It’s My Number

Robocall Challenge Proposal
David Frankel, CEO, ZipDX LLC
January 17, 2013

Brief Description

A cadre of rogue robocallers is calling millions of consumers, creating a rising level of anger and frustration. Thousands of complaints pour into the FTC daily. Stopping the robocalls at the receiving end is a gargantuan technology deployment challenge and requires effort on the part of every aggrieved (or potentially aggrieved) telephone subscriber. There are tremendous issues with “false positives” that will interfere with regular phone calls. We can be certain that the robocallers will continue to use any means, even if illegal, to subvert whatever screening techniques we put in place.

Ideally, illegal robocalls would be stopped at the source. That would completely remove the burden and frustration from the end-users. The regulators have diligently attempted to stop the most egregious abusers, but the limited data available, plus the obfuscation (such as caller-ID spoofing) used by the perpetrators and the circuitous paths taken by the calls makes it extremely difficult to identify the point of origination with current technologies and procedures.

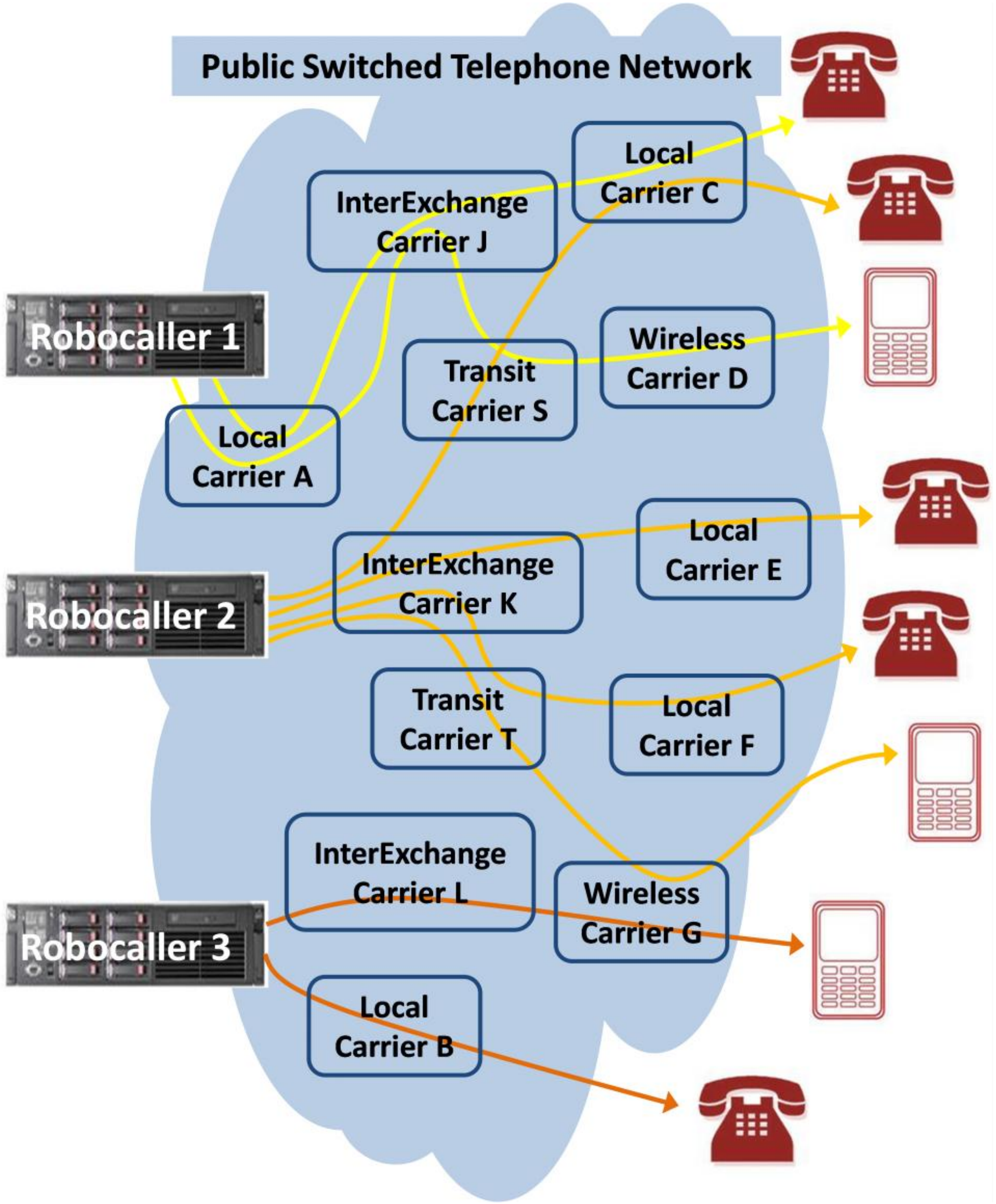
Our solution is a “mash-up” of crowd-sourcing (200,000 complaints to the FTC each month plus 20,000 more to the FCC) and big data (the extensive call signaling records captured by the telephone companies) with straightforward analytics to identify the sources of these illegal calls. In near-real-time, we take complaint data, as well as data from our own “honeypot” numbers, and automatically track the calls to their origin using detailed carrier-by-carrier signaling data. Once we know unequivocally where the calls are coming from, validated by multiple complaints pointing back to the same source, we can use laser-focused enforcement techniques to stop the illegal activity. Within a day or two of a new robocaller cropping up (potentially even faster), we can find it and shut it down. Ultimately, this serves as a huge deterrent to illegal robocalling in the first place.

This is an “industry solution,” depending on cooperation of carriers and regulators. We leverage the complaints ALREADY being filed by those end-users that voluntarily do this today, and data ALREADY captured by carriers. But ALL end-users, complainants or not, benefit from a wholesale reduction in illegal calls. We don’t require universal cooperation, but the greater carrier participation in our effort, the more completely we can eradicate this scourge. With regulatory “encouragement” from the FCC, we believe that we can drive carrier participation to a high level.

This solution is called “It’s My Number” because we are allowing end-users to take back their phone numbers from the law-breakers that have made, in some cases, US phone service more burdensome than beneficial.

Stopping at Origin vs. Destination

Suggesting that each owner of the 200 million phone numbers on the national Do-Not-Call list must deploy some hardware or software to actually stop the unwanted calls is impractical and expensive. It is much more efficient and pragmatic to stop the calls at the source. Once we know the source, we work with the perpetrators to prevent future illegal calls. The diagram below shows how robocalls move through the network.



The arrows show the path each call takes to get from the robocalling origin to the annoyed consumer. By tracing robocalls backwards through the network (through multiple carriers if necessary), we determine how they originally entered the network. We will know the Local Carrier or Inter-Exchange Carrier that initially granted them access to the PSTN. And that carrier will know the identity of the perpetrator (or at least of the non-US-carrier entity responsible for the call). Correlating multiple calls back to a common point of origin gives us an increasingly accurate picture of an illegal source.

Anatomy of a Robocall

Developing a method to stop illegal robocallers requires a detailed understanding of how they operate. While a wide array of technologies and techniques are used, the following elements are generally involved:

A computer-based call generator can easily place several calls per second, or on the order of 10,000 calls per hour. Working from 8 AM Eastern time to 9 PM Pacific time (apologies to Hawaii and Alaska), that's 160,000 calls per day – over one million calls per week. And that's just one system with a hardware cost of a few thousand dollars or less. It's fairly trivial for a robocaller to scale to much higher volumes.

These call generators may deployed directly by the organization trying to sell or scam the end-user. Or, that organization will engage an intermediary to perform "voice broadcasting" on their behalf. Voice broadcasters run their own networks of call generators and specialize in making huge volumes of outbound calls, typically charging a small fee for each completed call. Such services can be activated in a matter of minutes via the Internet. Many voice broadcasters operate legitimately, but some perform no diligence on their customers.

The call generator is connected to the Public Switched Telephone network via a "legacy" telephone trunk (ISDN Primary Rate Interface, or conventional T-1 trunk). Or, it may be connected using VoIP technology (perhaps through an intermediary, maybe outside the United States). Ultimately, it gets to a US-licensed Local Carrier (there are a few thousand of these) or Inter-Exchange Carrier (there are a few hundred of these).

The point of entry to the PSTN is called the INGRESS CARRIER.

When the call generator places a call, it typically provides the following call signaling parameters:

CallED Number	Destination of the call	Taken from some list, or generated randomly. May or may not have been screened against local or national Do-Not-Call lists.
CallING Number	Required by regulation to indicate the source of the call	May be valid or may be chosen specifically to obscure the call origin; call can route regardless.
Charge Number	Sometimes used by telephone companies to determine call charges	May or may not be valid. Need not be valid for call routing.
Presentation Indicator	Specifies whether the CallING number is to be made available to the callED party.	

The Ingress Carrier may or may not inspect the CallING Number and/or the Charge Number for validity. Robocallers can "spoof" these values and, if not screened by the Ingress Carrier, the call will arrive at the destination with whatever values were supplied by the Robocaller.

By examining the CallED Number and referencing its own and industry routing tables, the Ingress Carrier determines the identity of the Egress Carrier (that is, the carrier that serves the end-user with the specified CallED Number) and thus where to next send the call.

There are several possibilities:

1. The Ingress Carrier and the Egress Carrier are the same. This means that the Ingress carrier can route the call directly to the end-user using its own facilities.
2. The Ingress Carrier is directly connected to the Egress Carrier. The Ingress Carrier sends the call to the Egress Carrier for completion.
3. The Ingress Carrier and the Egress Carrier are not directly connected. The call will be sent to an intermediate carrier (Inter-Exchange or Tandem) and the process will repeat, perhaps through several intermediate carriers, until it reaches the Egress Carrier.

As the call moves from each carrier toward the callED party, the original signaling information is normally passed along and regulations stipulate that it not be modified en-route. However, in some circumstances it may be technically infeasible to maintain this data; other times, it is purposefully manipulated as part of some economic fraud. Most of the time, it arrives intact at the Egress Carrier.

The traditional PSTN signaling system (SS7) does NOT keep track, in one spot, of the complete end-to-end path taken by a call. Each involved carrier knows only the immediate neighbor from which it got the call and the next neighbor to which it is sending it. (Of course, telephone calls are bi-directional, but we talk about directionality of the call as from the callING party towards the callED party.)

In earlier days, the cost of aggregating and storing the details for billions of calls was enormous, and carriers retained only the minimal data they needed to generate bills. (For example, they wouldn't bother to save any data for calls that were not completed, since they couldn't be charged.) Now, however, most carrier networks use modern switching technology that readily records most of the signaling data associated with every call attempted through their network. They typically aggregate this data in a central repository and make it searchable for use not only for billing, but for network trouble-shooting, traffic analysis, capacity planning, fraud detection, legal mandates, and other business purposes. Data captured generally includes (VoIP terms are shown in parenthesis):

CallED (To:) Number, CallING (From:) Number, Charge (P-Charge-Info:) Number (each 10 digits), Presentation Restriction	Provided by the original caller, or (for the last 3) substituted/inserted by the Ingress Carrier
Local Routing Number (10 digits if required)	Pseudo phone number used to route the call if it has been ported from one carrier to another
Jurisdiction Indicator Parameter / JIP (6 digits; available in some cases)	Provided by the Ingress Carrier, indicating the carrier and location of the originating call (not provided by all carriers for all calls)
Originating Point Code (Origin IP Address)	The Signaling System Node Address from which the carrier received the call
Destination Point Code (Destination IP Address)	The Signaling System Node Address to which the carrier sent the call
Other Source/Destination Information	Trunk and/or Switch information for end user connections, or for carrier connections using older technology
Redirecting (Diversion:) Number(s)	Record of end-user "call forwarding"
Date and Time, Duration, Status	Status=Answered, Busy, Invalid, etc.

Despite tremendous improvements in data storage economics, it still may be impractical to retain this data indefinitely, so some carriers only keep the most detailed information for something on the order of 48 hours.

It’s My Number In Action – Our Proposal

When we learn that an end-user has received an illegal robocall, our system springs into action, searching backwards with our participating carriers to find the origin. We learn about calls in two ways:

We will operate our own “honeypot” numbers (and would also like to leverage those already operated by the FTC). These are recycled telephone numbers assigned to us from the standard number pool, served by a variety of different local exchange carriers, including mobile operators. These undisclosed numbers are not used for any purpose other than to receive calls. They are answered by an automated system that provides a simplistic imitation of a human (“Hello, this is George?”) and records the received audio. Calls that match a “robocall profile” trigger subsequent investigation steps; we generally expect these numbers only to receive robocalls and wrongly-dialed calls.

We encourage complaints from end-users. We will operate our own web site, and will have an analogous telephone response system so that people can also file complaints over the phone. We will allow end-users with the appropriate technology to forward robocalls to a honeypot number we publish for this purpose. But most importantly, we want to connect, in some fashion suitable to the agencies, to the FTC and FCC on-line complaint forms so that we can get near-real-time access to the steady stream of complaints they receive. [We’d like to work cooperatively on the forms used, and appreciate the comprehensive nature of the FCC form in particular. To accurate time-of-call information and timely reporting, we’d change from requesting “date and time of the call” to “how long ago did you receive this call” (5 minutes, 30 minutes, etc.). Other optimizations are possible.]

Armed with a candidate callED phone number and time of the call, we then AUTOMATICALLY:

A. Assign a unique identifier (UID) to this call
B. Look up whether the callED number is on the DNC list, and if so, when it was added
C. Look up the callED number in the industry Local Number Portability (LNP) database and determine the Egress Carrier (for toll-free numbers, complainant must provide Egress Carrier)
D. If the Carrier is an It’s-My-Number member:
    i. Query the Carrier over a secure connection for the call signaling details associated with any calls to the CallED Number within a narrow window around the call time; if the CallING number is provided (spoofed or not), use that to further qualify the search
    ii. If no calls are found, note that in our database and give up
    iii. If more than one call is found, assign UIDs to the additional calls and fork this process to process each individually; proceed here with the first call in the list
    iv. Capture and associate this signaling information with the UID assigned to the call; and
    v. If the call has Redirecting Number information, re-initiate the query process using the appropriate CallED number, or…
    vi. If the call originated with this Carrier, declare this carrier the Ingress Carrier, mark it as such for this UID and cease our query process; otherwise…
    vii. If the JIP is available, determine the (tentative) Ingress Carrier based on the JIP using the industry Local Exchange Routing Guide (LERG) and perform an iterative query (Step D); and also…
    viii. Determine the prior carrier from the Originating Point Code (or other origination data) and perform an iterative query (Step D).
E. If the Carrier is NOT an It’s-My-Number member, note that in our database and stop.

It is important to note that our process does not depend on the CallING Number. We capture this number when available and use it to filter our searches and (tentatively) correlate our analytics. But we do not require that the CallING Number be present or valid to do our tracing and analysis.

Our intention is that the above process is fully automated and the data retrieved in seconds. To the extent that technical barriers prevent us from achieving that goal initially, we will employ semi-automated techniques (such as automatically dispatching secure emails to designated contacts at participating carriers, requesting manual call traces with automatic parsing of the returned results). This will allow us to grow into the large volume of transactions that will ultimately be required.

Since the laws and regulations vary depending on additional details of the call, we will store in our database: whether the callED number is served by a wireless carrier; DNC status and add date; Calling Name data (retrieved from the industry CNAM database); and we'll capture call characteristics reported by the complainant or recorded by the honeypot system (verbal identification provided by caller, if any; verbal call-back number; DNC option offered and exercised; pre-existing business relationship or express permission to call; abandonment status and announcement if any, etc.). All of this information will prove useful in determining the compliance of the call and bringing illegal robocallers to justice.

Many of our trace attempts will fail when we are stymied by a non-participating carrier. But our database will grow quickly, to the point that the following processes will have statistical significance:

- Examine signaling details from the Ingress Carrier records we've captured and rank according to matching origination details. Review the full set of entries associated with these calls, and retrieve call recordings, if available, from our honeypot numbers. Research the validity of the CallING Number and Charge Number parameters. Contact the perpetrator and/or the Ingress Carrier for resolution.
- Examine our intermediate records associated with calls where we could not trace back to the Ingress Carrier. Rank according to which non-participating carriers are blocking our ability to trace. Contact these carriers and enlist their cooperation.

While the data mining aspects of these steps will be largely automated, significant human interaction will be required to interface with carriers and robocallers. We also expect to engage heavily with the FTC and FCC to create public awareness, to optimize data gathering, and to pursue enforcement actions.

It's My Number is targeted at robocalls, but it will work against any set of calls sourced from the same point, whether placed by robocallers or predictive dialers or humans. Because our system relies on cross-correlation of complaint data, and because we don't expect to get 100% participation by all carriers, those making massive numbers of calls will appear first on our radar. We will find a predictive dialer placing 100,000 calls divided among four different ingress carriers over two weeks. But we may not identify a real estate agent's assistant manually dialing 250 numbers in the community directory.

Carrier Participation

Our solution requires participation by telecommunications carriers. The more voluntary participation we get, the more effective our solution can be. We need only a few participating carriers to start. There are a few thousand carriers registered with the FCC, but the largest have a dominant market share with the remainder comprising a very long tail. The chart below shows the top carriers by subscriber count (numbers are approximate and come from Wikipedia, Leichtman Research Group, Strategy Analytics, FCC, CTIA and company reports; date shifts make the data somewhat less accurate):

Wireline Residential		
Carrier	Subscribers	Cum %
AT&T	21,232,000	25%
Verizon	12,626,000	40%
Comcast	9,342,000	51%
CenturyLink	9,040,000	62%
Time Warner	4,544,000	67%
Frontier	3,267,487	71%
Cox	3,170,000	75%
Cablevision	2,357,000	78%
Windstream	1,931,700	80%
Charter	1,791,300	82%
ALL	84,355,000	

Mobile		
Carrier	Subscribers	Cum %
Verizon Wireless	111,000,000	33%
AT&T Mobility	106,000,000	65%
Sprint Nextel	55,000,000	81%
T-Mobile USA	35,000,000	92%
MetroPCS	10,000,000	95%
Cricket / Leap	6,000,000	96%
U.S. Cellular	5,800,000	98%
C Spire Wireless	800,000	98%
Alltel	600,000	99%
Cincinnati Bell	446,000	99%
ALL	335,000,000	

Most important for us is that the end consumer – that is, the recipient of the rogue robocall – is served by a participating carrier. That allows us to start our tracing process and begin to populate our database with valuable call signaling information.

The carriers to whom we have spoken express enthusiasm regarding participation. It's their customers that are suffering from the robocallers. These frustrated customers are dropping landline subscriptions "because all I get is robocalls." Intrusive wireless calls cause customers to ignore their mobile phone or worse, put it on "silent". Robocalls are devaluing the product these carriers sell.

While we will aggressively seek participation by the larger carriers, we welcome participation by all. And we are anxious to have participation by as many interexchange (transit) carriers as possible, as they are important links in the chain backwards from the called end-user to the robocaller. (In many cases, carriers listed above also have sizable interexchange traffic.)

As a general rule, the larger carriers have modern call signaling systems and real-time, searchable call databases that are compatible with our approach. Of course, many smaller carriers also do.

Applicable Laws and Regulations

There are already laws and regulations in place that prohibit the most annoying robocalls. Despite large penalties for violations ($10,000-$16,000 per violation payable to regulator, and $500-$1,500 to end-user), the laws are largely ignored because they are rarely enforced. And enforcement is minimal because it has been extremely difficult if not impossible – until now, with It's My Number.

The chart below attempts to summarize the existing rules. The Telemarketing Sales Rule (codified and enforced by the FTC) and the Telephone Consumer Protection Act (codified and enforced by the FCC) generally mirror each other. The Do-Not-Call Implementation Act established the Do-Not-Call list and is enforced by the FTC. The Truth-In-Caller-ID Act is enforced by the FCC and has been embellished with additional call signaling rules. All were designed to reduce end-user frustration and annoyance. If we could get compliance, we'd virtually eradicate the problem. We don't need Congress to pass new laws.

Rule	Exemptions	Law
Applying to Auto-Dialed Calls (including robocalls OR transfer to live agent)		
Not permitted to wireless numbers	No-charge calls from Wireless Service Provider; Noncommercial with prior oral or written consent; telemarketing with prior written consent; HIPAA	TSR & TCPA
Calls that fail to transfer to live agent within 2 seconds must deliver a prerecorded ID message when abandoning call that includes: opt-out number; interactive opt-out mechanism. Abandon rate cannot exceed 3%	Tax-Exempt Non-Profit; HIPAA	TSR & TCPA
Applying to Auto-Dialed Robocalls (delivering a pre-recorded message)		
No calls to residences	Non-Commercial; HIPAA; prior written consent; existing business relationship	TSR & TCPA
Must identify, at beginning of message, identity of entity making call; plus telephone number or address of entity; info must be valid, verifiable, and actionable	HIPAA	TSR & TCPA
Must offer interactive opt-out; if left on voicemail, must include toll-free opt-out number	HIPAA	TSR & TCPA
Applying to All Telephone Solicitations (telemarketing; auto-dialed or not)		
No calls to numbers on Do-Not-Call list	Prior express permission; established business relationship; tax-exempt non-profit	DNC
Calls must include proper Caller-ID		TSR & TCPA
Applying to All Calls		
Illegal to transmit misleading or inaccurate CID with intent to defraud, cause harm, or wrongfully obtain anything of value	Law Enforcement; Court-Ordered	Truth-in-CID

Those that have received annoying robocalls will recognize immediately that they are routinely non-compliant in multiple respects. With so many infractions, prosecution would be relatively straightforward – PROVIDED that the perpetrators can be identified.

Carrier Best Practices – the PSTN as a “Walled Garden”

Carriers are the guardians of the United States PSTN. Responsible Carriers make it their business to insure that the network operates reliably and efficiently, and that the traffic on the network is lawful. All traffic comes into the PSTN via a Carrier. Sometimes there are other “service providers” in front of the Ingress Carrier; for example, some VoIP providers aggregate traffic from many customers and then pass that traffic to a partner Carrier to put it on the PSTN. International traffic comes in legacy or VoIP format from an overseas provider and enters the US PSTN through a US Carrier. In these cases there is always a business arrangement (typically a contract) between the originating provider and the Carrier.

Carriers accepting "terminating traffic" generally dictate and enforce terms designed to protect their business interests and the integrity of the network. These terms can include (among many other items):

- Number of calls that can be active simultaneously
- Rate at which new calls can be initiated
- Signaling information required to allow proper rating and jurisdiction of calls
- Conformance to technical standards
- Prohibition against harassing or illegal calls
- Declaration that the Provider is responsible for calls placed by or on behalf of their customers
- Deposit or pre-payment to protect the Carrier from financial loss
- Carrier exclusion of liability when action is taken to enforce terms

Carriers are aware of specific issues with robocalling; they call it "dialer traffic." (Google that.) It can wreak havoc on their network due to:

- A high percentage of unanswered calls
- Short call durations
- Improper signaling content (invalid CallED or CallING number)

With respect to these parameters, many Carriers have limits on the traffic they will accept, and/or financial penalties for traffic that falls outside the limits.

When a robocalling violation comes to a Carrier's attention, most are enthusiastic about working with their customer to bring them into compliance or terminate their service. For example, "traffic aggregators" (that blend illegal robocalls into traditional traffic to evade detection and blocking by their Ingress Carrier) will find all of their business at risk when their Carrier presents them with robocalling complaints.

As enforcement heats up, robocallers will pop up in new places. We believe the FCC can encourage carriers to only accept dialer traffic from "trusted" sources that are verified to be making legal calls. If nothing else, carriers can "pace" traffic from unverified sources (limiting the number of calls they can place each second), and they can enforce validated CallING Number and Charge Number parameters unless the originator has demonstrated a need and made appropriate arrangements to provide numbers of their own. It's My Number can help by publishing Carrier Best Practices that tighten the net through which illegal robocalls might slip, while not impeding legal calls.

We know that an enormous number of robocalls are originated via overseas providers. Since these providers (and their customers) are beyond the jurisdiction of the US regulators, this situation deserves special attention. We suggest a focus on commercial arrangements to encourage compliance:

- It's My Number will track the number of robocall complaints traced to each (US) Ingress Carrier.
- A Carrier exceeding a specified threshold of complaints in any given month will be subject to an escalating FCC fine based on the number of complaints.
- We would expect Carriers to seek recourse from the offending customer (including service providers and foreign carriers that are the Ingress Carrier's customer), likely from deposits taken for this purpose.
- An Ingress Carrier that cannot recover the fine from its customer(s) would absorb the expense.
- An Ingress Carrier would be relieved of its fine obligation in any instance where It's My Number or a regulator collected actual penalties directly from the offending Customer.
- Carriers would have the opportunity to show that legal calls had been misclassified as illegal.

Fines would only apply when It’s My Number provides timely notification to the Carrier of the offending call (e.g., two days). This gives the Carrier an opportunity to stop the offenses quickly, avoiding ringing up huge numbers of illegal calls (which both annoy end-users and result in even larger fines). Carriers can ramp traffic for customers gradually, to avoid being suddenly swamped with illegal calls.

Operational Economics and Structure

It’s My Number could operate as a stand-alone government-sanctioned entity chartered to perform the functions outlined here. It is also possible that our solution could be implemented under the umbrella of some other third party, or within the FTC or FCC itself. We believe that we will be able to do it more quickly and efficiently than any other alternative, but are happy to debate that further.

Regardless of the structural details, this solution will be far more cost-effective, in terms of number of robocalls defeated per dollar expended, than any other. Funding for the effort could come from government sources and/or carriers. An incentive (success-based) approach could work.

Since this is a cooperative industry effort, we suggest that an It’s My Number Governing Board be established with representation from the carrier and regulatory community.

Privacy Considerations

Data regarding who called whom, and when, is confidential. Our exchange of information with carriers and any other partners will be covered under comprehensive written agreements that guarantee privacy protection. We will comply with the FTC and FCC privacy policies when we exchange data with those agencies.

We will not provide information back to individuals filing complaints (other than to say “Thanks” and recognize their contribution if and when it results in specific action against a robocaller). We want to make sure that nobody can “trick” us into revealing data inappropriately. Nobody will be able to file a “complaint” with us, and then have us tell them, “Oh, that wasn’t a robocaller that called you; it was your ex-wife calling from this address.”

If we obtain signaling data that carries an explicit privacy expectation (e.g., Calling Party Number marked “presentation restricted”), we will only use it in aggregated form (when multiple complaints are received regarding the same call source), and only when those calls are determined to be in violation of the rules, and then only revealing the number to the ingress carrier and the robocall originator. We believe that we won’t run afoul of CPNI rules, because we already have the call information from the called party, and we’re just looking for the “route” (which is not CPNI) – but we may need additional cover from the FCC so that carriers are comfortable exchanging the necessary data with us.

Carrier Feedback

As part of our research for this submission, we spoke to a number of carriers and carrier representatives. Below we present some of their feedback and our responses:

TECHNOLOGY SOLUTIONS AND WHACK-A-MOLE – Carriers make the point that a challenge with virtually any technology solution is that when the good guys put something in place, the bad guys inevitably find a way to work around it. We generally agree. If the solution is to have a pre-screening system that says “If you are not a robocaller, press 2 and your call will be connected” then the robocallers will have their recorded announcements send a “2”. If you get cleverer and choose a different digit each time, the robocallers will use speech detection and learn to press the right digit. If you use caller-ID to only allow the “good” numbers to get through, the robocallers will appropriate those numbers (airline, school, whatever) and use them.

Our “technical solution” is a little different. It really is a TRACKING and ENFORCEMENT tool. Once an illegal robocall is received (either at a honeypot number, or based on a complaint), the solution allows us to trace it back to the source. The technology doesn’t prevent robocalls per se; rather, it is a deterrent in that it allows us to be much more quick and efficient and cost-effective at policing and enforcing laws that are already in place.

We believe it will be very difficult for illegal robocallers to evade this. The nature of the PSTN is such that we WILL be able to trace at least SOME of their calls back to the perpetrators, or at least to their carrier. Illegal robocallers may try to hide behind others, passing their traffic through intermediate services that aren’t diligent in screening their customers, or carriers that are “on the fringe”. Certainly they will increasingly move offshore. That is why we need the FCC to put some teeth into holding carriers accountable for facilitating these illegal calls. We WILL be able to find these providers.

Another thing to keep in mind is that the scale of these violations is ENORMOUS. The illegal robocallers are placing millions and BILLIONS of calls. They are not doing this through some unsuspecting small business with a leaky PBX. They are paying money to somebody who is complicit, to some degree, in their scheme, because those co-conspirators are providing enormous amounts of capacity to let this happen.

One thing we should do (and this was pointed out by one of the carrier regulatory people that we spoke with) is make sure, as we move forward toward the “All-IP PSTN”, that we don’t make this problem even worse. One of the “good” things about today’s PSTN is that it is a somewhat “gated community” and only licensed carriers can put traffic on it. A mandate to allow “anybody with an internet connection” unfettered access to that network would certainly exacerbate the robocall problem and perhaps truly make it intractable. Of course, we can still make great use of the Internet PROTOCOL, but we need to be very prudent about the mechanisms and policies by which calls actually reach the telephone endpoints – at least those endpoints that have not opted-in to a less rigorously protected network.

NO MORE REGULATION – Carriers indicated that carriers generally are not in favor of more regulations, and certainly more liabilities, being thrust upon them. As a general rule, of course we agree. We don’t want any more rules and we don’t want any more taxes. However, across all aspects of our lives, it seems that the rules and the taxes keep coming. “Resistance is futile.”

We do think there is occasionally a place for prudent regulations. Have you never uttered, “There oughtta be a law…”? Telecommunications has turned into the Wild West, and while that brings plenty of innovation and benefits, it isn’t all good news and there are clearly some bad actors that need to be reined in.

We believe that carriers will be best served by being at the table as any new rules are crafted. The rules need not be punitive to those that are operating professionally and adhering to best practices. We understand that a few rogue calls might leak through, and that a company like AT&T or Verizon that is already processing billions of calls a day has more of a “needle in a haystack” problem detecting an illegal robocaller than does a tiny CLEC that puts extra facilities in place just so they can capture a few extra bucks from a dark-side customer that wants to make a few million “suspicious” calls. Our expectation of any new rules is that they would provide for ample warning and clear opportunity for the accused to mount an explanation or defense prior to levying of sanctions, and that carriers with “best practices” in place would earn some immunity.

ECONOMIC CONSIDERATIONS – A first reaction of carriers is they don’t want to be forced to spend money. With this solution, it is going to cost them money to link their internal signaling databases to the It’s My Number tracking system. The good news, and perhaps part of the novelty of our solution, is that we want to drive it to be as fully automated as possible. Essentially there’s a “nominal capital investment” up front to get the software systems in place to support this. But we’re sure that cost is a lot lower than putting new software into all the end-office and mobile switches that carriers have already deployed.

More importantly, there are going to be important cost BENEFITS when we get this problem corralled. We already know that robocalls cost carriers money in terms of network congestion, traffic engineering, trouble calls, and customer complaints, not to mention the manual tracing efforts where huge numbers of man-hours are expended on relatively small numbers of calls. Sometimes robocalling events result in a need to file formal outage reports because they’ve made it impossible for “real” traffic (including emergency traffic) to go through.

And at the highest level, illegal robocalls are DEVALUING the product that carriers provide. Remember that this is the MOST COMPLAINED ABOUT issue that the FTC receives, SWAMPING all the other categories COMBINED! If we could make a decent dent in the volume of these calls, it would restore some of the luster to telephone service.

Follow-Up

The robocall problem is indeed a challenge. Our solution has evolved extensively over the course of the Challenge period. We know it will require further refinement, not only in the initial deployment but also as the robocallers begin to react.

We are happy to dialogue with you further as you evaluate our proposal. We can provide more technical detail; we can share our thoughts on regulatory refinements that would be helpful; we can talk about operational aspects of the solution. If there are aspects of the problem that you believe we have overlooked, we’d like the opportunity to fill those gaps.

Contest Scoring

(i) Does it work? (50%)

- How successful is the proposed solution likely to be in blocking illegal robocalls? Will it block wanted calls? An ideal solution blocks all illegal robocalls and no calls that are legally permitted. (For example, automated calls by political parties, charities, and health care providers, as well as reverse 911 calls, are not illegal robocalls.)

  Our solution stops illegal robocalls at the source. We trace calls to their origin, and work with the perpetrator and the ingress carrier to stop the calls (or bring them into compliance, or turn them over for prosecution). We do not pursue legal robocalls.

  After a short time in operation, our solution will serve as a significant deterrent to anyone contemplating placing illegal robocalls. It is difficult to predict how effective we will be (and how bold the perpetrators will be). Our solution is very effective at finding and stopping those making huge volumes of calls; we will be less effective on those placing few calls. However, mass calling is the nature of illegal robocalling. We are confident that we will reduce illegal robocalls by at least 95%.

  Critically, this solution does not block any legal robocalls (including the airline calling to inform you of a schedule change, the school asking where your child is, and reverse 911). Other solutions that require a "white list" fail to recognize how intractable that would be to maintain.

- How many consumer phones can be protected? What types of phones? Mobile phones? Traditional wired lines? VoIP land lines? Proposals that will work for all phones will be more heavily weighted.

  Our solution protects all consumers, including fixed-line, mobile and VoIP.

- What evidence do you already have to support your idea? Running code? Experiments? Peer-reviewed publications?

  We have experience working with carriers on our own call tracing issues. We have a good understanding of end-to-end call flows and the data available within the carriers. We have engaged with selected carriers that have vetted this proposal and expressed enthusiasm.

- How easy might it be for robocallers to adapt and counter your scheme? How flexible is your scheme to adapt to new calling techniques? How have you validated these points? Remember that the real test of a security system is not whether or not you can break it; it's whether or not other people can.

  Our solution does not depend on the CallING Number provided by the robocallers; nor does it depend on some audio interaction ("Press 1 if you are not a robocaller" or "Prove that you are not a robocaller by responding with the sum of 2 and 6"). Robocallers can try to use increasingly obscure methods to enter the PSTN, but we will track them to their ingress carrier and hold that carrier responsible for their misdeeds. Even internationally-originated robocalls have to enter the US PSTN through a US carrier. Perpetrators will find that they can run, but they can't hide.

(ii) Is it easy to use? (25%)

- How difficult would it be for a consumer to learn to use your solution?

  Consumers are not required to take any action to benefit from this solution. We will encourage consumers to file complaints when they receive illegal robocalls (as they already do, in droves), but everyone will benefit from these good deeds (not just the complainants). Our web form and telephone response system will be thoughtful and user-friendly.

- How efficient would it be to use your solution, from a consumer's perspective?

  Our solution is extremely efficient. Consumers do not have to purchase any equipment or activate and program any telephone features. Those consumers electing to file complaints will find a simple, friendly web form (or telephone voice response system) that happily registers their call data.

- Are there mistakes consumers might make in using your solution, and how severe would they be?

  We will vet all the consumer complaints we receive (by using our crowd-sourcing and data correlation techniques). Complaints that are filed by consumers "accidentally" complaining about legal calls will generally fall to the bottom of our pursuit list. If we end up with numerous complaints about a particular robocaller that is in fact operating legally, we'll work with that robocaller and the regulators to address it (but won't interfere with the legal operation).

- How satisfying would it be to use your solution?

  We think all consumers will be delighted to see a dramatic reduction in illegal robocalling. We believe that those consumers that choose to file robocall complaints will take particular satisfaction that their contribution has made a difference. We intend to give feedback to consumers thanking them for their effort.

- Would your solution be accessible to people with disabilities?

  Yes. Our web-based complaint form will be designed with accessibility in mind. We will also accept complaints over the telephone for those without web access. And even those not participating in the complaint process will still benefit from the solution, which means anybody with a phone (disabled or not) will benefit.

  Also, since our solution does not require any special action on the part of legitimate callers ("Press 1 if you are not a robocaller"), it will not interfere with calls placed by those with disabilities.

(iii) Can it be rolled out? (25%)

- What has to be changed for your idea to work? Can it function in today's marketplace? (E.g., Does it require changes to all phone switches world-wide, and require active cooperation by all of the world's phone companies and VoIP gateways, or can it work with limited adoption?) Solutions that are deployable at once will be more heavily weighted, as will solutions that give immediate benefits with even small-scale deployment.

  Our solution does not require any changes to end-user equipment or telephone company switches, and it does not require any behavioral changes on the part of telephone network users.

  We depend on data that is generally already collected and internally available to most telecommunications carriers. Effort will be required to link this data to the It's My Number database and operational systems.

  Our system can be effective even if only a few carriers participate. Involvement of the larger carriers will have significant results thanks to our crowd-sourcing approach. The solution becomes even more iron-clad as the "long tail" of smaller carriers become involved.

- Is deployment economically realistic?

  Yes, this is a very cost-effective solution by virtually any metric. We believe we can effectively protect all the numbers on the Do-Not-Call list for a penny per year each.

- How rapidly can your idea be put into production?

  Our web site, voice response system, database and analytics all use off-the-shelf technology and are fairly straightforward and inexpensive. The long-lead item will be the time it takes to get fully automated systems enabled with participating carriers. We should be able to start testing using manual systems within 60 days, and be fully operational in 180 days.

Contestant Background

ZipDX LLC is a start-up provider of innovative information and conferencing services. ZipDX offers its services to business customers globally via the PSTN and over the Internet, and operates redundant data centers on the US East and West coasts. ZipDX works closely with large and small telecommunications carriers. ZipDX is a California Limited Liability Company headquartered in Silicon Valley with fewer than 10 employees and qualifies as a "Small Organization" under the Contest rules. See www.ZipDX.com.

David Frankel is the founder and CEO of ZipDX. He has worked in high performance computing, networking, and telecommunications for 40 years. He founded Jetstream Communications, a venture-backed voice-over-packet manufacturer, in 1995 and started ZipDX in 2007. He holds seven US patents related to these endeavors. He has participated in state and federal telecommunications regulatory efforts, including participation in an FCC panel on Intercarrier Compensation. He has a Bachelor's degree in Electrical Engineering from the University of Illinois.

dfrankel@zipdx.com 1-800-372-6535 16785 Magneson Loop
Los Gatos, CA 95032