Robocall Handling Improvement Program
Technical Proposal

Submitted to the FTC Robocall Challenge by
InCharge Systems, Inc.[1]
January 16, 2013

Abstract

InCharge Systems, Inc. (ICS) proposes a Robocall Handling Improvement Program for the FTC's Robocall Challenge. Since no single solution can block all illegal robocalls to consumers while still allowing permitted legal robocalls to go through, a combination of components can significantly increase consumer protections against illegal robocalls, improve the identification of legal robocalls, assist carriers and law enforcement, and provide incentives for innovation. The proposed approach provides consistent and uniform basic robocall screening to potentially all consumers, using existing technology, new information repositories, and dedicated numbers.

Contents

1. Executive Summary

Currently, robocalls that, at least in part, traverse the PSTN may involve many network elements and a range of scenarios. No single solution can handle all robocalls appropriately because perfect knowledge of each caller, called party, and call routing is unattainable. However, robocall handling can be improved significantly by using a combination of components.

ICS envisions the following as key components of a Robocall Handling Improvement Program:

Robocall Information Repositories:
- Enhanced Do Not Call List
- Dedicated Numbering Range
- Legal Robocaller Registry

Consumer Services for Robocall Handling:
- Uniform Robocall Diversion Option
- Generic Robocall Handling Service

[1] Contact information: Andrew Gallant, VP, Applications Architecture, InCharge Systems, Inc.
Email: abgallant@inchargesys.com.

Taken together, this combination of key components will work to improve robocall handling for both consumers and legal robocallers. Some parts could start being rolled out in about a year, and all components could be in place in about two to three years. In addition, this approach will provide benefits for network and service providers, improve the pursuit of illegal robocallers by law enforcement and regulatory authorities, and stimulate innovation in robocall handling.

Although a strong solution based on digital signatures could be proposed now, the major challenges currently are in the existing PSTN and mobile switching systems. That is where this proposed approach is focused, leaving solutions based on digital signatures for later steps involving IP-based telecommunications.[2]

2. Program Description

The proposed Robocall Handling Improvement Program consists of five key components. This section describes those components. Subsequent sections illustrate how these components improve robocall handling, and then address the criteria for the FTC Robocall Challenge.

2.1. Robocall Information Repositories

Currently, information and resources for dealing with robocalls are fragmentary, incomplete, and possibly proprietary, even if they could be used together. The proposed new Robocall Information Repositories address three major sets of stakeholders: consumers, service providers, and legal robocallers. The information in these registries is also useful for services that provide robocall handling for consumers.

2.1.1. Enhanced Do Not Call List

An Enhanced Do Not Call List would be a registry for consumers to identify their choice of Robocall Handling Service for each of their telephone numbers. This registry would maintain secure individual accounts for each consumer. A consumer could store information about basic opt-in/opt-out preferences, and the list interface could also provide enhanced options for verifying registered numbers, handling calls, and filing robocall complaints.

Inputs to the Enhanced Do Not Call List would come from consumers, who would need to authenticate their numbers when registering them, or from legitimate Robocall Handling Services, who would be authorized by consumers to act on their behalf.

Legitimate robocallers could screen their call lists against numbers in this registry. In addition, they could pre-screen numbers for basic opt-in/opt-out preferences.

[2] Caller ID information is easily spoofed today as voice telephony transitions from TDM and SS7 technology to IP-based networks. Cryptographic techniques like digital signatures can be used to authenticate Caller ID information but cannot readily be deployed to interwork with the current PSTN. These practicable techniques would be highly effective in all-IP infrastructures and particularly valuable for law enforcement and public safety purposes. See the FCC's Report to Congress, "Caller Identification Information in Successor or Replacement Technologies," June 22, 2011, Par. 43, Par. 44, and Note 88, at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-11-1089A1.doc.

Important considerations for the Enhanced Do Not Call List include the following: protecting the privacy and security of consumers and their registered information; ensuring the integrity of information stored in the list; and enabling the provision of information, for legitimate robocall handling service providers, and access to information, for legal robocallers, in an appropriate, efficient, and effective manner.

2.1.2. Dedicated Numbering Range

One of the most common practices for screening incoming calls to consumers is to use some form of a calling number, for example, when Caller ID information is displayed. However, Caller ID is in theory tied to the calling party (or originating gateway) and robocalls would have to be identified by lookups against various lists in order to decide – on a per-call or per-number basis – whether such a call might or might not be legitimate.

A Dedicated Numbering Range for legal robocalling would allow for rapid and clear identification of potentially legal robocalls. Suppose, for example, and for illustrative purposes only, that an NPA-level resource such as 899 were to be used for legal robocallers.[3]

Then, at originating switches and gateways, calls from 899 numbers could be handled separately from calls from other number ranges. Operators then could use their origin-dependent routing functions to handle or deny robocalls from ingress trunks from which those calls are not supposed to originate, e.g., from international inbound gateways. Also, illegal calls using 899 numbers would be in violation of the Truth in Caller ID Act[4] and should become easier to detect and investigate.

Assignment procedures to set aside dedicated sub-ranges within 899 could also be used to identify political, charitable, health care, or other specific types of legal robocalls.

Suppose that regulatory measures were to make the use of a dedicated numbering range mandatory for legitimate robocall originating numbers. Then legitimate robocalls would be simpler to detect because their visibility would increase. Further, illegitimate uses of these numbers would be easier to trace and prosecute.

Other alternatives include non-mandatory use of a dedicated numbering range, perhaps coupled with lower rates or other measures to incentivize their use, coupled with higher rates for registering numbers outside the dedicated range. Even if an identified dedicated numbering range were not mandatory but did come to be used, there would still be advantages and benefits for legal robocallers, consumers, and networks.

The use of dedicated numbering ranges for legitimate and registered robocall originators would have to be communicated to consumers. Authorities such as the FTC could conduct education and advertising campaigns to inform consumers about the chosen well-known NPA code and to prepare consumers to report when their Caller-ID displays show that robocallers are misusing

[3] According to NANPA's website, NPA 899 is an Easily Recognizable Code that is an Expansion Code and is not assignable (see http://www.nationalnanpa.com/area_codes/index.html). It is used here for discussion purposes only.
[4] See for example http://www.fcc.gov/document/rules-and-regulation-implementing-truth-caller-id-act-2009.

these numbers. As a side note, it would be desirable if all detected robocalls that originate from unregistered number ranges or that illegally use ordinary phone numbers could be reported by automatic or easier manual means to investigators.

2.1.3. Legal Robocaller Registry

A Legal Robocaller Registry would provide the ability for legitimate robocallers to register their identities, calling numbers, and types of legal robocalls. This repository would be populated by legal robocallers, and consumers and legitimate robocall handling services would be able to query the registry for information about specific robocallers and calling numbers. The information in the Legal Robocaller Registry could also be used by network operators and service providers, where it could be used as initial input to support white lists.

By registering, robocallers demonstrate their commitment to follow all applicable policies and procedures, and consumers can use the information in the registry to assure themselves of the status of robocallers. In effect, registered robocallers would be agreeing to follow best practices.

Robocallers would also provide contact information such as web links so consumers can find more information about opting in or opting out of robocalls from specific registered robocallers, or for verifying their current opt-in status with them. This would make it easier for a consumer to opt in to receive desired robocalls from a company where there is a pre-existing relationship.

The registry's policies and procedures should take into account the validation of registrants to prevent illegal robocallers from registering, and they should anticipate how to handle problems that legitimate robocallers may encounter when registering their numbers.

2.2. Consumer Services for Robocall Handling

Consumer services for robocall handling are intended to help consumers deal with incoming robocalls. First, consumers would have the option to enable robocall diversion, and this capability would be available in the terminating switch serving the customer. Second, consumers would have the option to select their choices of specific robocall handling services to act on their behalf. A generic robocall handling service could either be located within the network the consumer subscribes to, or it could be located outside that network, and it would satisfy the minimum requirements for robocall handling for consumers.

Specific robocall handling services and consumer solutions already exist, and this is an active area of growth and innovation. However, uniform call diversion and generic call handling requirements are needed to make these services and solutions available to potentially all phones and called parties, and to ensure that they would operate in a more uniform and consistent way.

2.2.1. Uniform Robocall Diversion Option

A Uniform Robocall Diversion Option is a service typically located at the consumer's serving or terminating switch. This is an opt-in service that forwards terminating calls to the consumer's

choice of robocall handling service. If the consumer's carrier also provides the Generic Robocall Handling Service, the consumer can use it as a default.[5]

This diversion service can be implemented in a straightforward manner by either consumer or network operator activated call forwarding. In particular, the forwarding destination could be, as a baseline, a trunk to a generic robocall handling service that would satisfy minimum requirements for handling robocalls. Then, calls received back from the generic robocall handling trunk (legitimate calls) would be required to be delivered straight to the subscriber.

Optionally, this uniform call diversion service can include white lists for calls that would be completed directly and not forwarded to the generic robocall handling service. Since this service would typically be provided by the consumer's subscribed carrier or service provider, the terminating switch could couple it with other services available to served customers.

It is important to note that this call diversion capability is available to all consumers and all kinds of phones. The uniform robocall diversion option is based on call forwarding, typically implemented in the terminating switch, and consumers can use it to divert robocalls to their choice of any service that meets the minimum requirements of generic robocall handling. It is clear that this enables choices for consumers, and it provides opportunities for growth and innovation in providing these choices to consumers.

2.2.2. Generic Robocall Handling Service

A Generic Robocall Handling Service is a basic set of functions provided to consumers on a platform that lets consumers set up options for handling incoming robocalls, including block all, block none, selective signal, or send to voicemail, and possibly has options for asking callers to respond to a voice prompt or to solve puzzles before a call is put through. Essentially, the robocall handling service acts on the consumer's behalf to screen and handle incoming calls.

The Generic Robocall Handling Service is located at or as an adjunct to the terminating switch, and it tests every delivered call against two sets of data: information derived from sources that include the repositories mentioned above and the call handling options chosen by the consumer. Depending on the results of tests, the call may be handled in a number of different ways:

- The incoming call can be rejected.
- The originator can be queried or given a simple puzzle to solve.
- The call can be delivered, perhaps with an announcement, to the consumer.

A call can be delivered straight to the customer by routing the call back to the terminating subscriber, e.g., by issuing a modified SS7 Initial Address Message (IAM), or the unmodified IAM could be routed back through the robocall trunk to avoid unneeded diversion and repeated robocall handling. Note that this approach only affects SS7 messaging, and it has no effect on the speech channel (unless a temporary channel is used to notify the originator about how the generic robocall handling service treated the call).

[5] A network operator or service provider could offer its own Generic Robocall Handling Service or could make arrangements with another entity to provide that service on behalf of the consumer's carrier.

The overall objective is to provide better blocking of illegitimate robocalls while ensuring that legal robocalls can go through. While consumers will potentially have many choices for handling robocalls, the creation of a generic robocall handling service ensures consumers that basic robocall handling will be widely available. This, combined with the availability of uniform robocall diversion, will help establish minimum levels of services that consumers can rely on.

2.3. Additional Considerations

There are three areas of additional considerations for the proposed Robocall Handling Improvement Program. First, there are several technical points that are related to the five key proposed components. Second, there are some considerations regarding industry roles. Finally, there are some thoughts about program management.

2.3.1. Additional Technical Considerations

In an environment where robocall handling services can evolve, operators have a number of technical measures they can choose to pursue. Besides testing robocalls at terminating switches, operators may also install robocall handling services for their own operations at their inbound trunks to unload malicious calls by simple routing paradigms. These services can include various tests that can be accomplished by routing or evaluation of originating calls. The following are some examples of tests and rejections that can be implemented with existing functionality of SS7 switches:

- Reject originating robocall number ranges from international inbound trunks.
- Reject originating robocall number ranges from national inbound trunks not coming from registered robocall originators.
- Reject all inbound calls from unassigned national numbers, i.e., spoofed number checking, which assumes there is access to an assigned number list.

Operators can also implement statistical measures such as unusual IAM volumes coming from certain origins, or other tests against the robocall information repositories mentioned above. However, these checks may require special gear and as such, would likely be applied to very exposed switches first. Additionally, these measures could provide further filtering by using existing mechanisms such as Killer Trunk Supervision or Noisy Port Supervision, features that are currently provided by existing PSTN switchgear.

2.3.2. Industry Roles

The active and coordinated participation of industry stakeholders is an essential part of improving robocall handling across the board. In particular, the commitment of all stakeholders to quickly develop and implement standards, policies, and procedures is critical. Specific areas where cooperative work could be leveraged include:

- Developing criteria and procedures for assigning numbers from dedicated ranges to legitimate robocallers,
- Establishing minimum requirements for generic robocall handling services,
- Designing appropriate requirements for information contents and flows for the robocaller registry,

- Compiling best practices for implementing uniform robocall diversion services, and
- Supporting the creation of, and migration to, the Enhanced Do Not Call List to increase its utility to consumers and the industry.

In addition, industry guidance would be extremely useful with helping all parties arrive at policy positions that could facilitate the roll-out of the robocall handling improvement program. Some of the considerations involved in this program include:

- How to incentivize legitimate robocallers to enroll in the robocaller registry and to request assignments from the dedicated numbering range,
- How to educate consumers about the new services available to them,
- How to encourage operators and service providers to keep consumer costs for these services as low as practicable,
- How to encourage consumers and operators to increase their reporting of illegal robocalls, and
- How to target industry efforts to support the timely and efficient specification, development, and roll-out of the key components of the proposed improvement program.

2.3.3. Program Management

The proposed approach absolutely requires clarity at the program management level. With a multitude of stakeholders, five key components, and many moving parts, the proposed robocall handling improvement program must be managed to foster and maintain progress. Accordingly, the program management approach would need to focus on the following:

- Establish a top level task force (or equivalent) and component-level working groups;
- Ensure that the scope, role, and objectives of each working group are clear;
- Focus on developing basic sets of common understandings, functions, and interworking;
- Identify and resolve issues as soon as possible; and
- Foster clear communications, good engineering, appropriate stakeholder participation, and the commitment to achieving good results.

2.3.4. Other Measures

The proposed approach to improve robocall handling is a program involving five key components. However, two additional measures are strongly recommended for strengthening the impact of this program in the ongoing actions against illegal robocalls:

- Legal authorities are strongly encouraged to prosecute illegal robocallers rapidly and aggressively, and to impose significant penalties against violators.
- Carriers and service providers should make it easier and less costly (if not free) for consumers to report robocalls.

3. Scenarios and Use Cases

This section discusses some scenarios and use cases for the key components of the proposed Robocall Handling Improvement Program.

3.1. Handling Robocalls to Consumers

A simplified call flow for legal robocalls is shown in Figure 1 below.

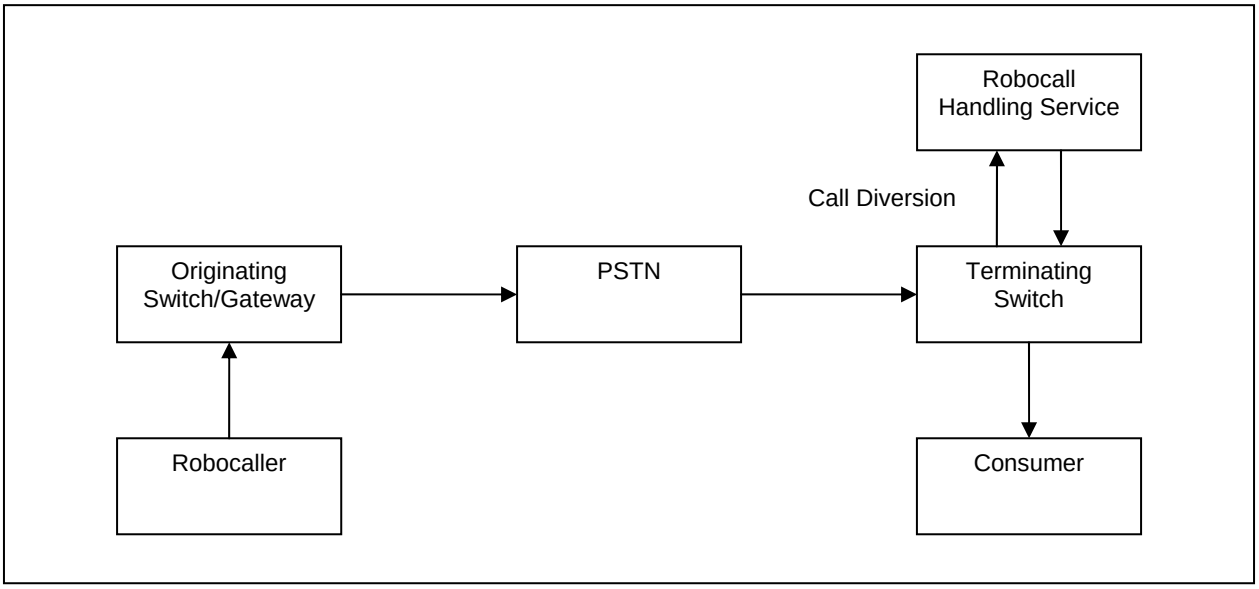

Figure 1. Simplified Call Flow for Legal Robocalls

In this scenario, a legal robocaller initiates a PSTN call via an originating switch, or equivalently, a VoIP call via an originating gateway. When the terminating switch, which serves the consumer, processes the call, it checks to see if Uniform Robocall Diversion is configured. If so, the call is diverted to the consumer's chosen Robocall Handling Service. There, the call is evaluated against the options chosen by the consumer. In this example, the consumer has opted to receive this legal robocall, so the call is passed back to the terminating switch for completion.

As another example (not shown in Figure 1), the following steps could occur:

- The robocall handling service is configured to query the consumer about the call,
- The service calls the consumer, announces the Caller ID information and follows with:
  - "To accept this call, press or say '1.'"
  - "To block this call, press or say '2.'"
  - "To send this call to voicemail, press or say '3.'"

If the robocall handling service determines that this is an illegal robocall, the service or the consumer could directly report the robocall, depending on how the options for handling this are configured.

Additionally, the service could determine special handling or signaling if the type of legal robocall is determined. For example, the consumer might choose to accept all public service robocalls, block all telemarketing robocalls, and send all political robocalls to voicemail.

The minimum requirements for the features that a robocall handling service can provide to a consumer will be determined by the functions specified for the Generic Robocall Handling

Service. These requirements also include ensuring that relevant consumer entries are present in the Enhanced Do Not Call List and that interworking via Uniform Call Diversion with the consumer's carrier is supported.

3.2. Configuring Robocall Handling for Consumers

Consumers would have a range of choices for configuring robocall handling. The most basic method is for the consumer to enter options via the Enhanced Do Not Call List.

However, many more choices are envisioned through the use of the uniform robocall diversion service, provided by the carrier that the consumer subscribes to, and by the robocall handling service chosen by the consumer.

For example, a robocall handling service could be set up to offer "one stop shopping" for consumers. A consumer would set up an account, identify a phone number, and select options for robocall handling. The robocall handling service would verify the consumer's identity and payment method, authenticate the phone number (for example, using callback methods), communicate with the consumer's subscribed carrier to set up robocall diversion, and populate the Enhanced Do Not Call List on behalf of the consumer.

4. Criteria Discussion

The criteria for the FTC Robocall Handling Challenge emphasize the most practical aspects of designing, deploying, and operating a robocall handling solution. The proposed solution, based on the aforementioned five key components, all which reflect a practical approach, will work, will be easy to use, and can be rolled out. It is not a perfect solution – it is highly unlikely that a perfect yet deployable solution exists – but it is a timely, cost effective, and reasonable attempt to deal with a range of robocall issues in a practical manner.

4.1. "Does it work? (weighted at 50%)"

In brief, each of the five key components work, and each provides benefits. Taken together, the components will vastly improve how robocalls impact customers. The real question is how well the proposed solution will work, i.e., how effective it would be considering that the primary objective is: "An ideal solution blocks all illegal robocalls and no calls that are legally permitted."[6] The proposed approach is based on, and extends, existing methods so that the combination provides significant benefits to consumers as well as other stakeholders.

4.1.1. Illegal and Legal Robocalls

Improved robocall handling services will make it easier for consumers to protect themselves from illegal and undesired robocalls. The information repositories and dedicated numbering will make it easier for network operators and service providers to identify and investigate illegal robocalls. The Generic Robocall Handling Service offers a range of options to consumers and the Uniform Call Diversion Service makes these options available to every consumer.

[6] See the Criteria details at http://robocall.challenge.gov/details/criteria.

While this approach does not specifically increase the identification of illegal robocalls at their origin, it does significantly increase how available information, for example, numbers used for illegal robocalling, can be used. This would lead to more consumers being able to block more calls from these numbers. In addition, robocall handling services could report more incidents of illegal robocalls, which should help provide more data for investigation of illegal activities.

A special benefit of the proposed approach is the clearer identification of legal robocalls and the significant potential for improving the handling of legal robocalls from the consumer point of view. As a corollary, these are benefits for legitimate robocallers and their providers as well, all accomplished by increased utilization of existing assets and infrastructure.

Finally, the use of dedicated numbering for robocalls provides incentives for legal robocallers as well as increased capabilities for network operators and service providers. For example, it should be very straightforward to not only detect illegal use of unregistered numbers in the robocall numbering space but to investigate calls from spoofed numbers in that space as well.

By implementing just the dedicated numbering range and the Enhanced Do Not Call List, the proposed approach is expected to correctly detect and handle a greatly increased number of robocalls. Furthermore, when coupled with a robocaller registry, this approach is fully expected to successfully handle the vast majority of robocalls. Finally, as these measures are deployed, and as they are used by more and more customers, it is expected that the volume of illegal or undesired robocalls will significantly decrease.

4.1.2. Consumer Phones

The biggest benefit to the proposed approach is that it makes robocall handling available to every consumer phone by leveraging existing infrastructure. That is because terminating switches have call forwarding capabilities that can be used to set up Uniform Call Diversion whether the consumer is using a traditional land line, a VoIP land line, or a mobile phone.

Even a basic phone could use the Generic Robocall Handling Service – smart phones or special applications would not be required. In fact, Uniform Call Diversion, coupled with the consumer's ability to choose a robocall handling service, can be expected to broaden the market for a wide range of innovative services and apps.

4.1.3. Rationale

It is extremely unlikely that a perfect solution exists. If it did, the solution would have to be able to correctly identify which calls are robocalls and then determine which of those calls are illegal or legal. To respect consumer choices requires information about called parties and their preferences. To sort out relevant information about calling parties requires the equivalent of identifying callers and authenticating their rights to make such calls.

However, requiring every caller to be securely identified is challenging at best, and it raises concerns about privacy. A number of related issues are discussed in a current Internet Draft.[7]

Therefore, the approach chosen in this proposal is to use a set of key components, all of which are doable, in a manner that combines their benefits to improve robocall handling while at the same time being very mindful of the costs of implementing and operating these measures.

4.1.4. Evolving Threats and Countermeasures

It is difficult to envision how threats to the proposed approach would actually evolve. Each of the five key components is fairly straightforward, and presumably, attacks against registries and call handling services are fairly well known and can be managed appropriately. Known approaches to call diversion and the possibility of a common approach to robocall handling should help as well. The use of a dedicated numbering range for legal robocalls, making it easier for carriers to detect and investigate misuse of their resources, could likely prove to be most beneficial. Finally, the increasing deployment of the proposed approach would itself provide additional protection to consumers and benefits to other stakeholders.

It is possible to imagine threats evolving in several ways. Illegal robocallers could make more use of numbers outside the dedicated number range. As mentioned in the executive summary, methods for dealing with this take more time and expense to implement and are outside of the scope of this initial robocall handling improvement proposal. It is expected that as legal robocall traffic transitions to the dedicated numbering range, robocall activity elsewhere should be easier to detect and investigate by statistical or other malicious call traffic tracing and measurement means implemented in PSTN switches.

Another threat vector is analogous to some trends in spam where targeted attacks are coupled with social engineering. One such attack could exploit a "pirated" address book by making calls to all the numbers in that address book appear to come from the rightful owner's corresponding phone number. While the bad news is such spoofed calls would likely evade detection (until, for example, phone number authentication can be implemented in IP-based networks), the overall volume of these illegal robocalls should decrease as this is likely to be a more expensive attack with a much lower rate of return for the bad actor.

4.2. "Is it easy to use? (weighted at 25%)"

Ease of use for consumers should drastically increase as the proposed key components for this solution are implemented and deployed. The most significant part of this approach is to empower consumers who want to protect themselves from illegal robocalls.

4.2.1. Usability

The proposed approach is itself easy for consumers to understand, and when they configure and use their services (or interact with the Enhanced Do Not Call List), they should benefit from

[7] See "Secure Call Origin Identification" by Alissa Cooper, Hannes Tschofenig, Jon Peterson, Bernard Aboba, November 30, 2012, at http://www.ietf.org/id/draft-cooper-iab-secure-origin-00.txt.

design and implementation goals that include well-designed web pages, simple voice tools, and consideration of other human factors. These consumer activities can also be provided by call centers of operators or providers of the generic robocall handling service, which should also take ease of use into account.

4.2.2. Potential Problems

Consumers may experience problems if they misconfigure their options or if they err in responding to robocall handling service interactions. These mistakes are somewhat analogous to setting up call forwarding to the wrong number, deleting rather than saving a voicemail, or inadvertently hanging up on an important call.

Many problems will be the result of normal human behavior, and human error should be expected. Simple design and development practices coupled with familiar and straightforward configuration decisions should help limit potential errors and consumer confusion.

How a consumer authenticates numbers is also a consideration. Using callbacks to those numbers is a starting point, but alternative authentication means will also have to be provided.

4.2.3. Other Human Factors

Existing methods for providing service to people with disabilities should be incorporated in all user interfaces and voice prompts.

For example, the voice prompts mentioned include “Say or press ‘1’,” which allows someone who can’t use a keypad (whether due to a disability or a limitation of a hands-free mobile call) to make the appropriate response.

4.3. “Can it be rolled out? (weighted at 25%)”

Each of the five key components of the proposed approach is based on, or extends, current technology and methods. This section looks at some of the dependencies, economic implications, and timing related to developing and implementing these components.

4.3.1. Dependencies and Alternatives

There are a number of anticipated dependencies that would affect the deployment of the key components of the proposed approach. Many of these will involve work by suitable industry groups to develop relevant guidelines, requirements, and policies, as well as to make recommendations about how implementation would proceed.

To implement an Enhanced Do Not Call List would involve specifying:

- The information contents and additional functionality,
- How consumers and robocall handling services provide information,
- How robocallers retrieve information, and
- How the existing system and its information could be migrated to the new one.

To set up a Dedicated Numbering Range for robocalling would require involving suitable industry groups to:

- Develop assignment guidelines,
- Select a suitable NPA-level resource,
- Set up a Numbering Administrator, and
- Plan for opening up the use of these numbers.

For a Legal Robocaller Registry, work items would include:

- Developing registration criteria and procedures for legal robocallers,
- Developing guidelines for registry operations,
- Selecting a Registry Operator, and
- Overseeing the development and implementation of the registry.

To facilitate the deployment of Uniform Robocall Diversion, industry groups would need to develop several sets of guidelines, including:

- How call diversion works overall,
- How consumers opt for call diversion,
- How terminating switches identify calls for diversion,
- How calls are diverted to the Generic Robocall Handling Service (and others), and
- How calls that are accepted are put through to the called party.

For the fifth component, Generic Robocall Handling, several different sorts of issues need to be worked on. First is to determine the requirements, which would include:

- Which functions for handling robocalls to consumers are supported,
- How consumers enroll their numbers and configure their robocall options,
- How interworking with switches providing Uniform Robocall Diversion is configured and performed, and
- How the Generic Robocall Handling Service interworks with the Enhanced Do Not Call List and other information repositories.

Next come steps leading to implementation and deployment of Generic Robocall Handling, which could include:

- Architecture issues such as the number and location of entities providing this service;
- Procurement issues such as selection of those entities, funding for development and deployment, and management of the overall implementation process; and
- Operations issues such as the creation of a suitable body to oversee operations, quality assurance, finances, compliance, and other matters.

In addition, the requirements for Generic Robocall Handling will become the core of the basic requirements for any other robocall handling service that could be reached through Uniform Robocall Diversion. If an entity wanted to provide enhanced robocall handling services, it would have to demonstrate compliance with the basic requirements for consumer services, call diversion interworking, and all other minimum requirements. This means that a registry for

these entities would have to be created, and that guidelines and procedures would need to be created.

Finally, there would need to be campaigns to educate consumers about the parts of the Robocall Handling Improvement Program that directly affect them, such as using the Enhanced Do Not Call List, recognizing the new range of dedicated robocall numbers, and dealing with their carriers or various robocall handling services.

4.3.2. Economic Implications

It would be desirable to keep consumer costs low. High costs to consumers would lower their participation, and that would lower the effectiveness of the proposed approach for all stakeholders. Since network operators and service providers, as well as legal robocallers, would also benefit from the proposed approach, it also makes sense to consider not only how these various components are funded, but also to consider how to incentivize various stakeholders to participate.

Funding for the Dedicated Numbering Range could come from applicants, and robocallers who join the Robocaller Registry could be required to pay annual subscription fees. Cost recovery for Uniform Call Diversion would likely be added to consumers' phone bills, either on a per subscriber basis or as a charge to all subscribers. Robocall Handling Services would most likely charge their customers. Balancing cost recovery with cost burdens will be an interesting issue.

Some cost savings may be possible when looking at implementation alternatives. In particular, one participant in the FTC's Robocall Summit described a product that handles robocalls and is beginning to be licensed to other carriers.[8] So, in the development of the Generic Robocall Handling that is part of the proposed approach, it may be possible to arrange for licensing such an existing product and to select appropriate portions of it to use as part of Generic Robocall Handling. Not only could that ensure uniformity by deploying a common implementation, it could well provide significant cost savings compared to the alternative of developing everything.

4.3.3. Timing

Rough estimates for developing, implementing, and deploying the key components of the proposed approach are discussed below.

The Enhanced Do Not Call List is estimated to take 12 to 18 months until operations could begin, although interworking with the Generic Robocall Handling service providers is estimated to take 18 to 24 months.

To set up and begin using a Dedicated Numbering range is estimated to take 9 to 12 months overall. This includes implementing origin-dependent routing rules that reject false robocalls on

[8] The FTC Robocall Summit's session on Call-Blocking included a presentation by Matt Stein of Primus Telecommunications Canada Inc. on the Telemarketing Guard product. Webcast videos, the Summit transcript, and presentations can be found at http://www.ftc.gov/bcp/workshops/robocalls/.

ingress routes from which robocalls are not supposed to originate. The actual deployment of the range itself could take 1 to 3 months using standard PSTN configuration measures.

A Legal Robocaller Registry is estimated to take about 12 to 18 months to begin operating.

Basic functions for Uniform Robocall Diversion could begin in an estimated 9 to 12 months since it uses existing PSTN functions. Although implementing diversion in switches would likely take 1 to 3 months, it is estimated that laying the groundwork for a harmonized approach would take 9 to 12 months, with the objective of allowing interworking on standard trunks without having to modify PSTN software. Also, interworking with the Generic Robocall Handling service providers is estimated to take 18 to 24 months.

Last of the key components is Generic Robocall Handling Service. Basic functions are likely to take no less than 18 to 24 months to be ready for initial operation.

In summary, it is expected that significant efforts in the first year of the proposed program would lay the groundwork for all of the key components. Some of these could be made ready to begin operations in about a year, and Uniform Robocall Diversion and Generic Robocall Handling could come in the second half of the second year.

5. Conclusion

The objective of the proposed approach is to make consistent and uniform basic robocall screening available to potentially all consumers by using existing technology, new information repositories, and dedicated numbers.

The key benefits for consumers come from using Uniform Robocall Diversion (based on call forwarding) to enable access to Generic Robocall Handling (for basic robocall screening). Wide-spread adoption of these and the other proposed measures should significantly mitigate the high volume and impact of illegal robocalls.

Legal robocallers would benefit from the proposed Legal Robocaller Registry and the Enhanced Do Not Call List, and all stakeholders would benefit from the use of a dedicated numbering range for legal robocalls. Networks, service providers, and others will find opportunities for innovation, additional revenues, and improved capabilities for dealing with robocalls.

Finally, a comprehensive and coordinated program to improve robocall handling will increase customer satisfaction in the near and mid term. In the longer term, cryptographic measures such as digitally signed Caller ID information could be implemented in all-IP networks in the future.[9]

ICS thanks the FTC for offering this Robocall Challenge and looks forward to the better future this Challenge will lead to.

---

[9] Such measures could not only improve robocall handling but could be valuable for law enforcement and public safety purposes as well. See Note 2 above.