure 1: ENUM Using "Calling Party Control" Approach**

The critical aspect of the "calling party control" approach is that the person initiating the call *always* receives all possible contact methods, and can choose which to use.[15] In addition, the calling party may retain all of the information and use it for other purposes.

[15] To be clear, in most cases this interaction will take place between the *client software* of the Calling Party and the DNS system. In other words, the Calling Party's software will receive all possible contact methods from the DNS system, and can either choose which method to use according to the Calling Party's previously expressed instructions, or offer the (human) Calling Party a direct choice.

### 2. Called Party Control Model – Using ENUM with a Proxy Server

In contrast to the "Calling Party Control" model, the "Called Party Control" approach imposes constraints on the calling party's access to data about the called party. Only a single method of contact is placed in the DNS record, and that contact method points only to a "proxy server," which can perform screening or other functions set by the person being called (the "called" party). A common implementation of this approach would use the "Session Initiation Protocol" (or "SIP") to run the proxy server, and thus the server would be termed a "SIP server."[16]

In this approach, the calling party first submits a query to the DNS system, and receives back a pointer to the called party's proxy or SIP server. The calling party would then contact the proxy/SIP server, and that server – based on rules set by the called party – would decide what contact method (*if any*) should be provided to the calling party.

This approach allows the person being contacted (the "called" party) to choose which of the forms of contact to use, if any. This approach to ENUM is illustrated in Figure 2 below:

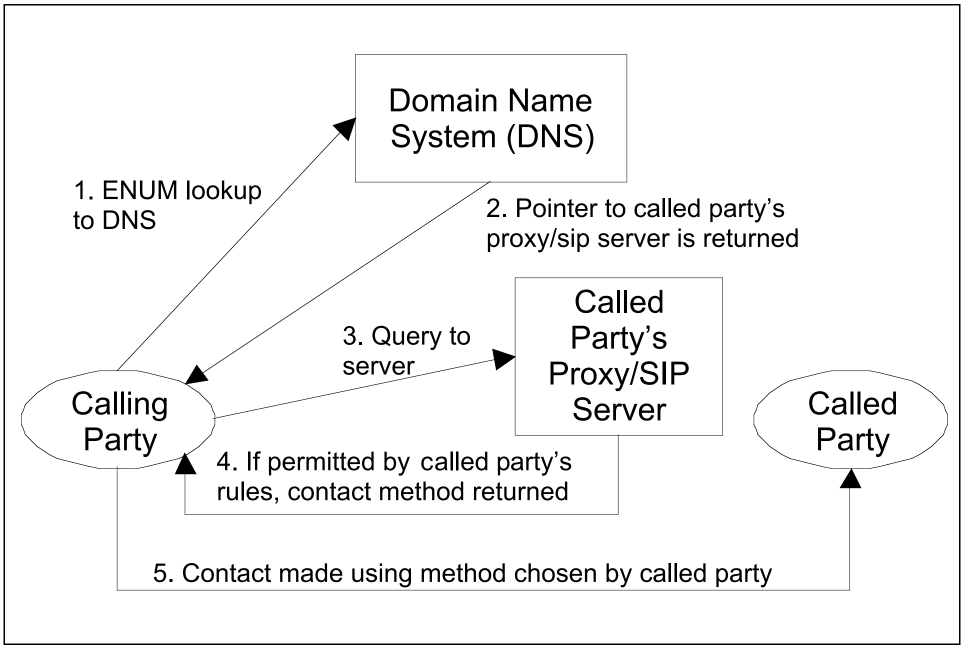
Domain Name System (DNS)
1. ENUM lookup to DNS
2. Pointer to called party's proxy/sip server is returned
3. Query to server
Called Party's Proxy/SIP Server
Calling Party
Called Party
4. If permitted by called party's rules, contact method returned
5. Contact made using method chosen by called party

**Figure 2: ENUM Using "Called Party Control" Approach**

[16] As a technical matter, this "Called Party Control" approach only uses the ENUM protocol to point to a proxy or SIP server. The operation of these servers is not part of the ENUM technical specification. Thus, "Called Party Control" is essentially the use of ENUM in conjunction with a separate proxy service. What is critical from a public policy perspective is that an ENUM user be permitted to create an ENUM record that points only to an external proxy or SIP server.

The critical aspect of the "called party control" approach is that the called party chooses whether and how the contact can be made.

This Called Party Control model can be implemented by having the called party contract with a third party service provider to operate a proxy/SIP server on behalf of the called party. Alternatively, the called party can operate proxy/SIP server equipment on its premises. This approach might be common in the case of a large corporation. As such servers become more common, they may also be built into individuals' computers or in "small office/home office" servers.

Within a proxy or SIP server would be rules or scripts that define how a call is to be processed, and who is permitted to receive details on specific contact methods (such as voice, fax, e-mail, etc.). For example, hypothetical rules could state that:

1. Anyone can receive my office VoIP address at anytime
2. Colleagues from my company can receive my cellular phone number during business hours on weekdays
3. My family can receive all contact methods at any time

The ultimate ENUM end user would likely be able to define these and other rules (such as call forwarding, etc.) through a World Wide Web site. To be clear, SIP-based services are today only in the early stages of their evolution and refinement, and so the details of what rules might be possible and how those rules might be implemented are not certain. In particular, it is not yet clear how individuals in a particular group (e.g., "my family") will be able to "authenticate" themselves are part of an exchange with a SIP proxy. A range of possible authentication technologies is under development.

In both the Calling Party Control and Called Party Control models, the queries to and responses from the DNS and the proxy/SIP servers all happen essentially instantaneously. A telephone call placed using ENUM, as implemented in either of these models, would likely be connected as quickly as with the normal telephone system.

### 3. Using Both Models at the Same Time

The "calling party control" and "called party control" approaches are not mutually exclusive – both could be used together. First, any ENUM service provider would be able to offer to customers both models of ENUM usage. The fact that one customer chooses to use the "calling party control" model would have no bearing at all on another customer's ability to choose the "called party control" model. As discussed more fully below, we believe it is important that both models be available in the marketplace.

Moreover, a single ENUM user would be able to use both models within the same single ENUM DNS record. For example, a user might choose to made his or her office telephone number and office fax number widely available, but might prefer to keep his or her e-mail address, cell number, and home number more closely guarded. In this hypothetical, the user could place three contact methods in the publicly available ENUM DNS record: (a) an office number, (b) and office fax number, and (c) a pointer to a proxy/SIP server. A calling party could choose to use either of the two office numbers, or could choose to submit a query to the proxy/SIP server, which would in turn only provide more contact information according to rules set by the called party. Thus, the ENUM user would gain the benefit of widespread availability of his or her office numbers, while retaining control over who can access the other methods of contact.

### F. What Transaction Data Would Be Available About ENUM-Facilitated Calls, and Where Would Such Data be Located?

ENUM service providers likely would not be able to keep records of individual calls, and indeed would likely not even be aware of any particular use of ENUM to facilitate a communication. The primary task of an ENUM service provider would be to ensure that accurate, authorized, and correctly formatted data is entered into an ENUM DNS record for a given ENUM subscriber. Once the DNS record is created, the ENUM service provider would need to have no involvement in any ENUM-facilitated communication.[17] In this regard, ENUM is like ordinary "directory assistance" on the telephone network – once a directory assistance service provides a number to a caller, the service is not involved in, and cannot track, a call placed to the number given (unless the caller chooses to have the service provider connect the call). The ENUM lookup and the communication based on ENUM data are two separate, sequential transactions.

More generally with regard to VoIP calls (whether ENUM is used or not), there is no technical requirement that necessitates that any transaction data be collected and recorded by any commercial entity. A VoIP call can be placed over the Internet on a direct computer-to-computer basis, without involving any special "VoIP service." There do exist, however, commercial VoIP service providers that offer to link VoIP calls to the PSTN, and those providers may create and maintain individual call records (especially if they bill their customers on a per call basis). It is also possible that some server logs might reflect a given VoIP communication, but nothing in the ENUM or SIP specifications would lead to the creation of such records. Technical and policy issues concerning the retention of server logs in the ENUM or SIP are essentially the same as the issues raised in the context of web surfing and e-mail.

Calls placed using ENUM or SIP, and transactional data associated with those calls, would be susceptible to interception by law enforcement authorities, using the same tools and techniques used to intercept Internet traffic more generally. ENUM and SIP neither facilitate nor inhibit such surveillance.

[17] If an ENUM service provider maintains a DNS server, the provider *might* have server log entries related to some initial DNS queries. But given the architecture of the DNS system, the provider would likely not be aware of subsequent ENUM DNS queries.

## G. How Will ENUM Numbers Be Administered?

Underlying the structure of the ENUM protocol is the assumption that sovereign nations should separately control the implementation of ENUM for their respective "country codes," just as those nations control the numbering under the standard telephone system. Thus, for example, the international dialing country code for Germany is 49, and by international agreement Germany controls the numbering for any telephone numbers accessed using the 49 country code. The ENUM protocol will be implemented in keeping with this system of national control, such that Germany will control the handling of any ENUM numbers that reference country code 49 (which in the ENUM format would have an entry in the Domain Name System that *ends* with "9.4.e164.arpa"). The International Telecommunications Union ("ITU") has responsibility for designating – based on instructions from each country – what entity will control ENUM implementation within each country.

Thus, most rules governing the creation and control of ENUM records for each separate country code will be set by each separate nation, in whatever manner the country deems appropriate. This means that decisions such as whether "called party control" will be available within an area would in most cases be made on a nation-by-nation basis.

For the United States, Canada, and certain Caribbean countries, this approach is complicated by the fact that country code "1" covers all of them, and thus any handing of ENUM numbers ending in "1.e164.arpa" will initially apply to all countries in country code "1." The way that the DNS system and the ENUM protocol work, however, the administration of ENUM numbers within a given country code (such as "1") can be delegated down to the area code level (or farther down, if desired). Thus, a Canadian authority will be able to control ENUM numbers that, for example, relate to area code 416 in country code 1 (which is Toronto, Canada, in the standard telephone system) – that authority would thus control all ENUM numbers that end with "6.1.4.1.e164.arpa."

## H. What is the Current Status of ENUM Deployment?

ENUM is not currently deployed and commercially available anywhere in the world. ENUM "trials" are on going in a number of countries, including Australia, Austria, China, France, Germany, Korea, Netherlands, Sweden, Switzerland, and the United Kingdom. Typically, these trials are being operated by would-be ENUM service providers and telephone carriers to allow the various networks and companies to test how ENUM would operate if fully deployed. In some countries, these tests have generated significant concern among privacy advocates and other public policy organizations.[18]

[18] For example, the ENUM trial in Australia has prompted a number of reports raising broad privacy and other policy concerns. *See* Roger Clarke, "ENUM - A Case Study in Social Irresponsibility," Mar. 2003, http://www.anu.edu.au/people/Roger.Clarke/DV/enumISOC02.html; Australian Privacy Foundation, "Submission to the Australian Communications Authority," Nov. 2, 2002, http://www.privacy.org.au/Papers/SubmnACA021102.html; Electronic Frontiers Australia, "Submission to the Australian Communications Authority," Nov. 18, 2002, http://www.efa.org.au/Publish/efasubm-enum.html.

In the United States, no formal ENUM trial has been approved or initiated by the U.S. Government. In February 2003, the U.S. Department of Commerce issued a letter endorsing U.S. participation in ENUM, and setting out a series of "guidelines" that the Department believes should be followed in any U.S. implementation of ENUM, including a guideline on privacy:

> **Protect users' security and privacy:** Domestic implementation of ENUM must be done in a manner that maximizes the privacy and security of user data entered in the ENUM DNS domain. For example, ENUM providers should develop systems to ensure the authentication and authorization of users who enter and update their personal information.[19]

As in other countries, United States privacy advocates have also expressed concerns about ENUM.[20] Within the U.S., the leading companies interested in implementing ENUM have formed an organization named the ENUM Forum. The ENUM Forum has developed and published proposed plans for the implementation of ENUM in the U.S., including provisions that address some, but not all, of the privacy concerns raised below.[21]

## II. Privacy and Other Public Policy Concerns Raised by ENUM

Public policy concerns about ENUM can be divided into two categories: (1) privacy concerns that are inherent in design of the ENUM protocol itself, and (2) privacy and other concerns that largely depend on how ENUM will be implemented within each particular country.

In the United States and throughout the world, the privacy of information is typically guided by principles of "fair information practices." Most authoritatively detailed by the Organization for Economic Co-operation and Development (OECD),[22] these principles represent basic guidelines for responsible information practices that respect the

[19] Letter from Nancy J. Victory (Department of Commerce) to David A. Gross (Department of State), Feb. 12, 2003, http://www.ntia.doc.gov/ntiahome/ntiageneral/enum/enum_02122003.htm.

[20] *See* Electronic Privacy Information Center, "EPIC Comments on Privacy Issues in ENUM Forum 11-01-02 Unified Document," Nov. 2002, http://www.epic.org/privacy/enum/enumcomments11.02.html.

[21] *See* ENUM Forum, "ENUM Forum 11-01-02 Unified Document," Nov. 1, 2002, http://www.enum-forum.org/documents/6000_0_8.doc.

[22] *See* OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, http://www.oecd.org/EN/document/0,,EN-document-0-nodirectorate-no-24-10255-0,00.html. The OECD principles were in turn based on the Code of Fair Information Practices developed in the 1970s by the U.S. Department of Health, Education and Welfare. *See* U.S. Dept. of Health, Education and Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, July 1973.

privacy interests of individuals.[23] They form the foundation of national and local privacy laws and are incorporated into industry codes of best practices, as well as the underpinnings of international agreements on data protection. Finally, they provide a framework that, if followed in implementations of ENUM, can protect privacy by limiting data collection to that which is necessary for transactions and ensuring that individuals are the arbiters of their personal information.

A set of public policy issues raised by ENUM that are *not* addressed in this paper concern the administration and control of the Domain Name System, and the question of whether there should be a single "root" for ENUM numbers in the DNS (and whether that

[23] As expressed by the OECD, fair information practices include:

> 1. Collection Limitation: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> 2. Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> 3. Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> 4. Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.
>
> 5. Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
>
> 6. Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> 7. Individual participation: An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him:
>
> - within a reasonable time;
> - at a charge, if any, that is not excessive;
> - in a reasonable manner; and,
> - in a form that is readily intelligible to him;
>
> (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
>
> 8. Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.

http://www.oecd.org/EN/document/0,,EN-document-0-nodirectorate-no-24-10255-0,00.html.

root should be "e164.arpa" as current defined by the Internet Engineering Task Force). A key question raised is how competing "ENUM-like" services should interrelate with the ENUM standard. These policy issues are extensively discussed in other literature.[24]

## A. Privacy Concerns Raised by the Core ENUM Protocol

The entire ENUM protocol is based on a simple and unavoidable premise: contact information is stored in the global Internet's Domain Name System (DNS). Because the contents of a DNS record can be accessed by anyone at anytime, any contact information stored in an ENUM DNS record is completely exposed to the world. Thus, to the extent that the ENUM information contains personally identifiable information, ENUM raises a significant privacy concern.

This privacy concern is heightened when an individual or company chooses to place *multiple* contact methods in the ENUM DNS record. In such a case, *all* of the contact information is available to the world. Such broad disclosure of, for example, telephone and fax numbers could result in unwanted telemarketing, and the inclusion of an e-mail address in the ENUM record would likely lead to an increase in unsolicited commercial e-mail (or "spam") to the revealed e-mail address.[25] In some cases, the disclosure of private information could create significant risk of harm to the user.

For some individuals or companies, the value of providing clients, customers, family, or friends with multiple contact methods may outweigh the privacy implications of revealing all of the contact information to the world. Real estate agents in the United States often already post multiple telephone numbers (for office, home, mobile, fax) and an e-mail address on their web sites. For those individuals and companies, the privacy risk posed by ENUM data in the DNS will likely be acceptable.

But for many other people, the exposure of personal contact information through an ENUM DNS record will *not* be acceptable. Thus, for those people to take advantage of the benefits that ENUM offers, it is critical that any national implementation of ENUM permit the "Called Party Control" model discussed above. With this approach to ENUM, an individual's actual contact information can be protected behind a "proxy server" that will only disclose portions of the contact information according to rules and procedures set by

[24] For a recent and comprehensive look at these policy issues, see Craig McTaggart, "The ENUM Protocol, Telecommunications Numbering, and Internet Governance," Mar. 2003, http://www.innovationlaw.org/cm/ writing/cm-enum-cardozo.pdf. For additional references and links concerning these issues, see the listing under "ICANN" on the Washington Internet Project ENUM Page, http://www.cybertelecom.org/dns/enum.htm.

[25] ENUM records in the DNS will likely be "mined" for data even more readily than similar information is obtained today off of web sites. *See* "Why Am I Getting All This Spam?," Center for Democracy & Technology, March 2003, available at http://www.cdt.org/speech/spam/030319spamreport.pdf (discussing mining of e-mail records off of web pages). This is because – in an ENUM DNS record – the telephone numbers, e-mail addresses, and other contact information must be in precise, machine-readable formats, and thus that information cannot be conveyed in an unconventional (and thus less machine-readable) format, as it can be conveyed on a web page.

the called party. These rules could, for example, permit access to a home or mobile telephone number only by specified individuals or groups.

The key to the "Called Party Control" model is that *no* personally identifiable information is revealed in the Domain Name System (DNS). Instead, the only information that is publicly viewable is the Internet address of the Called Party's proxy or SIP server. All other information is protected behind the referenced server.

Even with "Calling Party Control" implementations of ENUM, it will be critical that each ENUM user be able to control what information is listed in the ENUM record. Thus, a user may choose to list office voice and fax numbers in the ENUM DNS record, but may choose to omit an office e-mail address, because of the significant risk of "spam" that will likely arise from any ENUM record containing an e-mail address.

## B. Public Policy Concerns Raised by the Administration of ENUM

The privacy issue discussed above arises because of the technical design of the ENUM protocol (because contact information is placed in the publicly available DNS system). A host of other privacy and public policy concerns will arise out of the administration of ENUM, including the registration of ENUM numbers and control over information in ENUM DNS records.

### 1. Opt-In Requirement for ENUM

Proponents of ENUM have generally assumed that ENUM will be implemented as an "opt-in" service. In other words, the general expectation is that no ENUM record at all will be created for a given telephone number without the consent of the subscriber using that number.

An "opt-in" approach, however, is not guaranteed. There is nothing in the technology that would prevent either (a) the wholesale inclusion of *all* phone numbers within a given jurisdiction in an ENUM system, or (b) the inclusion of individual phone numbers without the consent of the telephone subscriber. These are policy choices.

Because ENUM will be separately implemented by hundreds of national telephone authorities around the world, the question of consent must be separately considered in every jurisdiction. For example, if a state telephone monopoly in a country is converting its internal network to "voice over the Internet" technology, the monopoly may prefer to register, on a wholesale basis, all phone numbers into a national ENUM system. Such a wholesale registration of ENUM numbers would most likely be done using the "Calling Party Control" model, which places telephone contact information directly into the DNS system. In such a scenario, individuals with unlisted or unpublished numbers would find their previously private phone numbers listed as accessible through the DNS system (although the subscribers' names would not necessarily be listed in the DNS system).[26]

[26] Of course, even in the traditional PSTN, unlisted telephone numbers can still be dialed, and thus using sequential autodialers marketers can still reach unlisted numbers. Nevertheless, PSTN subscribers

We recommend that ENUM be implemented on an "opt-in" basis, not on the basis of blanket or automatic inclusion. It is also important that any "opt-in" by a user be based on a full understanding of the privacy implications and risks raised by ENUM, and that the opt-in decision be explicitly made.

Assuming that ENUM is implemented on an "opt-in" basis, however, does *not* obviate the need to address the other privacy and policy issues discussed here. If ENUM becomes widely accepted and used within society, the "opt in" choice ceases to be voluntary – in other words, if ENUM becomes an important part of a society's system of communication, then it is no longer optional. Specifically, although today VoIP technology can be used without ENUM, it is possible that ENUM will become an essential tool for using VoIP, and if so, then ENUM usage will effectively become mandatory. Thus, the fact that appropriate implementations of ENUM should be done on an "opt-in" basis does not eliminate the need to address other privacy and policy concerns raised by ENUM.

### 2. Privacy of Registration Information

A critical question affecting the privacy (or lack of privacy) of an ENUM system will turn on (a) what personal information is required to obtain an ENUM record, and (b) whether any of that information will be accessible in a public database.

Arguably, an ENUM DNS record is analogous to the DNS record that points to a site on the World Wide Web. In the case of a domain registration for a web site, the owner of the domain is required to list – in the wholly public "whois" database – current contact information, including (for an individual) a home address (raising a host of privacy concerns).[27]

If similar information is required in a whois-like database in order to enter an ENUM record in the DNS, then the harmful privacy risks posed by ENUM are greatly magnified. The entire idea behind the "Called Party Control" model discussed above – to hide personal information behind a server controlled by the called party – would be completely defeated if personal information must be publicly disclosed in order register for an ENUM record in the first place.

There is, however, no reason that information about the ultimate ENUM subscriber (the registrant, to use the terminology from the domain name context) should be placed into a whois-like database in the first place. Most of the reasons given to justify the whois database (as it relates to normal web domain names) simply do not apply to ENUM

(unlisted or not) should not have their numbers entered into the ENUM system without prior consent. A risk posed by ENUM is that the privacy of unlisted numbers could be diminished by the automatic inclusion of all number in the ENUM system.

[27] The whois database and the personally identifiable information that it contains raise privacy concerns, but those concerns are not the focus of this paper.

records. For example, there is no chance that anyone will have a trademark or other intellectual property interest in an ENUM number (which is simply a string of numbers). Because ENUM numbers are not used to "host" content (as with the World Wide Web), copyright owners would not need to be able to identify the owner of a web site that might be infringing on a copyright. Finally, because the allocation of ENUM numbers is controlled, ultimately, by a central national authority, there is no need (as with domain names) to be able to quickly determine the domain name provider (or registrar) that created the domain.

*One* of the justifications for the whois database in the domain context *would* apply in the ENUM context. There would be a need to be able to troubleshoot technical problems in an ENUM DNS record. At most, however, the only information needed about an ENUM registration would be a *technical* point of contact, which could point to a technical contact at the relevant ENUM service provider or, in some cases, the ENUM number registrar (a company that assigns ENUM numbers to end users). Such a technical contact could assist in troubleshooting ENUM calls.[28] Thus, although there is value in having a publicly available database of *technical* contacts, there is simply no need for such a database to contain information about the identity of the ultimate subscriber/user of the ENUM record.[29]

Of course, the authority and/or company (or companies) responsible for registering ENUM records within a given country would need to maintain an internal database of ENUM subscribers (just as a traditional telephone company today maintains internal records of telephone subscribers). But that data can and should be protected from disclosure by strict privacy rules.

By avoiding a whois-like database, the ENUM protocol can reasonably support the concept of "unlisted" or "unpublished" numbers. The fact that a particular ENUM number exists within the DNS system would be unavoidably public, but no publicly available identity needs to be associated with that ENUM number.

[28] Such a database of technical contacts would satisfy the arguable need that law enforcement might have to determine who is using a particular ENUM number, because the technical contact information would indicate what company has the identity of an ENUM user in a private database. Armed with the technical contact information, law enforcement could use lawful process to order to obtain, in an appropriate case, the disclosure of the identity of the ENUM user.

[29] Any database, even of technical contacts, should not be created using the current whois database. Any whois-like information to be stored in a public database should be stored in a more secure and less freely available form, such as that being defined by the "Cross Registry Information Service Protocol" (or "crisp") Working Group of the Internet Engineering Task Force. *See* http://www.ietf.org/ html.charters/crisp-charter.html. But even if a more secure crisp-like structure is used, there is no compelling justification to require that the identity of the ultimate ENUM users be disclosed in a publicly available database.

### 3. Control over ENUM DNS Records

It is important that ENUM subscribers have easy, quick, and direct control over the contents of their ENUM records. Because an ENUM record can, in some cases, disclose important personal information, the authorized subscriber must be able to make changes to that information, and the changes must be promptly implemented through the DNS update system.[30] Such control could be implemented through a secure web interface.

Along with the ability to change information in an ENUM record, an ENUM subscriber must be fully and clearly informed about the privacy consequences of ENUM record changes. At the time any information is entered into an ENUM record, the ENUM subscriber should clearly understand that data in the ENUM DNS record would be publicly available.

Some users of ENUM may not want to control their ENUM records directly, or may not understand how the DNS and ENUM systems work. To avoid inadvertent or unintended disclosures of private information, it is important that any ENUM registration system must default to privacy-protecting options. Thus, by default, the least amount of information should be disclosed in the ENUM DNS record, and any greater exposure must follow a clear explanation of the privacy risks.

### 4. Authority to Change ENUM DNS Records

On the flip side of the need for direct and effective user control of the information in an ENUM record is the critical need to ensure (a) that only authorized ENUM subscribers can make changes to an ENUM record, and (b) that those changes are made in a secure framework. The power to change an ENUM record will inherently include the power to redirect all communications to a new destination, and such power should obviously only be wielded by individuals with clear authority to edit the ENUM record.

Thus, for example, one person should not be able to change another person's ENUM record without specific and verified authority. We note that the mechanisms for providing this type of authentication and authorization online are still for the most part poorly developed.

### 5. Control over Registration of ENUM Numbers

Within each country (or more precisely, within each existing PSTN country code), the national telephone authority will have to decide what entity or entities will administer the registration of ENUM numbers. Given the structure of ENUM and the DNS, authority within a country code could theoretically be delegated at an area- or city- code level (in

[30] Any ENUM subscriber, however, must understand that as with the normal DNS system, it can take more than two days for changes to ENUM DNS records to be propagated throughout the Internet.

other word, one entity could have responsibility over one or more area codes, and another entity could have responsibility over a different set of area codes).

Among the specific questions that a national authority must answer are:

a. Will the ENUM registration authority be administered in a tiered system as is used with domain name registries and registrars, such that one or a few entities have ultimate control over ENUM numbers, but a larger number of private companies can offer ENUM numbers and services directly to the public?

b. Will the registration authorities be governmental or private entities?

c. Will existing local telephone companies have a role in the registration of ENUM numbers, and if so, how much influence can those companies exert over the types of services that can be offered using ENUM?

d. Will small or startup companies be able to offer ENUM numbers and services, thereby maximizing the potential for innovative services?

The answers to these questions may vary depending on the country and the structure of the existing PSTN. In the United States, a tiered structure involving private companies is likely to best promote innovation and competition among providers of ENUM-related services.

On the question of whether the existing local telephone companies should have a role in the registration of ENUM numbers, the answer in most cases will be "yes" (although that role may not necessarily be an exclusive role). A key theory of ENUM is that one's normal PSTN telephone number can be translated into an ENUM number, and thus the phone number can be used on either the PSTN or over the Internet. To accomplish this, and to avoid other significant potential problems, the registration of an ENUM number corresponding to an existing telephone number should be restricted to the subscriber of that number. Thus, any telephone company that currently assigns to end users phone numbers on the PSTN will have to play a role in ensuring that ENUM numbers are controlled by the authorized users of the corresponding PSTN numbers. It is vitally important, however, that telephone companies not be able to (a) dictate how ENUM numbers will be used, or (b) erect barriers to the use of the ENUM numbers for particular uses (such as to bypass traditional telephone companies).

### 6. Specific Policy Questions about ENUM Numbering

As suggested above, the standard rule will be that a specific ENUM number is available only to a user who has the corresponding PSTN telephone number. ENUM will, however, raise a host of difficult questions about "number portability" and other numbering issues. Among the questions raised in any ENUM implementation will be:

a. Can a user retain an ENUM number once he or she no longer subscribes to the local telephone number over the PSTN? Initially, ENUM users will likely obtain ENUM numbers that correspond to their existing telephone numbers, and will retain both the PSTN and the ENUM service. Once ENUM (and VoIP more generally) become more widely used, however, an ENUM user may no longer want to continue to maintain local phone service through the PSTN. Will such a user be able to retain his or her long-held ENUM number (recognizing that such retention would almost certainly mean that the number could *not* be reassigned within the PSTN)?

b. Similarly, can a user retain an ENUM number if he or she moves to a wholly new location (with wholly new area codes)? If a user has lived in a particular location for many years, and the user's ENUM number is well known and heavily used, can the user retain the number if the user moves out of town (or out of the country)?

c. Can a user obtain a new ENUM number in a particular area code without ever subscribing to the corresponding PSTN number?

There are important competing considerations raised by these questions. On the one hand, allowing flexible "number portability" (such as the ability to keep a particular ENUM number even if a subscriber no longer uses the corresponding PSTN number) could facilitate greater competition in markets to provide voice services (whether PSTN or Internet based). Such flexibility might more generally speed the deployment of VoIP services.

On the other hand, all of the above scenarios would effectively "tie up" a PSTN number even if it was not being used, and thereby exacerbate the potential for a shortage of local telephone numbers (which in turn creates pressure to split area codes). Moreover, it is not readily apparently what a geographically-identified ENUM number (such as one ending in 2.0.2.1.e164.arpa, which might suggest the Washington, D.C. area) would mean if such a number were not related to a corresponding PSTN number. In this hypothetical, such an ENUM number would *not* be reachable using the normal PSTN in area code 202. It is likely that disassociating geographically-suggestive ENUM numbers from their PSTN counterparts would create confusion about whether one can reach that number over the PSTN. Moreover, there would not, in fact, be any geographical significance to such an ENUM number, because it could point to methods of contact anywhere in the world.

Notwithstanding these questions, there is a value in permitting the creation of ENUM numbers that are independent of any pre-existing PSTN numbers. There will certainly be situations where ENUM numbers can be valuable even where there is no need for any corresponding PSTN line. Thus, there should be the capability to obtain an ENUM number that is wholly divorced from the existing PSTN numbering plan. Such an approach could be implemented both globally (by the creation of one or more ENUM-specific "country codes") and within a given country (by the creation of ENUM-specific "area" or "city" codes). This type of ENUM number would allow someone to choose to have a persistent ENUM number, which they would retain no matter if or where they have a standard PSTN number. Critically, this type of ENUM number would also allow the creation of numbers that are anonymous as to the geographic locale of the user. To avoid numbering conflicts, the creation of such ENUM-specific numbers would have to be coordinated with the International Telecommunications Union (for ENUM-specific country codes) and/or with the national numbering authority (for ENUM-specific area or city codes).

### 7. National Administration and Oversight

In light of all of the issues discussed above, it is clear that the administration of and oversight over ENUM will require careful attention. There is a range of possible ways to implement ENUM, and certain of the approaches could be very harmful to privacy and other policy concerns. It is thus vital that the rules to govern the administration of ENUM within a particular country be developed in close consultation with the public interest and civil society sector, the communications industry, and the Internet industry.

## C. Public Policy Requirements For ENUM Implementations

It is vital that ENUM be implemented with great care and sensitivity to privacy and other public policy concerns. Below are specific policy recommendations that the Center for Democracy & Technology believes should be followed in any ENUM implementation:

a. The "Called Party Control" model should be a meaningful option within any country's implementation of ENUM. Thus, there should be no structural or administrative barriers to the provision of "Called Party Control" service. Specifically, ENUM subscribers should be permitted to create ENUM records that point *only* to proxy or SIP servers. See Section II.A above.

b. In particular, (i) small and startup companies should be permitted to offer effective "Called Party Control" ENUM services, and (ii) individuals who choose to operate their own proxy/SIP servers (to provide "Called Party Control" functionality to themselves) should be permitted to do so without significant administrative barriers. See Sections II.A, II.B.5 above.

c. At no time should *any* ENUM record be created without the express consent of the individual or entity that subscribes to the corresponding telephone number on the PSTN. An ENUM user should explicitly "opt-in" to the ENUM service. The only exception to this rule should be in cases where a telephone company or VoIP service provider creates a *wholly internal and completely private* ENUM system (including a wholly private DNS-like database) to be used to route calls of subscribers. See Section II.B.1 above.

d. Prior to any "opt-in" by a potential ENUM subscriber, the subscriber should have full notice of the privacy risks of ENUM, and the available ways to reduce or control those risks (including, for example, the "Called Party Control" model). See Section II.B.1 above.

e. No publicly accessible whois-like database of ENUM subscribers should be created. Any publicly accessible database of *technical* contacts should not require personal information about the ultimate ENUM subscribers. Any internal database of ENUM subscribers maintained by an ENUM service provider should be maintained with full security and privacy protections. See Section II.B.2 above.

f. An individual who chooses to operate his or her own proxy/SIP server (to provide "Called Party Control") should be able to do so without providing personally identifiable information in a publicly available whois-like database (even one limited to technical contacts). See Sections II.B.2, II.A above.

g. A reasonable equivalent of an "unlisted" or "unpublished" telephone number should be available in any ENUM implementation. See Section II.B.2 above.

h. ENUM subscribers should have direct, easy, and quick access to and control over the information in their public ENUM records. Subscribers, however, should also be advised that changes to an ENUM DNS record will take one to three days to propagate throughout the global DNS system (which is standard for any changes to the DNS). See Section II.B.3 above.

i. At the time ENUM subscribers make changes to their public ENUM DNS records, they should receive clear notice of the privacy risks and consequences of their changes. See Section II.B.3 above.

j. ENUM records should default to a privacy protecting state in the absence of express subscriber changes or input. See Section II.B.3 above.

k. Changes to ENUM records should be done in a secure and authenticated manner to ensure that only authorized individuals can change an ENUM record. See Section II.B.4 above.

l. Control over the registration and administration of ENUM numbers should be structured in a way to (a) maximize the ability of a diversity of service providers to compete in the provision of VoIP and ENUM services, and (b) minimize the ability of existing telephone entities to create barriers to competition in the provision of voice services. See Section II.B.5 above.

m. ENUM users should be able to obtain ENUM numbers that are wholly divorced from any PSTN telephone number and any particular physical geography (such as through the use of ENUM-specific country, area, and/or city codes). See Section II.B.6 above.

n. ENUM policy within a country should be set in close consultation with the public interest and civil society sector, the communications industry, and the Internet industry. See Section II.B.7 above.

## III. Conclusion

ENUM offers a range of potential benefits, and if properly implemented could increase end users' control over their privacy, and their communications services more generally. There are, however, public policy risks posed by ENUM, and ENUM could be administered in a manner that fails to respect privacy. The recommendations in this paper should guide both national ENUM administrators and ENUM service providers in designing and implementing a robust, user-enabling, and privacy-protecting ENUM system.

## IV. Bibliography of Useful Documents and Links About ENUM

### Good Background and Overview Articles about ENUM:

Geoff Huston, "ENUM–Mapping the E.164 Number Space into the DNS," Internet Protocol Journal, June 2002, http://www.cisco.com/warp/public/759/ipj_5-2.pdf

Junseok Hwang and Milton Mueller, “Economics of New Numbering Systems Over Cable Broadband Access Networks: ENUM Service and Infrastructure Development,” August, 2002, http://web.syr.edu/~jshwang/resource/its-enum-v5.pdf

Craig McTaggart, "The ENUM Protocol, Telecommunications Numbering, and Internet Governance," Mar. 2003, http://www.innovationlaw.org/cm/writing/cm-enum-cardozo.pdf

### Important ENUM-related Web Sites:

International Telecommunications Union ENUM Page, http://www.itu.int/osg/spu/enum/index.html

Internet Engineering Task Force ENUM Working Group Charter, http://www.ietf.org/html.charters/enum-charter.html

The ENUM Forum, http://www.enum-forum.org

## Statements by Privacy Advocates Concerning ENUM:

Australian Privacy Foundation, "Submission to the Australian Communications Authority," Nov. 2, 2002, http://www.privacy.org.au/Papers/SubmnACA021102.html

Roger Clarke, "ENUM - A Case Study in Social Irresponsibility," Mar. 2003, http://www.anu.edu.au/people/Roger.Clarke/DV/enumISOC02.html

Electronic Frontiers Australia, "Submission to the Australian Communications Authority," Nov. 18, 2002, http://www.efa.org.au/Publish/efasubm-enum.html

Electronic Privacy Information Center, "EPIC Comments on Privacy Issues in ENUM Forum 11-01-02 Unified Document," Nov. 2002, http://www.epic.org/privacy/enum/enumcomments11.02.html

## Pages with Extensive Links, Articles, and References concerning ENUM:

Washington Internet Project ENUM Page, http://www.cybertelecom.org/dns/enum.htm [most extensive page]

Electronic Privacy Information Center, http://www.epic.org/privacy/enum/

ENUM Forum, http://www.enum-forum.org/links.html

ICANNWatch ENUM Page, http://www.icannwatch.org/search.pl?topic=22

International Telecommunications Union ENUM Page, http://www.itu.int/osg/spu/enum/index.html