tmdenton.com
37 Heney Street
Ottawa, Ontario
Canada K1N 5V6
http://www.tmdenton.com

☎613-789-5397
✉ 613-789-5398
tim@tmdenton.com

Privacy Issues in ENUM

October 21, 2003

A study for Industry Canada

Contract Number 5009207

tmdenton.com

Success Through Understanding Technology

1. Background

The scope of this paper concerns a relatively small but important set of issues of interest to governments and consumers. The larger set of issues, namely how ENUM works, how the industry that makes it possible will be organized, and how it might be introduced in Canada, are beyond the scope of this paper.

ENUM is a protocol[1] that translates telephone numbers into domain names. More precisely, ENUM is a protocol that defines a method to convert an ordinary telephone number into a format that can be used on the Internet to look up Internet addressing information, such as, for example, VoIP or email addresses.

Two further points:

1. the Internet addressing information associated with an ENUM number is stored within the domain name system (DNS), and
2. More than one piece of contact information can be stored in the DNS record that is associated with a particular ENUM number, and this information may encode directions as to how the person wishes to be contacted, by device, by time of day and so forth.

ENUM has several foreseeable consequences:

- The organizations that handle domain names are well suited to handle ENUM-enabled telephone numbers, in addition to the agencies that have always handled telephone numbers.
- Once telephone numbers have become, in effect, domain names, then a "call" can be made to any ENUM-enabled telephone number. Consequently, for there to be seamless interoperation of VoIP devices with the telephone system, the numbering plan of telephony must be supported by the domain name system, and vice versa.
- New or existing organizations may offer telephony-like services, such as Voice over IP (VoIP), without necessarily passing through a switch of the circuit switched telephone network. While ENUM is NOT essential to the existence of VoIP, it surely facilitates it.

ENUM has the potential to constitute a significant change in the telecommunications industry. On the other hand, ENUM may well be a transitional service with little consumer impact. The US Center for Democracy and Technology believes that "the first broad use of ENUM will more likely be to facilitate the transition away from the PSTN and to use the Internet as the primary carrier of voice communications."[2]

In the next year, it is likely that a process will be initiated in the CRTC Interconnection Steering Committee (CISC) involving most every player in telecommunications and the Internet,

[1] http://www.faqs.org/rfcs/rfc2916.html

[2] CDT, Standards technology and Policy Project. *ENUM: Mapping Telephone Numbers onto the Internet, Potential Benefits and Public Policy Risks*, April 2003 at www.cdt.org/standards

that will delve into all matters related to the introduction of ENUM into Canada. It is evident that work on ENUM is well advanced in the United States[3] and that, at the time of writing, Canada is behind the United States in terms of organizing itself to adapt to the possibilities of ENUM. Nevertheless, the work already done in the ENUM Forum is frequently transferable in whole or in part to Canada.

2. What is ENUM?

Addressing ENUM is difficult because the subject is technical, jargon-laden, difficult, and boring. As Craig McTaggart writes, "the ENUM issue marries the relatively boring subject of telephone numbering with the ongoing quagmire over the administration of the Internet domain name system (DNS)." [4] This presentation tries to simplify the subject as much as possible, and relate to features of the domain name world with which we are already familiar. I offer no apologies to those who find the description insufficiently technical.

2.1 ENUM is the DNS

"It is important to note that ENUM is first and foremost the DNS."[5] Since people have become familiar with domain names, it may be helpful to start with what we know about domain names and see how that world would map onto the world of telephone numbers. When, at some future date, a person decides to register their telephone number as ENUM-enabled, basic features of the domain name world are immediately transferable to the management of telephone numbers since, by definition, an ENUM-enabled telephone number *is* a domain name. In short, important features of the telephone numbering system can migrate to a new technological basis by means of the choice of people to subscribe to ENUM-type services. As telephone numbers become ENUM-enabled, they transmute into domain names. The rules, features, and characteristics of the domain name world would apply, with such exceptions as governments and designers of the ENUM system have provided or shall provide for.

A person seeking to contact another who uses an ENUM-enabled telephone number generates an inquiry, which goes through a series of computers, called nameservers, and which arrives at the customer's information. Along the way to that destination, the inquiry has had to be guided to the nameserver by other computers, which maintain records of where in the world resides the computer holding the required information.

The ENUM system must maintain enough information about the ENUM subscriber to enable the higher-level computers to locate the relevant nameserver, and, when the inquiry finally reaches the nameserver, it opens the record of preferences of the ENUM customer. (No

[3] See, for instance, "ENUM specifications for US Implementation of ENUM" at www.enumf.org
[4] "The ENUM protocol, Telecommunications Numbering, and Internet Governance", by Craig McTaggart, prepared for a conference at Cardozo School of Law, Yeshiva University, New York, NY 17 March 2003.
[5] Richard Shockey, Privacy and Security Issues in ENUM, draft-shockey-enum-privacy-security-00.txt, IETF ENUM Working Group, October 2002. A later version is found at <http://www.cdt.org/standards/draft-ietf-enum-privacy-security-01.pdf>

such record is available unless the customer explicitly chooses to be ENUM-enabled.) Supposing they were written in plain English, the instructions might look like the following.

> Customer: John Fathead
> Try 1: telephone number 1-nnx-xxxx between 9:00 and 18:00 hrs., and , if no,
> Try 2: telephone number 1-nnx-xxxx, between 18:00 hrs and 23:30 hrs, and, if no
> Try 3: Blackberry XXXX XXXX, if no
> Try 4: john.fathead@collossus.com

This record of preferences as to how the person will be reached might specify, for instance, at what time of day to use which communications medium. The customer could change his preferences frequently. (This scenario assumes one of the possible outcomes of ENUM's introduction, and is for the purpose of illustration only.)

This record was called the "Naming Authority Pointer" record by the authors of ENUM, or NAPTR record. In case this is not sufficiently jargon-laden, the IETF[6] ENUM committee calls these records "Resource records" or NAPTR RRs.

Privacy issues arise from the nature of, and publicity associated with, the personal information that must be revealed in order for the ENUM system to work. We shall address these privacy issues further when the basic outlines of the technical system have been made clear, to the extent that is possible.

When the ENUM inquiry has located the subscriber's record, the system then follows the instructions contained in the NAPTR record to open a channel of communication to the subscriber. The IETF would describe the process as contacting a "resource" associated with that telephone number. The "resource" is a SIP (session initiation protocol) URL (Uniform Resource Locator). The Session Initiation Protocol is a powerful net-based protocol designed to allow all manner of video and audio communications among multiple parties.[7]

Imagine a telephone number that was also a hyperlink. Thus my number 1-613-789- 5397 becomes a domain name, linking to the domain name system (DNS), and thereby allowing a number punched into a keypad to access resources and services on the Internet. The DNS is a system of record keeping. It allows us to route traffic to a domain name, and keeps records of who owns which domain name. The ENUM world would work in an identical fashion, by keeping specialized records of information about subscribers at various levels of the hierarchy. Likewise, the organizations that would handle the look-up process would resemble that which prevails in the existing domain name business.

---

[6] The IETF, Internet Engineering Task Force, is the self-organizing forum of experts that devise Internet standards. See www.ietf.org

[7] http://www.cs.columbia.edu/sip/ The statement was made above that ENUM enables contact to be made among people using (ENUM-enabled) telephone numbers without at the same time relying on telephone switching. SIP is the protocol that would facilitate this.

The Domain Name System involves records that attribute ownership and responsibility to people who choose to record their numbers in ENUM. The record-keeping systems in ENUM and the DNS have to answer the following questions:

- On what nameserver (a specialized computer) does the record exist for the owner of telephone number 1-nxx-xxxx?
- In the case of ENUM, what services do they want from a service provider, in what order of preference?

"Services" in the sense used here would refer to how people choose to be contacted, through which media, and the order in which various media should be tried, such as, for instance, first cell telephone, then landline, then Blackberry, then email. The record of this set of preferences is contained within the Naming Authority Pointer (NAPTR) record.

It is a feature of an ENUM system that different information about a subscriber would be kept by different players. The organization of the domain name system provides a handy model.

2.1 Organization of the DNS

The DNS is organized into registries, such as the managers of dot com and dot ca, and registrars, who deal with the public. Set forth below is an explanation of the industry structure that the ITU and others envisage for ENUM.

Notionally, the implementation of ENUM will employ a DNS-based tiered architecture[8]:

> Tier 0 – this is the authority, based in the International Telecommunications Union (ITU) Telecommunications Standardization Bureau (TSB) that delegates the authority over country codes to a tier 1 registry. Each Tier 0 database entry would list the recognized Tier 1 registry for the country code, and give the address of the name servers that can resolve ENUM domain names falling under that country code.
>
> Tier 1 – corresponds to a Country Code or a portion of an integrated numbering plan that is assigned to an individual country. The Tier 1 registry would provide information about the location of name servers operated by Tier 2 ENUM service providers which contain records pertaining to individual subscribers.
>
> In the case of Canada, the Caribbean, and the United States, which share the country code "1" the situation is more complicated than for a country which does not share its country code with another. In the case of the "1" zone, there will need to be way of separating area codes by country, but the principle is the same.[9]

[8] ITU-T, E.164 Supplement 3 "Operational and Administrative issues associated with national implementations of the ENUM functions", May 2002available from www.itu.int

[9] Scott Bradner writes : Its far from clear how it will finally work but my best guess is that there will be a contractor running the server for "1.e164.arpa"

An ENUM Tier 1 *manager* is the entity responsible for managing the numbering plan in the country (e.g. a government).

The Tier 1 *registry* is the registry for the domain names that map to the telephone numbers[10] in the various area codes assigned to a particular country. The name servers of the registry contain records that point to the authoritative name servers for telephone numbers or blocks of telephone numbers in the country code or portion thereof.

Tier 2 –is the registrar level. Notionally two different functions are accommodated at this level. One function is to hold the record of the preferences[11] of the ENUM subscriber for the types of services to which he subscribes. This function is provided by the *Name Service Provider.*

The second function is to be a registrar for the ENUM registrant, who is the ultimate consumer. The *registrar* could be any organization (telephone company, registrar of domain names, cable company) accredited to the Tier 1 registry. The organization of the registrar level is left to the decision of the country involved.

The *Name Server Provider* may be the same or different from the *registrar*.

1. Thus, the degree of competition in the market at the registrar level is a matter for the country in question to decide.
2. The *registrar* may be the same as or different from Tier 2 *Name Service Providers*.

The Registrant in this situation is the person who elects to register their telephone number in ENUM.

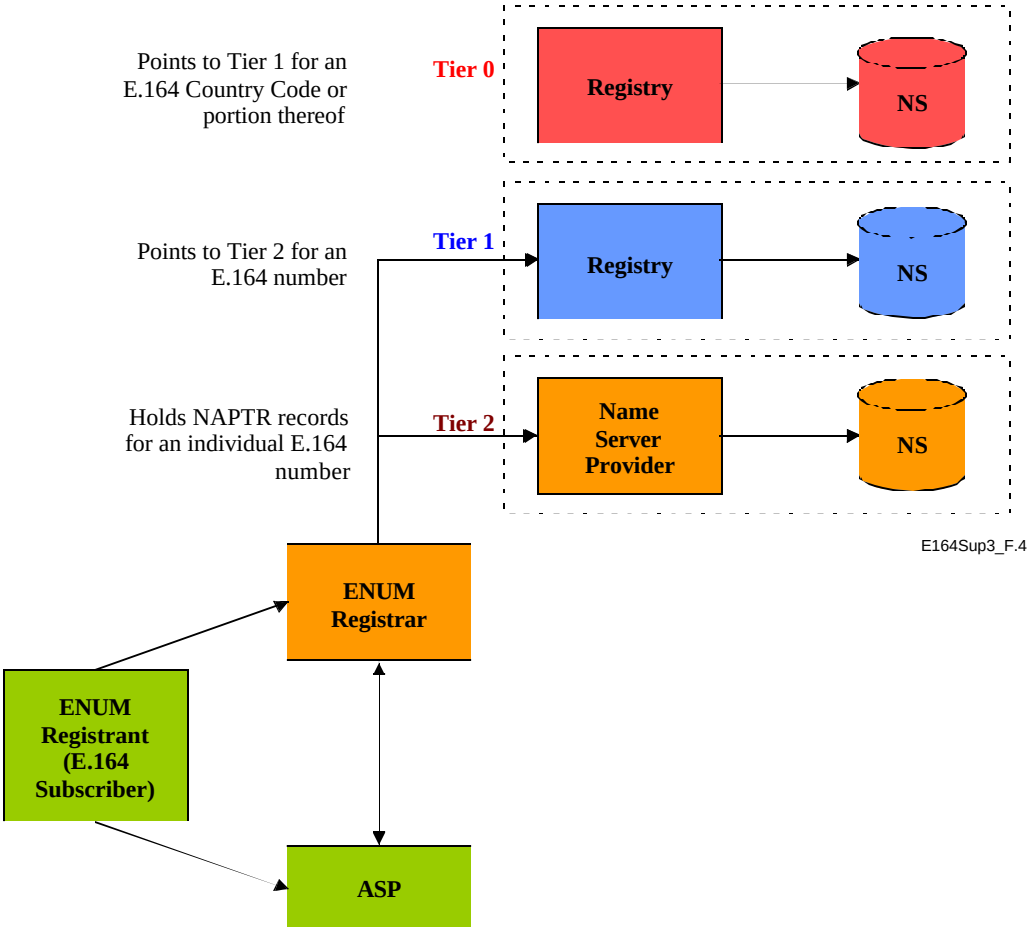
Figure 1. A Schematic Representation of ENUM Tiers

---

that points to a 2nd tier set of servers that are separated by area code. The other option is for RIPE to operate 1.e164.arpa as part of their operation of e164.arpa with pointers to area code servers." October 8, 2003 via email to the author.

[10] The correct term for a telephone number in this context is "the E.164 number", referring to the protocol whereby telephone numbers are ordered in the jargon of the ITU. The author has tried to avoid the term in this report on the ground that it adds nothing to one's comprehension of the privacy issues.

[11] These are called Naming Authority Pointer (NAPTR) records, in the ceaseless profusion of jargon.



2.2 The Nature of Records Kept in the ENUM Databases

Two different kinds of records must be kept in databases for the ENUM system to work:

1. The actual data which is entered into the global ENUM DN system, called the NAPTR (naming authority pointer) records, that can be accessed by any IP end point anywhere in the world, without restriction, and
2. the data that will be required to maintain appropriate authentication, valid registration, administrative and technical contact for DNS servers.

The two different sorts of records constitute the basis of international and national matters in ENUM. One is tied to the operations of the Domain Name System and conditioned by new signaling protocols. The other is fully within the power of country to regulate through contracts, statute or common law.

2.3 National versus International Matters

> "The agreements between the Internet Architecture Board and the ITU over the management of the E.164 global numbering plan clearly articulates that the administration, management, and control of the zones and administrative portions of the E.164 plan are nation-state issues governed by appropriate national laws and regulations, many of which have yet to be determined."[12]

Consequently, it is within the purview of the federal government, among others, to be aware of and concerned with the way in which information will be stored, gathered and deleted in a domestic ENUM system.

Indeed, only matters concerning Tier 0 are international. All matters concerning Tier 1 or lower are within national jurisdictions.

Yet because of the way the Domain Name System works, certain technical aspects of ENUM – those that rely on the DNS – are not really well addressed on a national basis, and for this reason may better be addressed through ICANN, by official representations to the US Department of Commerce, to which ICANN is contracted, or by the activity of Canadians or other interested people in the workings of the IETF.

3. Privacy Issues

3.1 Nature of issues described

Concerns about privacy have been prominent in every discussion of ENUM, and for good reasons. ENUM employs an open and public database of contact information. The ENUM database can also include certain rules for contacting a person, such as devices to be used by a caller according to the time of day.

The Electronic Privacy and Information Center (EPIC) states the problems as follows:

> "ENUM may also become a tool of marketers, spammers, and individuals who wish to harass others. The ENUM database is public and can be searched by anyone. It is likely that marketers, spammers, and malicious

[12] Shockey, supra, note 4

> actors will mine the database for personal contact information. Since there are no statutory protections in place regulating the use of ENUM contact information, marketers and spammers may use the contact information for junk mail, unsolicited commercial e-mail, and other forms of commercial solicitations. The system could facilitate an unprecedented amount of spam because programs could be designed to send solicitations to all of the registrant's communications devices."[13]

Recall that the essence of ENUM is the return of the Naming Authority Pointer (NAPTR) records associated with a registrant's telephone number in response to a DNS query that can be initiated by any party based on a telephone number.

While a registrant determines the exact information to be placed in the NAPTR records, he is obliged to supply enough information to make the look-up work. Each NAPTR contains information that is processed to derive an Internet address, called a Uniform Resource Identifier, and information that determines the sequence in which NAPTR records and the derived Uniform Resource Indicators (URIs) should be processed and employed to reach the person wanted. 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.

The question to be answered is how much personally identifying information is *necessarily* exposed in the ENUM system, and how much of this problem can be eliminated by technical means, and how much can be alleviated by law and policy.

In the worst case scenario, ENUM would generate issues as serious as that which arise in the case of the DNS Whois look-up system. (In fact, it does not, for reasons explained below). Given that the Whois is suspected of being a ready source of e-mail addresses for spammers, there is cause for concern, but our view should be balanced by other considerations. One factor balancing the risk of damage is how governments and industry propose to implement ENUM. Another factor is whatever technical solutions that can be brought to bear. Both sorts of remedy will greatly affect the level of risk that personal data will be abused. Measures to abate the risk of abuse are discussed further below.

3.2 Two models for how ENUM might work

ENUM functions, at a minimum, as a benign number translation database that exposes the minimal subset of data necessary to establish a connection between two endpoints. This is the

[13] http://www.epic.org/privacy/enum/

model on which the DNS works now, by translating http://www.website.ca into a set of IP numbers necessary for a client to find a server running HTTP (hyper text transfer protocol).

This is not the only view that can be taken of how ENUM will work. There is a critical choice about how ENUM will be implemented, that directly affects the privacy concerns associated with it. One is called the *calling party control* model, and the other is named the *called party control* model. The choice has not yet been made in the United States or elsewhere which model may prevail, or whether both models may be available.

Briefly, in the *calling party controlled* model, the amount of data entered into an ENUM record is maximized. All available forms of contact information are entered into the Domain Name System record, thereby permitting the person initiating the contact to choose which of the forms of contact to use.

The *called party controlled* model imposes constraints on the calling party's access to data about the contacted 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 called party. The screening function can be implemented by having a third party operate a proxy server on behalf of the called party, or the called party might operate the server on its own premises.

As Richard Shockey writes[14], speaking of the capacities of SIP (Session Initiation Protocol) to manage the privacy issues:

> "The called party's proxy can also be used to enforce policy about sessions including how, when and from whom to establish sessions. The presumption of this model is that only the minimum information about an endpoint is necessary to expose in the global DNS, since proxies perform all other forms of session negotiation and policy enforcement….
>
> "Because SIP can negotiate the session creation between end points, it is not necessary to expose in the global DNS specific personal identification elements, such as a personal name, to establish a successful end-to-end SIP connection.
>
> "Information, such as a personal name, is exposed only because an end-user chooses to do so by configuration of their entries into the DNS."

Not good enough! respond some critics. Roger Clarke[15] of Australia is a particularly vociferous critic of ENUM, and while it is difficult to ignore his arguments, it is also necessary to assess whether in fact they have been answered or will be answered in the implementation of ENUM. He states that:

[14] *Privacy and Security Considerations in ENUM*, www.cdt.org/standards/draft-ietf-enum-privacy-security-01.pdf
[15] www.anu.edu.au/people/RogerClarke/DV/enumISOC02.html

- ENUM creates a unique individual identifier, which facilitates the location and tracking of subscribers by marketers, spammers and governments.
- Privacy protection features are seriously inadequate, and the mooted "Service resolution service" to support pseudonymity, is as yet undefined.

As is typical of many Internet engineering discussions, the thing in question is being invented on the fly. SIP is an approved protocol; it functions. It did not exist even a few years ago. By contrast, the idea of a "service resolution service" is still a discussion paper within the IETF.

Shockey responds to concerns for privacy with the following:

> "Current discussion in the IETF ENUM Working Group have explored the concept of indirect resolution to all forms of communications, not just SIP, through the use of presence servers or a concept called a "service resolution service". [PETERSON 2] Once again the called party who is registering their phone number in the global ENUM system would then have control of how he or she could be contacted by any method, on any device, by means of configuring in that presence or SRS service only that data that they choose to expose to persons wishing to contact them. The calling party in this scenario would first executing a query to DNS to find the presence server or SRS and based on locally controlled policy the server would return the options available.
>
> "This represents a more robust and expansive concept of presence where a presence server or SRS would not automatically reveal or display the physical or network presence of an individual or the services under the called parties control, but becomes a point of control for how, why when and where presence and a form of communication session might be established.

In other words, in order to obviate certain concerns about how ENUM would work, members of the IETF are considering ways in which privacy features can be built into the scheme, by the perfection of additional software and the establishment of a service model that allows the system to work with anonymity built in. This implies that privacy features are not now built into the scheme of ENUM, in such a way as to answer some expressed concerns about that degree of exposure of personal information which is a necessary consequence of how the DNS works.

The technical aspects of the DNS are largely under the jurisdiction of the IETF, while the management of the root computers, the introduction of domain names and the Whois look-up system is managed under aegis of ICANN, which in turn is answerable to the US Department of Commerce.

We shall briefly allude to Canada's range of points of intervention in ENUM when the whole scheme has been analyzed.

As regards the called party controlled model, or the calling party controlled model, opinion differs. Proponents of ENUM like Richard Shockey state that there is no reason to prohibit the calling party controlled model.

> "No implementation of ENUM should preclude or inhibit the use of either the Called Party Control or the Calling Party Control models."[16]

The Center for Democracy and Technology[17] strongly disagrees:

> "It is critical for any national implementation of ENUM permit the "Called Party Control" model…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 the called party.…
>
> 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."

Perhaps because he is thinking of larger considerations, Richard Shockey appears to change his mind in the course of his paper on privacy concerns in ENUM. He contrasts the features of SIP to that of the PSTN, noting that

> "SIP, as an application technology at the edges of the Internet, reverses the PSTN control model. SIP endpoints and proxies are assumed to be "intelligent" and configurable by network administrators….
>
> "The Called Party Control model of ENUM, therefore, relies on and will promote the broad deployment of applications such as SIP that give consumers direct control over their communications options, and more generally allow the user to control who accesses personal information about the user."

Because the Called Party Control model empowers the consumer at the expense of the command and control model of the PSTN, and because that model requires SIP, Shockey appears to come around to favouring it.[18]

3.3 Is a Whois Look-up System Required by ENUM?

Its proponents argue that ENUM has no need for a centralized registry of registrants. The Whois system was originally designed to trace responsibility for every domain name to an

[16] Shockey, op. cit. p 9
[17] http://www.cdt.org/standards/enum/ Enum: Mapping Telephone Numbers Onto The Internet Potential Benefits with Public Policy Risks. April 2003 pp 17-18
[18] Shockey, op. cit. p 10

administrative and a technical contact. It has since been used for the purposes of enforcement of intellectual property rights, and for police work. IP and police interests argue for a completely accurate, and globally available, record of who is responsible for each domain name. That debate is ongoing within ICANN and within the technical community of the IETF, in the form of the CRISP working group.[19]

The logic of not needing a Whois consists of the following: if anyone, such as an intellectual property rights holder needs to contact the owner of one service that is referred to in an ENUM record, they use the URI or URL of the service referred to locate the relevant party. The ENUM cannot be the subject of appropriation, as a telephone number nowhere constitutes the holder's intellectual property. Nor are ENUM numbers used to host content on the Internet, so that no liability for "content" attaches to an ENUM number.

On the other hand, there is a need for a technical contact for each ENUM registration. The operators of the servers that make the system work need to be reachable by other operators. However this has nothing to do with privacy concerns; the technical contacts are in the business and have a well understood relationship to other system operators.

3.4 Privacy of registrant's information in registrar and registry records

The previous discussion dealt with issues arising from ENUM's reliance on the operation of the DNS. A second level of privacy concerns arise from issues within national jurisdiction.

3.4.1 Opt-in

Shockey writes:

> With both the Called Party Control model of ENUM, and especially with the Calling Party Control model, some degree of personal contact information is exposed in the global DNS. It is important that information regarding end telephone users NOT be imported on a blanket or wholesale basis into the ENUM/DNS system. Users should have a choice of whether to have any information about them listed in the publicly-available DNS. Such an approach will, for example, reasonably preserve the ability of end users to maintain an "unlisted" telephone number, even using VoIP technology. Assuming users are given a choice about enrolling in the ENUM system, a user could forego the benefits of ENUM in favor of directly providing (for example) a SIP address of record to trusted family members and associates.

[19] www.ietf.org/html.charters/crisp-charter.html

No privacy advocate or anyone else disagrees on this. Registration of one's telephone number in ENUM should be entirely voluntary. However, social forces may eventually compel the use of ENUM. It was for this reason that the CDT advocated the "called party control" model of ENUM. In that model, no personally identifiable information is revealed in the DNS. Instead, the only information that is publicly viewable is the Internet address of the Called Party's proxy or SIP server.

The CDT points out that

> "an opt-in approach 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."[20]

If ENUM becomes the essential tool for using VoIP, and VoIP becomes the standard form of telephony, then in practice ENUM ceases to be an option for most people. Here then a privacy concern may become a decisive influence over whether a *called party control* or *calling party control* is selected.

3.4.2 Control Over Data In the ENUM Record

Because some degree of personal contact information is exposed in the global DNS, it is important that the ENUM registrants be provided effective and efficient control over that information. It is also important that ENUM registrants fully understand the privacy implications of placing information in the global DNS.

However, it can be questioned whether people are really aware yet that placing an email or SIP address in the DNS opens one up to spam. More to the point, the degree of informed consent can be questioned when the technology is new and the appreciation of its effects is speculative.

The corollary of effective user control of ENUM records is that only authorized users should be able to control the content of ENUM records.

Fair Information Practices

As guiding principles, consumer privacy protection in many parts of the world is based on "fair information practices," which were authoritatively detailed by the Organization for Economic Co-operation and Development. The principles should be considered in any implementation of ENUM. Fair information practices include the following principles:

[20] CDT, op. cit. at p.18

- Notice and Consent - before the collection of data, the data subject should be provided: notice of what information is being collected and for what purpose and an opportunity to choose whether to accept the data collection and use. In Europe, data collection cannot proceed unless data subject has unambiguously given his consent (with exceptions).
- Collection Limitation - data should be collected for specified, explicit and legitimate purposes. The data collected should be adequate, relevant and not excessive in relation to the purposes for which they are collected.
- Use/Disclosure Limitation - data should be used only for the purpose for which it was collected and should not be used or disclosed in any way incompatible with those purposes.
- Retention Limitation - data should be kept in a form that permits identification of the data subject no longer than is necessary for the purposes for which the data were collected.
- Accuracy - the party collecting and storing data is obligated to ensure its accuracy and, where necessary, keep it up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete are corrected or deleted.
- Access - a data subject should have access to data about himself, in order to verify its accuracy and to determine how it is being used.
- Security - those holding data about others must take steps to protect its confidentiality.

Privacy advocates are suspicious of the adequacy of several of the proposals for privacy protection that have been put forward in the ENUM Forum[21], for example. In some instances, the ENUM Forum's recommendations are more sanguine and significantly less privacy conscious than, for example, Richard Shockey, a major proponent of ENUM[22].

> "Since disclosure of NAPTR contents is an essential element of ENUM capability, Registrants should be cautioned that, if they have special privacy concerns, e.g., an unlisted phone number, they should work with their applications service providers so as to use URIs that could not be examined to determine identity"[23]

The *called party control* model tends to answer concerns about privacy more directly and effectively through the use of proxy servers, which make it impossible to use the publicly available information in the DNS to access an ENUM registrant directly. Fair information practices may be sufficient for the registrant-registrar relationship, but technical obviation of the problem is the course recommended for any information that goes to the DNS.

[21] www.enumf.org and see ENUM Forum Working Document: *ENUM Forum Specifications for US Implementation of ENUM*, March 14, 2003, Document 6000_1_0 especially section 9, Privacy Considerations for ENUM

[22] Refer to note 14

[23] see note 21, at page 38

4. Process for Creating ENUM in Canada

At the moment, a process for creating ENUM does not yet operate. It is envisaged that ENUM would probably require a committee of the CRTC's CISC to be chartered. CISC is the CRTC Interconnection Steering Committee.

"The mandate of the CISC is to undertake tasks related to technological, administrative, and operational issues on matters assigned by the Canadian Radio-television and Telecommunications Commission (CRTC) or originated by the public, that fall within the CRTC's jurisdiction."[24]

It is probable that a CISC Working Group on ENUM will get going sometime in early 2004. In that case, the concerns about privacy in the implementation of ENUM can form part of the deliberations, and privacy advocates can work alongside the technicians, engineers, government officials and lawyers to create the Canadian version of ENUM.

The Working Group will issue papers on various aspects of the implementation of ENUM. Generally these working groups are composed of people from different companies, who try to achieve consensus.

The CRTC's authority in the matter is established by section 46 (1) of the *Telecommunications Act*.

> 46.1 The Commission may, if it determines that to do so would facilitate the interoperation of Canadian telecommunications networks,
> (a)administer
> (I) databases or information, administrative or operational systems related to the functioning of telecommunications networks, or
> (ii) numbering resources used in the functioning of telecommunications networks, including the portion of the North American Numbering Plan resources that relates to Canadian telecommunications networks; and
> (b) determine any matter and make any order with respect to the databases, information, administrative or operational systems or numbering resources.
>
> 46.2
> (1) The Commission may, in writing and on specified terms, delegate any of its powers under section 46.1 to any person, including any body created by the Commission for that purpose.
> (2) For the purposes of sections 62 and 63, a decision of a delegate is deemed to be a decision of the Commission.
> (3) For greater certainty, a delegation of powers is a decision of the Commission.
> (4) The Commission may, in writing, revoke a delegation of powers. A revocation is deemed not to be a decision of the Commission.

[24] CISC Admin Guidelines, 2001-03-31, section 2 "mandate". http://www.crtc.gc.ca/eng/cisc.htm and http://www.crtc.gc.ca/cisc/eng/Ciscadmn.htm

That the ENUM issue also concerns the operation of the DNS as well as telephone numbers may or may not be a problem in law, but in fact participants in the DNS such as registrars and registries can make useful contributions to the evolution of a Canadian ENUM capacity.

Contracts between the registry of ENUM-enabled numbers and the registrars may provide the means for solving many problems of privacy.

Nevertheless, fundamental technical design decisions imply and engage policy decisions regarding privacy. This will be particularly true of the relationship of the *called party control* model to the use of SIP and of proxy servers to keep the calling party from knowing too much about the individual ENUM registrant.

5. Conclusion

Privacy concerns in the implementation of ENUM are substantial. The successful take-up of ENUM services by consumers may well depend on a satisfactory resolution of privacy concerns. Therefore, technical design criteria should be sensitive to the legitimate interests of people in controlling what information about them is made publicly available.