ROBOBLASTER ILLEGAL ROBOCALLER BLOCKER

1. OVERVIEW AND THE BIG PICTURE

How the RoboBlaster Works and What it all Entails

The RoboBlaster blocks 95% of illegal robocaller calls to the consumer "on the fly". The process to block at least 95% of illegal robocallers for all consumers is performed in four steps:

1. Apply a list-based blocking algorithm to block all known illegal robocallers based upon a number of caller lists. If an incoming call is not a reverse 911 call, the Caller ID is first compared to entries in an Individual White List managed by the consumer, and next to entries in an Individual Black List managed by the consumer, and finally to entries in a Service Provider Black List managed jointly by service providers in the telephone industry. If the Caller ID is found in the white list, Caller ID processing stops and the call is completed. If the Caller ID is found in either black list, the call is blocked. Comparison to the Service Provider Black List also incorporates the caller's service provider information that is available at the network-to-network interface of the recipient's service provider's connection to other networks around the world. If the caller appears in none of these lists, the blocking process continues to the next step to identify unknown illegal robocallers.
2. Apply extensions to the blocking algorithm to block unknown illegal robocallers "on the fly" by analyzing the Caller ID to determine if the caller is misrepresenting itself to the recipient. The extensions of the blocking algorithm analyze the Caller ID for anonymous indications according to the recipient preference, syntax anomalies such as an incomplete phone number, and context "hints" in the name such as "WINNER" or "SEX" or "PILLS". If the Caller ID is erroneous or contains certain keywords, the incoming call is blocked; otherwise, the call is completed.
3. Identify new illegal robocallers by analyzing Individual Black Lists of the entire customer base for identical reports from multiple call recipients and verifying those reports. The call recipient reports suspected illegal robocalls they receive by adding Caller ID information to their Individual Black List with a simple button sequence. The service provider periodically analyzes their customers' individual black lists for common additions by large numbers of customers to identify suspected illegal robocallers to verify. If the verification process determines that a robocaller is illegal, the robocaller information is added to the Service Provider Black List. If the verification process determines that a robocaller is legal, the robocaller information is added to the Service Provider Allowed List.
4. Update the Individual Black List, the Service Provider Black List and the Service Provider Allowed List continuously at various steps in the blocking process. The update process increases the blocking accuracy and minimizes total processing time. Share the Service Provider Black List and the Service Provider Allowed List updates with other service providers, and incorporate updates to these lists from other service providers.

By applying the blocking strategy above, the RoboBlaster Will Not block wanted calls, and it ensures that calls from a legitimate caller are passed to the intended call recipients while calls from a disguised illegal robocaller using a legitimate caller's telephone number are blocked. This blocking process assures that Reverse 911 calls are passed to the recipient unconditionally, and that legal robocaller calls that the consumer has not explicitly blocked previously are passed to the recipient reliably.

Figure 1 summarizes the proposed RoboBlaster illegal robocaller blocker. In this figure and all other figures included in the proposal, regions shaded in green are "building blocks" of functionality that currently exist with the telephone service provider, at least to a substantial degree; single black lines indicate process flows, double black lines indicate data flows, and broad grey lines illustrate feedback.

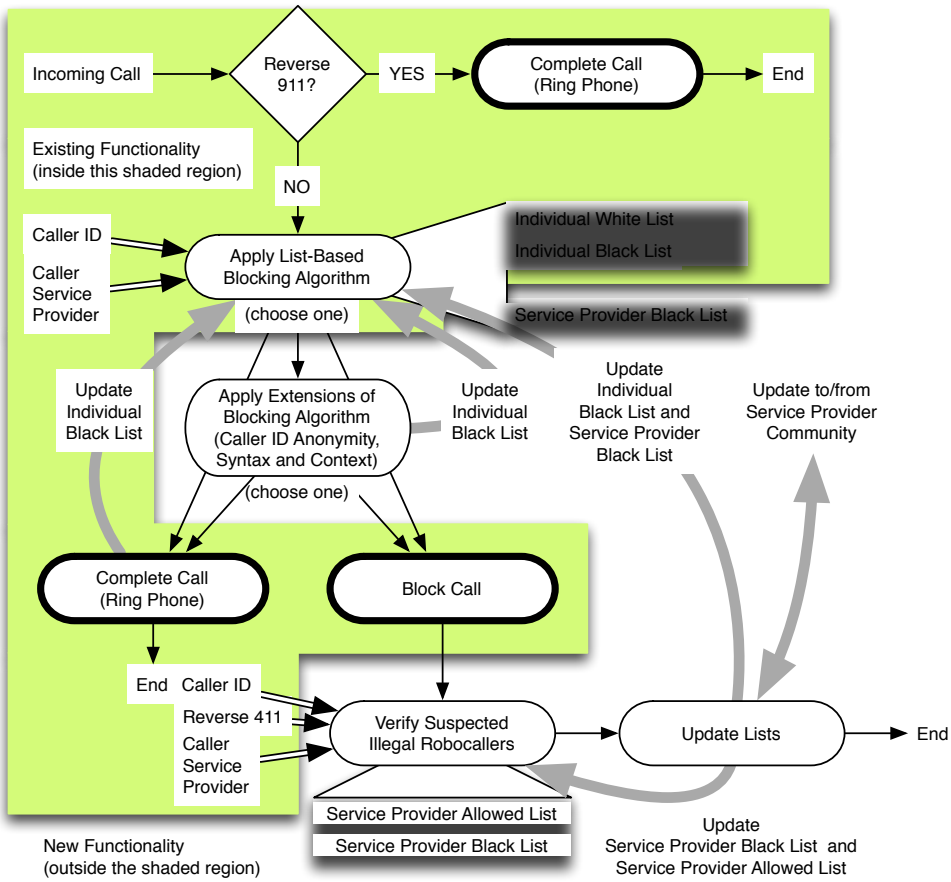

Figure 1 – Proposal Summary

The Roboblaster functions identically for every consumer of plain old telephone service (POTS), voice over IP (VoIP) and cellular telephone service to any device that uses push buttons for DTMF tones to dial a number – to virtually any landline, mobile phone currently in use manufactured since the 1980's and any VoIP phone in use today.

The socialized, industry-wide Service Provider Black List part of this proposal has been substantially borrowed from the Internet community and proven effective over many years of use by Internet service providers. Many Internet service providers filter all incoming e-mail against a worldwide Black List of known spammers to reliably block the vast majority (more than 95%) of spam e-mail messages for their customers. This concept can be extended in the telephone industry to a similar end to block known illegal robocallers. The Service Provider Black List is maintained by the telephone service provider industry through a verification process for suspected illegal robocaller reports from call recipients just as the e-mailer black list is maintained by the Internet service provider industry. Verified illegal robocallers are added to the Service Provider Black List, and updates to the Service Provider Black List are continuously communicated to all service providers in the telephone industry. This black list strategy is proven through years of use for e-mail service, and it is adaptable to the telephone industry.

The Service Provider Black List is fundamentally important to the blocking strategy. As the illegal robocaller changes Caller ID numbers and service providers to avoid blocking tools, the Service Provider Black List is continuously updated by the service provider community at large with new Caller ID and caller service provider information to defeat the known illegal robocaller. This list maintenance keeps pace with illegal robocaller changes to defeat each illegal robocaller as soon as it is discovered.

Maintenance strategies can also anticipate “next steps” by blocking specific blocks of numbers in combination with particular groups of service providers that have demonstrated a suspicious “reputation” based upon past experience to thwart the next iteration of change for the illegal robocaller.

The Blocking Algorithm Extensions are fundamentally important to defeating blocker adaptation and blocker avoidance strategies from the less sophisticated new illegal robocallers. The blocking algorithm extensions defeat obvious spoofing ploys on the fly, and the extensions are updatable to keep track of new illegal robocallers attempts to entice call recipients to answer their phones. The blocking algorithm extensions are analogous to an e-mail spam filtering application a PC user might purchase and install to augment the filtering already performed in the background by the service provider and in the foreground by the e-mail application.

The most troubling threat from the illegal robocaller to defeat the RoboBlaster or any other list-based blocking strategy is to hack and steal Individual White Lists to utilize for spoofing Caller IDs for robocalls directed to each Individual White List owner. The service provider security measures to protect white lists are not addressed in this proposal, but they should be of great concern as a white list caller always gets through to the recipient. Illegal robocaller sophistication does not currently expose this vulnerability, but it surely will in time.

An entirely new concept introduced by this proposal is an industry-wide Service Provider Allowed List of legal robocallers to compare suspected illegal robocallers to. A basis for this list already exists with every service provider that has standing requests to avoid taxes from consumers who document their qualified "501C" non-profit business organization status. The maintenance and socialization of the Service Provider Allowed List is very similar to the proposed industry-wide Service Provider Black List.

The RoboBlaster is Easy for the Consumer to Use

In its blocking operation, the Roboblaster is invisible to the consumer except for a simple process for the consumer to report suspected illegal robocallers that get past the blocking algorithms (the other 5%) immediately after the consumer hangs up their phone. From this perspective, it is identical to the existing phone feature that the recipient uses to command their service provider to block all future calls from the caller just received by pressing a simple sequence of buttons on their phone.

This proposal describes a generic consumer configuration and maintenance process for the individual white list and individual black list. The process is not described in detail as it may already exist with the service provider, but it could be performed in a web-based fill-in form, or from the phone keypad in conjunction with a voice-prompting system, or from an intelligent import and syncing method using the consumer’s electronic phonebook stored in their PC such as a Linked-In phonebook feature, or a combination of these tools. Tools currently in place for phone list building such as these are efficient, easy to use, and satisfactory for user communities including users with a variety of disabilities. Numerous time-proven options currently exist for list configuration and maintenance.

Typos and keypad errors by the user maintaining their individual white and black lists have limited impact. The most severe error is for a user to configure their Individual Black List from their “white list” phonebook. A list reset would resolve that error easily and conveniently for the error-prone user.

The RoboBlaster Can be Rolled Out Economically by the Service Provider

More than half of the solution to block at least 95% of illegal robocallers already exists with the service provider today, and the most beneficial elements of the proposal such as the Individual White List and the Individual Black List are deployable today without any additions to the telephone network infrastructure. The proposed illegal robocaller blocker primarily relies upon the Caller ID to identify and

block illegal robocallers. The Caller ID is a universal feature of every telephone voice service currently deployed in the United States, and it has been proven over decades of network deployment. Missing in the service provider infrastructure for a comprehensive feature to block illegal robocallers is the integration of several existing functions with several new functions and with databases for known and verified legal and illegal robocallers. Ever concepts proposed will be familiar to the service provider.

Deployment is economically realistic. Individual White Lists are supported for cellular services today by the larger service providers. Individual Black Lists are supported for all telephone services today by the vast majority service providers. White List and Black List services are sold to consumers as premium services by some service providers. Deployment of a Service Provider Allowed List and a Service Provider Black List are no more difficult or costly than the individual white list and black list features currently in use in the telephone industry and Internet industry.

It is essential that the service provider perform all of the processing necessary to block illegal robocallers if the required 95% of illegal robocallers are to be blocked successfully for all telephone services to all devices. An important element of the proposed robocaller blocker includes the collection and analysis of network path trace information to augment the analysis of the Caller ID for the Service Provider Black List. The network path trace is available from the recipient's service provider's network management systems, and this information identifies the robocaller's service provider at the network-to-network interface with other service providers' networks. Network Path Trace information is automatically exchanged between the vast majority of fiber optic networks deployed throughout the world today, and this information is routinely collected and utilized by service providers in the US today. The network path trace information is not passed to the recipient's telephone device, however, and this aspect of the blocker solution is the underlying reason that the service provider must perform the list-based processing to block illegal robocallers. The Network Path Trace is essential to identify stolen Caller IDs, sharpens the decision of whether or not to block a suspicious robocaller, and potentially provides a basis to initiate legal action against the owner of an illegal robocaller.

More than 50% of the proposed solution is available from service providers today with a black-list feature to block specified Caller IDs that eliminates repeat illegal robocaller calls immediately. This step towards the RoboBlaster implementation achieves a successful blocking "hit rate" of 50% or more as the majority or illegal robocallers call multiple times. All that is required for this step of the implementation to be effective immediately is for the service provider to make the feature available to all of their customers and extend the current feature by removing the limit for the number of callers blocked.

Incorporation of proven Internet spam e-mail blacklisting techniques tailored for a telephone industry Service Provider Black List with Caller ID in conjunction with caller service provider information extends the successful blocking "hit-rate" even further to 80% of more. This step requires new business agreements and information sharing agreements with new business partners. Deployment of a Service Provider Allowed List and a Service Provider Black List are no more difficult or costly than the individual white list and black list features currently in use in the telephone industry and Internet industry. This step of the solution can be accomplished in as little as six months in the current business environments that service providers operate in.

Extending the blocking algorithm for anonymity, syntax and context analysis for a 95% successful blocking "hit rate" in a first rollout of a smartphone "app" can be done in a matter of weeks by a skilled software developer. Incorporating the blocking algorithm extensions in service provider switching and routing systems instead is likely to be far more difficult and time consuming, demanding as long as two years to put first implementations in place. Improving these new features to fully meet consumer expectations and successfully adapt to clever illegal robocallers is likely to require an additional year or two after the first implementation before these blocking extensions work as optimally as possible.

2. OBSERVED ILLEGAL ROBOCALLER CHARACTERISTICS AND PLOYS

The proposal writer tracked and classified calls directed to the home phone for 30 days. The service provider has no easy way to provide these statistics for consideration:

- Illegal Robocalls Received: 17 or 32%
- Illegal Direct-Dialed Solicitation Calls Received: 6 or 11%
- Legal Robocalls Received: 3 or 6%
- Legal Product and Service-Related Calls Received: 4 or 8%
- Personal Calls Received: 21or 40%
- Work-related Calls Received: 2 or 4%

The home phone number was on the Do-Not-Call list for more than 30 days prior to counting calls. Only about two calls in every five were from people who were known – friends, family and business associates. About one-third of all calls received were illegal robocaller calls. Almost half of all calls received (the first two categories) were illegal and should not have been made if the Do-Not-Call List was regarded by the calling business.

Illegal robocallers had the following behavior and Caller ID indications:

- Four illegal robocallers called multiple times during the month;
- Two illegal robocallers were answered by service provider recordings that these numbers were not in service when the Caller ID number was dialed;
- Five illegal robocallers displayed names such as “PROMOTION” or “WINNER”
- Four illegal robocalls displayed an invalid phone number in the Caller ID;
- Four illegal robocalls displayed “Unknown Number in the Caller ID.

None of the illegal robocaller calls the proposal writer received on his home phone had valid and complete Caller ID information; conversely, all of the legal robocaller calls did have valid and complete Caller ID information. This finding is the key to blocking the illegal robocaller.

3. A BASIS FOR THE LISTS UTILIZED BY THE BLOCKING ALGORITHM

Assuring Essential Services and Desired “White List” Calls

The service provider delivers essential services such as Reverse 911 in any of several ways depending on the consumer’s services and devices. This proposed blocker does not preempt the delivery of Reverse 911 service in any way. Reverse 911 calls are to be passed to the consumer’s devices by the service provider before the service provider performs any call blocking.

After Reverse 911 calls have been assured, the Caller ID of an incoming call is compared to the consumer’s individual White List. Calls from white listed callers are completed before any attempt is made to block incoming calls. The consumer has an interest in assuring the completion of incoming calls from designated parties such as family members. These designated parties encompass the consumer’s Individual White List of numbers that are always passed to the consumer regardless of the any service provider’s preference to block them.

Figure 2 illustrates the proposed features and maintenance of the individual’s White List. The value of the individual’s White List associated with the illegal robocaller call blocking becomes apparent if a family member’s ID (telephone number) has been stolen by the robocaller for use in the illegal

robocaller's Caller ID, and the industry acts to block the illegal robocaller by erroneously blocking that family member's calls until the ID confusion is properly resolved. In the interim time, the individual's White List assures the completion of that family member's calls to the consumer. The individual's White List is an optional service element already supported by many cellular service providers today. It would be convenient if the individual's white list coincided and sync'ed with the consumer's electronic phone book.

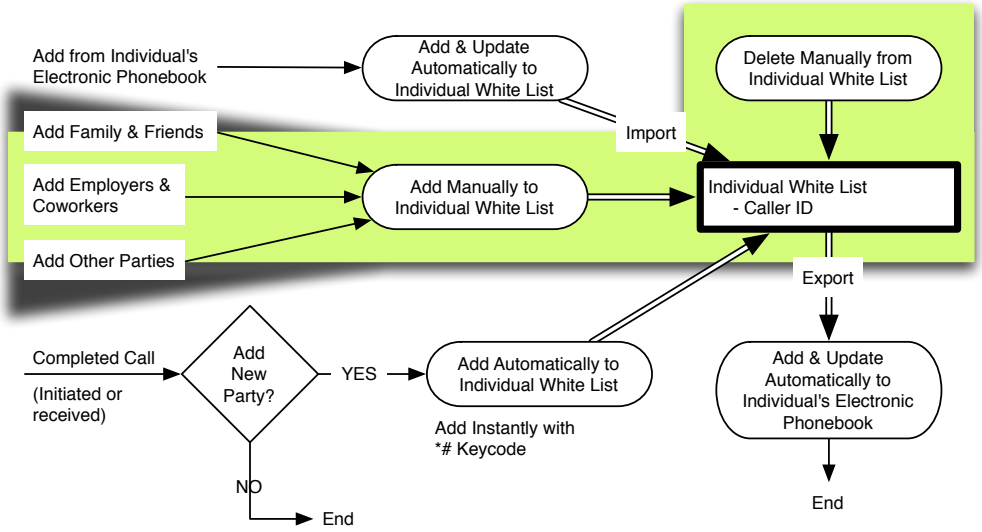

Figure 2 – Features and Maintenance of the Individual White List

Blocking Calls from Specifically Identified Numbers with "Black Lists"

Blocked caller lists or Black Lists are familiar to many telephone service consumers. An element of service currently available from virtually every service provider for virtually every telephone service is the Individual Black List. The Individual Black List is the first tool that is useful to block illegal robocallers. Regardless of the success of automatic techniques to block illegal robocallers discussed in subsequent sections of this proposal, the service consumer can always block future calls from some illegal robocallers that happen to "gets through" by adding the robocaller's Caller ID to their individual Black List. Individual Black List additions must be convenient for the consumer to make, and a designated *# key code from the telephone handset following an illegal robocall should be all that is required to update the individual's Black List with the illegal robocaller's Caller ID.

Current individual Black List features from various service providers can be extremely limited to small numbers of blocked callers; some service provider limit the blocked caller list to as few as six numbers, although twenty callers is a common limit. To be effective, the individual's Black List must allow for far more blocked numbers, and one hundred blocked numbers may be a useful limit. Figure 3 illustrates the proposed features and maintenance of the individual's Black List.

The Service Provider Black List is a new feature for most telephone service providers. The Service Provider Black List is a feature borrowed from the Internet community where comprehensive global black lists are used to filter spam e-mail and block it for the Internet service provider's customer. In a real sense, illegal robocaller calls are analogous to spam e-mail, and this problem has been effectively addressed with an Internet service provider's Black List. The same can be done in the telephone industry in much the same way.

It is important to note that the Service Provider Black List must maintain more information that just the Caller ID. In order to prevent erroneous blocking of a legitimate caller whose telephone number has

been hijacked by an illegal robocaller, it is vital to correlate the origin service provider with the Caller ID information. The origin service provider is determined from the network path trace information that is available from the management systems of any contemporary network that switches telephone traffic. The origin service provider information is necessary for billing records, and it is available on demand from these management systems today. Figure 4 illustrates the proposed features and maintenance of the Service Provider Black List.

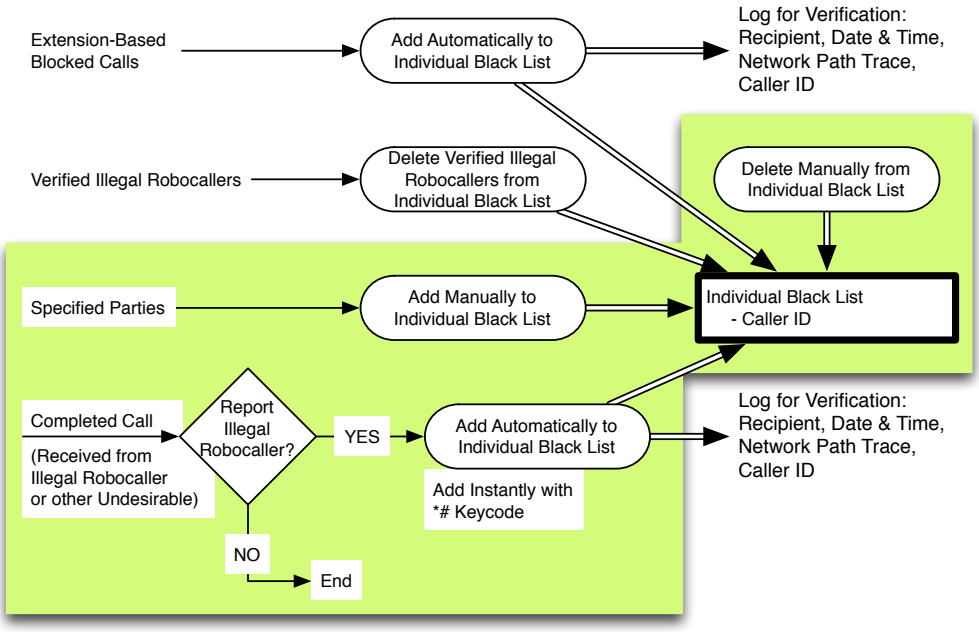

Figure 3 – Features and Maintenance of the Individual Black List

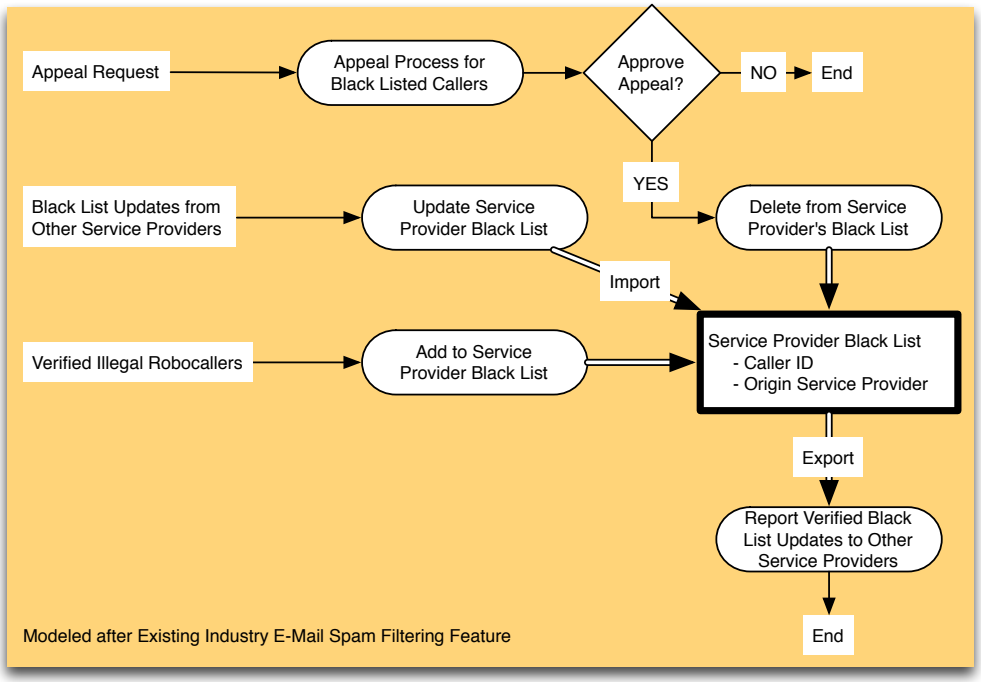

Figure 4 – Features and Maintenance of the Service Provider Black List

The following companies dominate e-mailer blacklisting or “reputation” services for ISPs in the US:

Spamhaus	(www.spamhaus.org)
Spam Cop	(www.spamcop.com)
Spews	(www.spews.org)
DSBL	(www.dsbl.org)
MAPS	(ers.trendmicro.com)

The above companies are experienced and suitably positioned to perform a similar Black List service for the telephone industry and contribute to the illegal robocaller blocking solution. Any robocaller that appears on a Service Provider Black List would be blocked for every call made to a recipient whose service provider subscribes to a black listing service that is self-maintained or offered by a company such as those listed above.

Assuring the Legal Robocaller’s Service with an “Allowed List”

The Service Provider Allowed List is another new feature for most telephone service providers. The Service Provider Allowed List is a service provider community list utilized in the illegal robocaller verification process to determine whether the reported illegal robocaller is known to be legal. The Service Provider Allowed List behavior is very similar to the Service Provider Black List. Maintenance and distribution of this allowed list could be performed by the same reputation service utilized for the Service Provider Black List.

Like the Service Provider Black List, the Allowed List must maintain more information that just the Caller ID. It is vital to correlate the origin service provider from the network path trace information with the Caller ID information to prevent erroneously blocking a legitimate robocaller whose telephone number has been hijacked. The origin service provider information is readily available from the management systems. Figure 5 illustrates the proposed features and maintenance of the Service Provider Allowed List.

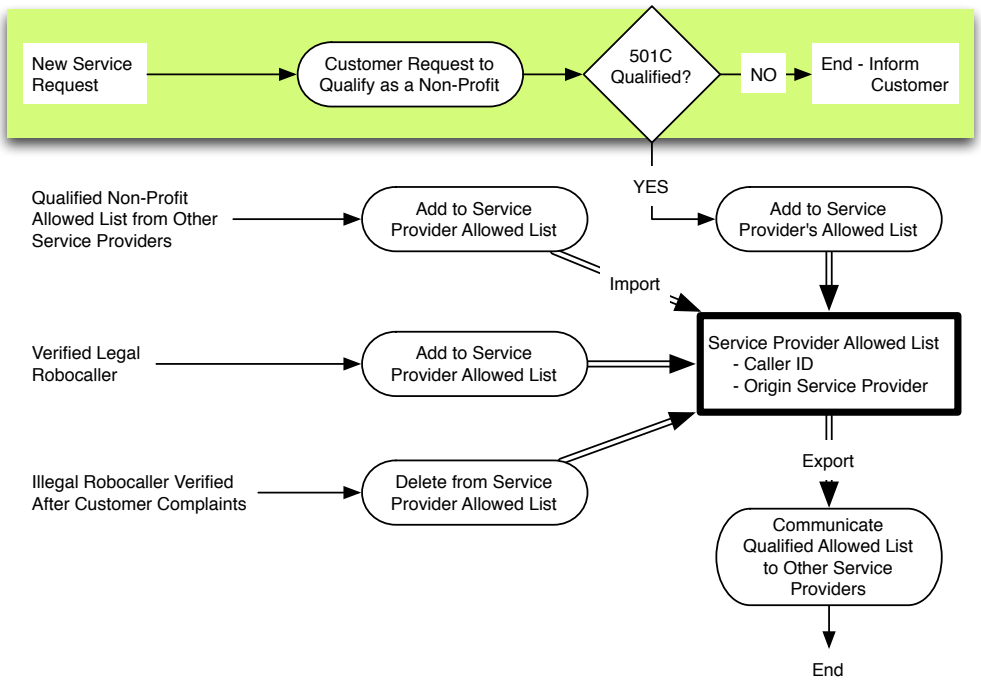

Figure 5 – Features and Maintenance of the Service Provider's Allowed List

4. PUTTING IT ALL TOGETHER

Using the Lists to Block Known and Suspected Illegal Robocallers

A basis for a number of lists that are useful to block illegal robocallers has been establish in this proposal. The key to blocking 95% of illegal robocallers without interfering with the completion of legitimate calls lies in the clever use of these lists. Figure 6 below summarizes the processing of incoming calls by comparing call information to these lists in a particular order. This processing flow enhances the blocking accuracy while minimizing the processing burden for the service provider. Figure 6 illustrates the list-based blocking algorithm to block known and suspected illegal robocallers.

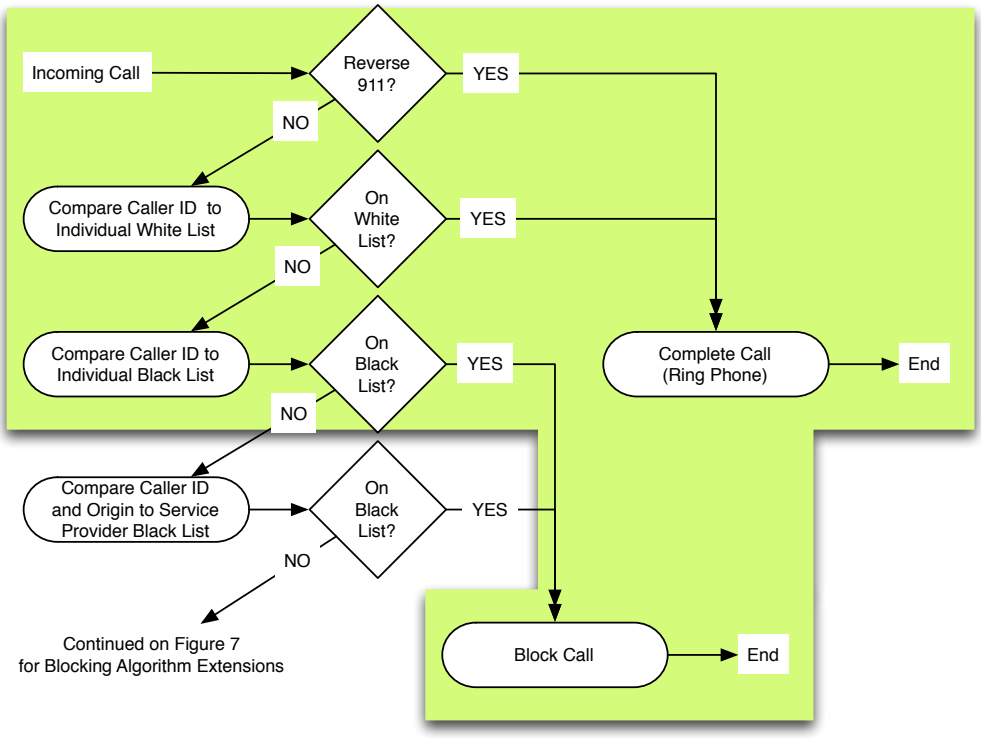

Figure 6 – List-Based Illegal Robocaller Blocking Algorithm

If the incoming call is a Reverse 911 call, it is passed to the recipient without further delay or processing of any kind.

The Caller ID of an incoming call is compared next to the Individual White List. This is essential to do before any comparisons to black lists. In the event that a desirable caller's phone number is erroneously black-listed by the service provider, adding that number to the Individual White List insures that an incoming call from that caller is always competed and passed to the recipient.

The Caller ID is compared next to the Individual Black List. The Individual Black List is processed before the Service Provider Black List for three reasons:

1. The Individual Black List is a shorter list than the service provider list and therefore requires less processor burden and time to compare the Caller ID to;
2. The Individual Black List addresses several service objectives including blocking nuisance calls as well as recently received illegal robocaller calls not yet verified by the service provider; the frequency of repeat nuisance calls and unverified illegal robocaller calls can be high;

3. The Individual Black List requires only the Caller ID, but the Service Provider Black List requires the origin service provider from the network path trace information provided by another management system that is unrelated to the system providing the Caller ID; the processing burden is significantly less for the Individual Black List.

Finally, the Caller ID and the service provider of the incoming call included in the network path trace are compared to the Service Provider Black list.

It is important to note that information related to the incoming call is not compared to the Service Provider Allowed List in the blocking algorithm. The objective of the illegal robocall-blocking algorithm is to make a decision to block an incoming call, and processing burden is prioritized to a blocking determination (and not a completion determination). The default if all blocking algorithm tests fail is to complete the incoming call with the same outcome as comparing incoming call information to the Allowed List as a last step, therefore an Allowed List test is not considered in the blocking decision.

If the incoming call is not completed or blocked based upon inclusion in a list, the Caller ID is analyzed even further to determine if it is likely to be from an illegal robocaller. The next section describes the follow-on Caller ID analysis.

Analyzing the Caller ID to Detect and Block Unknown Illegal Robocallers

The illegal robocaller Caller ID is often anonymous, displaying "Private Name" & "Private Number", "Unknown Name" & "Unknown Number", or a blank with no information displayed at all (null name and null number). The service consumer will block a great many illegal robocallers by asserting their preference to block all anonymous callers; however, some legitimate callers who insist on calling anonymously will be blocked erroneously in that event. Service provider equipment is capable of detecting anonymous Caller ID's, but no mechanism is in place for detected anonymous ID's to prompt the call blocking action.

The illegal robocaller Caller ID is often malformed. Examining the Caller ID syntax for a number of characteristics can detect as many as one-third of today's illegal robocallers. Current service provider equipment is capable of analyzing the Caller ID for compliance with a number of formal, standard, industry wide requirements for the Caller ID and indicating if a Caller ID is malformed. Common illegal robocaller Caller ID errors are:

- Reversing the name and number fields;
- Omitting the name or number field (leaving it blank);
- Displaying an incomplete number with fewer than normal digits such as 495-128;
- Displaying US numbers with area codes or exchanges that erroneously begin with 0 or 1;
- Displaying US numbers to appear to be toll-free but are in fact invalid such as 885-123-4567;
- Displaying International numbers (more than ten digits) that include erroneous country code or city code information.

Each the above illegal robocaller Caller ID errors can be detected by the service provider today. Automatically blocking all calls with malformed Caller ID's is an effective step to block most illegal robocallers as well as a great many criminal callers and nuisance callers. Service provider equipment is capable of detecting malformed Caller ID's, but no mechanism is in place for detected malformed ID's to prompt the call blocking action.

The illegal robocaller may display a "hook" keyword in the Caller ID such as PROMOTION or WINNER or GIFT CARD or SEX or PILLS. The illegal robocaller frequently also displays a contrived number

pattern in the Caller ID such as (444) 444-4444 or (999) 999-9999. Examining the context of Caller ID for suspicious keywords and number patterns and blocking those calls would require several new enhancements to current service provider software.

All these behaviors have been observed for illegal robocallers by the proposal author. All of these behaviors can be detected in the Caller ID information to prompt the action of blocking the illegal robocaller call. Figure 7 illustrates the most effective Caller ID processing flow to detect and block unknown illegal robocallers and other undesirable callers who misrepresent themselves with false Called ID information.

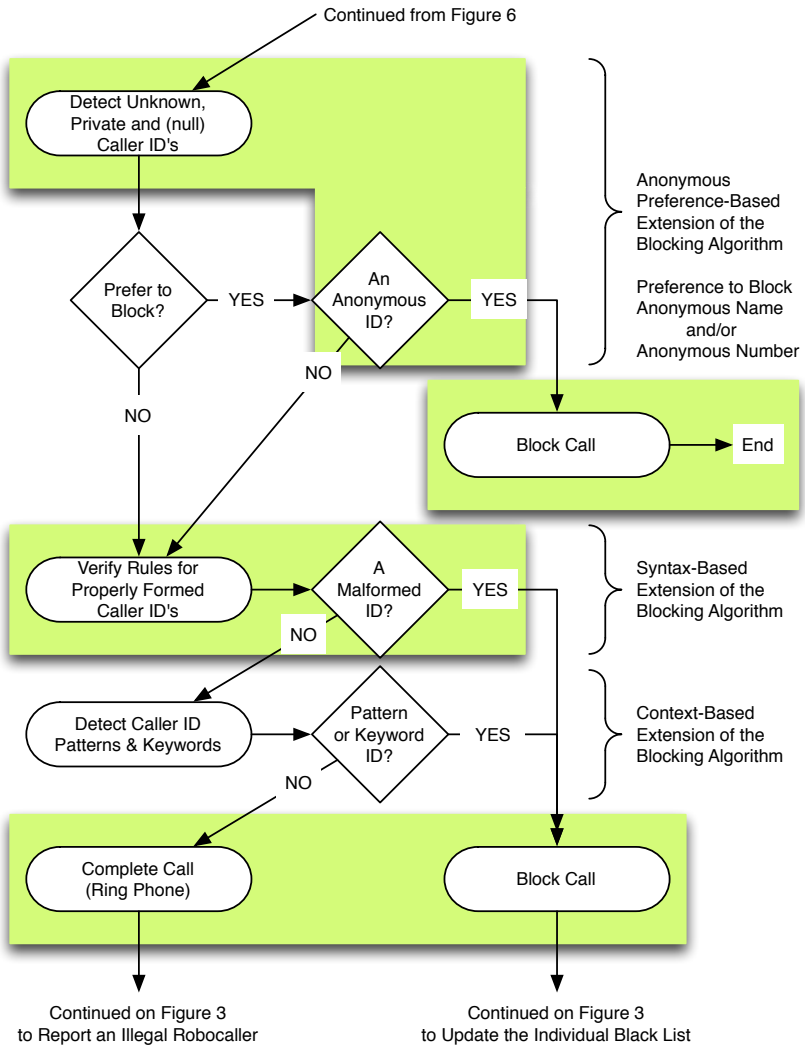

Figure 7 – Anonymous, Syntax and Context Extensions of the Illegal Robocaller Blocking Algorithm

The Caller ID information must be processed in the service provider's switching equipment to accommodate illegal robocaller Caller ID anomalies for all telephone services and devices. The robocaller blocking algorithm extensions described above could potentially be processed by a cellular "smartphone" or smart VoIP phone application to successfully block many unknown illegal robocallers with anomalous Caller ID's, but the significant numbers of POTS consumers and unsophisticated cellphone consumers would be unable to implement such a solution. It is therefore essential that the service provider perform all of the Caller ID processing in the switching equipment to block 95% of illegal robocallers for all telephone services and telephone devices.

Identifying and Verifying Suspected Illegal Robocallers

The illegal robocaller Caller ID may display a fictitious phone number (a stolen ID). Calling the number back in this case results a "Not In-Service" message or a puzzled person answering the return call. Service provider equipment is capable of performing an In-Service test of any telephone number, and one result of the test is simply a determination of whether or not that number is in service. Service provider equipment is also capable of performing a 411 Reverse Lookup of the number for the corresponding directory information, but no mechanism is in place to correlate the recovered directory information with a Caller ID to detect a mismatch of information. Although these tests are impractical for illegal robocaller detection due to intrinsic delays and processing burden, the In-Service and Reverse 411 tests are useful for illegal robocaller verification after a suspected illegal robocaller number has been reported to the service provider. Figure 8 illustrates the procedure to verify an illegal robocaller.

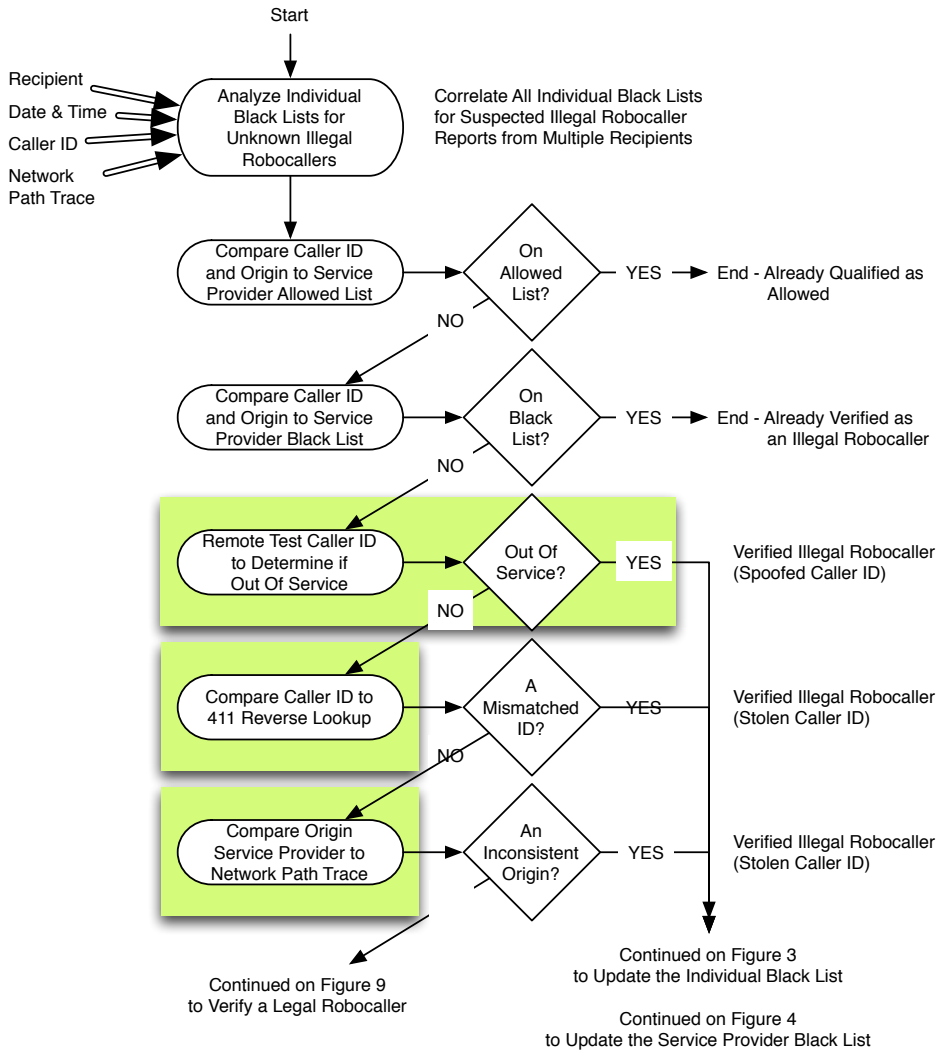

Figure 8 – Procedure to Verify an Illegal Robocaller

The illegal robocaller Caller ID may display a number that does not accept incoming calls in violation of the Telemarketing Sales Rule requiring legal robocallers to facilitate a "do not call" request from the call recipient. Calling the number back in this case results in a rapid busy signal or an endless ringing

behavior. Like the “Not In-Service“ message, this behavior is impractical for illegal robocaller detection, but it is useful to verify an illegal robocaller.

Finally, the network path trace information for the reported illegal robocaller call will include the service provider for the robocaller.

Figure 9 illustrates the procedure to verify a legal robocaller.

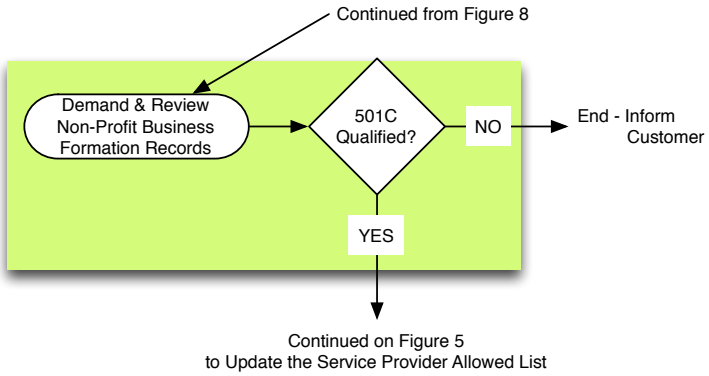

Figure 9 – Procedure to Verify a Legal Robocaller

Updating All the Lists – “Feedback Loops” are Essential

Throughout this proposal, the drawings refer to update procedures at the end of every step of the robocall blocking process to keep the lists current and accurate. These “feedback loops” are summarized in Figure 1 with broad grey arrows to indicate the data flows in the feedback mechanisms. The following update procedures are required to keep the lists up to date:

- Individual White List (figure 2) – Updated by the caller or the recipient from the telephone device during or immediately following a call to preserve the future ability to receive a call regardless of black list status of the caller’s telephone number;

- Individual Black List (figure 3) – Updated by the call recipient from the telephone device during or immediately following a call to block the illegal robocaller for all future calls; updated by the extensions of the blocking algorithm to block robocallers that the algorithm extensions indicate are suspected of being illegal; updated by the verification process to delete a number that has been added to the service provider black list;

- Service Provider Black List (figure 4) – Updated to add verified illegal robocallers; updated to delete verified legal robocallers; updated for additions and deletions based upon verifications by other service providers;

- Service Providers Allowed List (figure 5) – Updated to add verified legal robocallers; updated to delete verified illegal robocallers; updated for additions and deletions based upon verifications by other service providers;

These update procedures keep the lists current and sharpen the accuracy of illegal robocall blocking.

5. SERVICE PROVIDER CONSIDERATIONS

Incentives and Protections

It should be apparent to the reader that the illegal robocaller blocker requires time, money and infrastructure resources of the service provider to deploy and maintain. The service provider is likely to decline this proposal outright without incentives and protections. A number of service provider considerations are proposed below:

1. To offset service provider expenses, the service provider should be allowed to sell the comprehensive blocking service for a small fee as an optional service for their customers. A $5.00 monthly fee would seem to be reasonable.

2. The service provider should be able to block all calls with Caller IDs that have been modified by the customer to change the name from that on record or to change the number from that on record. A prohibition against Caller ID changes by the customer should appear in the service provider's terms and conditions of service. The FCC and the FTC should uphold this Caller ID change prohibition as a condition of service and a justification to stop service. It should be noted that all legal robocallers had accurate Caller ID information presented, and all illegal robocallers had inaccurate Caller ID information presented to the call recipient according to the 30-day findings of this proposal writer.

3. Exchanging Black List and Allowed List information between service providers must not be deemed as anti-competitive by the FCC or the FTC.

4. Blocking illegal robocallers calling from outside the recipient's service provider's network reduces network congestion and frees network resources for revenue generating opportunities for the recipient's service provider.

An Optional Service Provider White List

A Service Provider White List may provide an efficient and effective means to assure delivery of government calls and communications. Such a white list exists today in part in the form of the "Blue Pages" of government listings currently found in the service provider's telephone directory provided to many consumers doorstep. If deployed, the Service Provider's White List would be the first list referred to in the list-based blocking algorithm to assure government and service provider communications to the consumer. Figure 10 illustrates the proposed features and maintenance of the optional Service Provider White List.

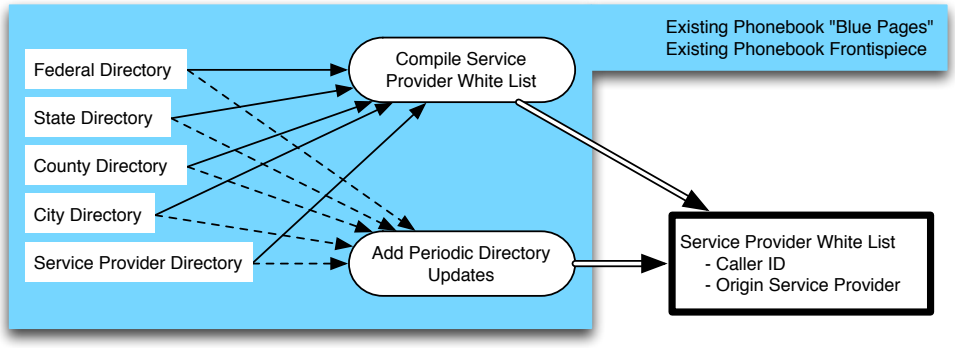

Figure 10 – Features and Maintenance of an Optional Service Provider's White List

A Significant Implementation Simplification

The requirement to block 95% of illegal robocaller calls for all services sets a high bar for implementation. A significant simplification for the service provider is possible if a lower call-blocking "hit rate" or success rate is allowed – say, about 80% today instead of 95% for POTS phone service and for any VoIP and cellular service consumers who use "dumb" devices (not smartphones).

This simplification potentially puts the blocking algorithm extensions in an "app" in the smartphone. A smartphone application could easily block anonymous callers according to user preference, block calls with malformed Caller ID's, and block calls with certain keywords embedded in the Caller ID. A smartphone call blocker "app" is analogous to an optional e-mail spam filter application that runs on one's PC.

This simplification offloads a significant processing burden for the service provider and shifts that burden to the smartphone. This simplification makes the service provider implementation less costly. This simplification also broadens a market for a new class of smartphone applications. The detractor for this simplification is simply 1) that the smartphone owner is the only consumer who realizes the objective 95% blocking "hit rate" that is required, and other telephone service consumers realize a greater number of unwanted illegal robocalls; and 2) that the smartphone user can potentially defeat the receipt of reverse 911 calls and other legitimate callers without realizing what they have done.

6. THE BOTTOM LINE

Implementing the RoboBlaster illegal robocaller blocker proposal will block 95% of all illegal robocalls for all public telephone services in the US. This proposal is comprehensive and completely describes the high-level illegal robocaller blocker solution. Without substantial FCC and FTC enforcement staff and budgets, illegal robocallers are likely to become more common, more aggressive, and more scam-oriented over time disrupting privacy and legal commerce unless they are blocked effectively as this proposal describes.

The RoboBlaster is virtually invisible to the user and presents nothing new to the user who is already familiar with white list and black list features that service providers currently offer.

The RoboBlaster is economically deployable. The RoboBlaster is a solution that can be deployed incrementally, and currently available features from the service provider have the potential to deliver significant benefit immediately. Full-scale deployment of the RoboBlaster can be achieved in as short a time as twelve months, but twenty-four months is a more likely deployment timeframe.

Through the clever design of the sequence of processing, blocking and list maintenance that is proposed, more than 95% of illegal robocaller calls will be blocked in short order for every telephone service consumer of plain old telephone service (POTS), Voice over IP (VoIP) and cellular service. The proposed algorithm to block illegal robocallers assures completion of Reverse-911 calls and avoids erroneously blocking legal robocallers and other legitimate and desired callers.