Dear FTC:

The following is my submission on the "best way to stop robocalls", and pulls on both my own experience in anti-telemarketing-abuse and anti-spam activity and—more particularly—my personal experience in investigation of the "worst actors" and coordinating with the Kentucky Attorney-General's office to get some of the worse offenders shut down.

A little bit of prelude/backstory is necessary to discuss my particular solution. Kentucky has had a particularly stringent do-not-call since the early 2000s even in comparison with the FTC's do-not-call regulations. Specifically, rather than being a mere civil offense, violation of telemarketing laws is a Class D felony in Kentucky (resulting from 1 to 5 years imprisonment). The majority of the issues that the Kentucky A/G (and myself, as a private actor) have had in stopping the worst offenders has been the following:

- Much of the problem is both technical and regulatory--the major technical issue is that the majority of "bad actors" are now using SIP-based VoIP calling from "phish farms" overseas which may not even be located in a specific call center but may be "farmed out" to people's homes worldwide from a central location. (A good example of the latter is the "Telemarketing 1-2-3/Total Home Systems" phish-farm located out of Guadalajara, Mexico which uses SIP-based "softphone" VoIP to conduct illegal telemarketing to Americans (and other countries) and which typically uses a client PC located in a worker's home to call from.)
- Most illegal robocalling is conducted by "phish farms" which may or may not have a US actor at all, but whose primary operations do seem to be located overseas; sometimes US companies hire out, some are overseas, but usually there is some US presence if via the PBX used on the American end of a VoIP call center setup.
- An increasing trend is the rise of the "pink telco" (so named after "pink providers", a slang term used in the anti-UCE community for an ISP that explicitly hosts spamvertised sites and which explicitly is spam- and spammer-friendly) which explicitly solicits or hosts illegal telemarketing operations--most of these are VoIP providers with US offices, but often these groups have shell companies overseas. (One of the rare cases of an actual telco engaging in this is "Pacific Telecom" associated with 'bad actor' telemarketer Telephone Management Corporation; the name is chosen to be similar to the now-long-since-borged-by-AT&T Pacific Bell, and may be the successor of Asia Pacific Telecom which was the locus of similar phishing schemes to those linked to Pacific Telecom numbers.)
- Almost all telemarketing fraud including illegal robocalling is best described as "vishing"--phishing via VoIP--and illegal robocalling in particular is best described as “SIP spam", VoIP spamming (http://en.wikipedia.org/wiki/VoIP_spam) or "SPIT". The IETF recognised as early as 2008 that SIP-based VoIP is as vulnerable to spamming as email or other Internet protocols and that SPIT-spam would be a risk as SIP-based VoIP was popularised.

In other words, the problem with illegal robocalling is part of two larger problems:

- The general problem of telemarketing fraud shifting to SPIT as the major method of injecting illegal telemarketing calls into the public telephone network and a general lack of regulatory tools to deal with telemarketing fraud increasingly taking on characteristics of other types of Internet-based fraud.
- The fact that SPIT can be treated as a subset of the general issues of "spam" or UCE on the Internet that have existed since the days when non-academic, non-governmental ISPs were first permitted access (and particularly since 1995 or so).

The reality is that stopping illegal telemarketing operations will require both technical and regulatory fixes, and by necessity the target is more on stopping "SPIT" rather than a focus on illegal robocalling (the illegal robocalls are in fact a subset of the "SPIT" problem, and with one notable exception the solutions to both are identical with the technology presently available or even theoretically feasible in future)--this will require in particular strengthening the security of SIP VoIP and approaches that borrow not only from telco and the existing legal frameworks for fighting telemarketing fraud but also approaches that have seen success at mitigating UCE from the business environment. (Unfortunately, one of the strongest legal tools in fighting UCE--suing spammers--was removed with the passage of CAN-SPAM, but similar remedies still exist in the telco world.)

No system will be perfect, and--especially in the present regulatory climate of telephone solicitation where "opt-out" rather than "opt-in" is the model--it may be functionally impossible to eliminate all problematic SPIT (including robocalls) without either causing minimal collateral damage or allowing the occasional SPIT call through. The most promising strategy would integrate technical, regulatory, and even educational changes--there is not much that can be done on a consumer level, but much will require telco and FTC intervention (though consumers will be important for reporting violations).

That said, here are my suggestions, both technical and regulatory, in mitigating SPITting (and by extension, the illegal robocall problem):

1) Require--by federal law--that companies be prohibited from forging CID save to a registered, routable, inbound call center (this will not interfere with companies that legitimately use overseas call centers, as they will be willing to register this info with the FTC) and if CID info does not match either what is listed in ANI records (or ANI+CPN records in the case of SIP-based VoIP), international call routing information, OR a registered inbound number (see 2 below) then that call is NOT to be routed.

This should not substantially interfere with legitimate telemarketing in the US nor would it substantially interfere with exempt telephone solicitation calls (charities, political calls, etc.)--if anything, this is a strengthening of a pre-existing rule prohibiting the forgery of CID and facilities to cross-check CID info transmitted and telephone routing information already exist in telcos. In addition, most robocalling is from overseas SPIT and the vast majority of lawful telephone solicitation operations in the US operate from US-based call centers.

2) In conjunction with this, mandate that ALL companies operating an outbound call center to the US from overseas have an established US office of operations and have on file a registered, routable, inbound call center number dialable from the US. The registry should include not only the company

operating the international call center but all inbound and outbound call center numbers and locations including jurisdictions. Any inbound call center number not originating from a company not on this list is

not to be routed by international call centers based in the US.

Again, this should not affect most lawful telemarketing operations, and facilities already exist for telcos to check this info--there is already an existing model for these operations in that 35 states require pre-registration for charities to conduct legal solicitation, and what would be created here is essentially a whitelist of known "good actors". Many states, including Kentucky, also require registration of telemarketers and these databases could be integrated with a federal list (in the case of Kentucky, also requiring payment of a yearly bond to the Attorney-General's office).

The only major change would be requiring telcos to drop connections from unregistered call centers and requiring a US base of operations--and even then it would only require registration for those companies that have outsourced technical support or maintain "rollover" call centers overseas, and should cause minimal disruption to operations.

3) One technical angle that could substantially reduce illegal robocalling are restrictions (including telcos being ordered to drop routing to) on the use of so-called "leaky PBX's" to disguise international call centers. (A leaky PBX routes calls from PBX A--located in an overseas call center--to PBX B (located in the US) via satellite or (far more frequently nowadays) dedicated lines or VoIP; without additional tracing, the call superficially appears to be from PBX B although originating in PBX A, which has resulted in issues tracing down known "bad actors" in strong-DNC-law states.) One known solution could be the FTC beginning a registry of known or suspected "leaky PBXs" and PBX operators, many of which may be linked to "pink telcos".

This is one of the few areas where a combination of telco, FTC, and consumer action would be useful--customers can report violative calls to their state A/G or the FTC, the FTC can use info to note which companies may be using "leaky PBXs", and the FTC could coordinate with the FCC to drop routing to known sources of abuse. This is functionally how blocklists of known open relays and TOR relays work with Internet sites and providers that block proxy connections due to abuse (Wikipedia uses proxy checkers and blocks known proxies and TOR relays to prevent abuse, and the same approach is used with several Internet Relay Chat host sites). We're basically establishing a "leaky PBX list" to use in conjunction with some blacklisting and Bayesian "spammishness" tests as will be noted below.

There may be SOME collateral damage, but this is not likely as most legitimate companies that would be using "leaky PBXs" are or have been transitioning to VoIP (usually SIP).

4) In the case of SIP-based VoIP (where most of the issue is coming from), one could conceivably mandate that telcos implement the suggestions in RFC 4474 (in its entirety at http://tools.ietf.org/html/draft-ietf-sip-identity-06) and RFC 5039 (http://tools.ietf.org/html/draft-ietf-SPIT-spam-05) which establishes a cryptographic "identity chain of custody" similar to ANI use for NANP number routing (and tracing by law enforcement). The suggestions in RFC 4474 in particular would largely mitigate any advantage for CID spoofing over VoIP and would make "spitting" considerably more

difficult and make it much easier to trace telemarketing fraud using "spitting" as the method of transmission.

RFC 4474 in particular proposes two additional headers in SIP header fields ("Identity" and "Identity-info"), whilst RFC 5039 explicitly discusses the authentication and identity issue in the first working paper devoted to the problem of SPIT (which was predicted to become a severe problem as even at this point SIP calls were cheaper than standard telephone calls) and discusses not only authentication measures but notes that the traditional "blacklist" approach is likely to be unusable for SIP-based spam as it is for email. (As practically all SPIT-related robocalls feature forged CID, we're already seeing a similar issue as occurs with forged email addresses and headers in more conventional spam.)

RFC 5039, in my opinion, is a prerequisite for anyone seriously wishing to study the problem of SPIT, as it also discusses other approaches that have been used for mitigation of other forms of Internet spam (including trusted user networks, Turing-testing, the use of captcha-like mechanisms, and even the use of escrow systems) and their suitability for dealing with SPIT. Even in this white-paper, it's explicitly acknowledged that a full system of mitigation will require legal frameworks (for penalising those spammers that get through) and trust frameworks as well as technical solutions (one segment, 3.13, even explicitly calls for a trusted list of SIP providers--similar to my proposal in 2) above).

The most novel approach noted in RFC 5039 (in section 4.1 and section 4.2) involves signature-based authentication of a manner similar to that used by PGP-signed email and message-board messages (and S/MIME and OpenPGP are explicitly proposed); section 5 of RFC 5039 explicitly notes that pretty much ANY mitigation strategy for SPIT will ultimately rely on a reliable method to authenticate identity for SIP messages (and, as noted in 1) and 2) above, to drop un-authenticable messages).

One of the difficulties that have presented themselves (both in the case of tracing SPIT-related telemarketing fraud and in law enforcement cases involving other forms of SIP-based telephony fraud and abuse) is that--whilst technical standards do exist for authentication of the source of a SIP call to its home ISP--very few SIP providers have used this in practice; as these are published IETF standards and almost all routing tools for SIP-based telephony provide for the use of these standards, it's a simple matter of requiring SOME method of authentication before these calls can be routed on the PSTN. Most business-class SIP tools will have this capacity built in, and consumer-level SIP can have "softphones" upgraded easily.

5) A number of other propsals have been published re increasing VoIP security and specifically aimed at stopping SPIT (http://www.cs.columbia.edu/~angelos/Papers/2011/cst.pdf), most of these taking explicit direction from approaches used to prevent UCE and other forms of unsolicited advertising on the Internet (basically treating "SPIT" as a subset of the general problem with Internet spamming). One approach that is in testing is SPIDER, which ranks callers on "trustworthiness" similarly to how the program SpamAssassin uses Bayesian filtering to detect how "spammy" a message is; the list of published papers in regards to the SPIDER project will be useful (http://www.projectspider.org/published.html) in research; Y. Rebahi, S. Dritsas, T. Golubenco, B. Pannier, and J. F. Juell, A Conceptual Architecture for SPIT Mitigation in SIP Handbook: Services,

Technologies, and Security of Session Initiation Protocol, S. A. Ahson and M.Ilyas, Eds., CRCPress, Inc., 2009, ch. 23, pp. 563–582 is a full published description. Other approaches in this vein include Voice Spam Detector (R. Dantu and P. Kolan, Detecting Spam in VoIP Networks, in Proceedings of the USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI), pp. 31–37, July 2005), SEAL (J. Seedorf, N. d'Heureuse, S. Niccolini, and T. Ewald, VoIP SEAL: A Research Prototype for Protecting Voice-over-IP Networks and Users, in Konferenzband der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft fur Informatik e.V.(GI), A. Alkassar and J. Siekmann, Eds., 2008) and (explicitly basing themselves on PageRank, a system for ranking pages used by Google that contains features designed to mitigate "SEO Gaming" and types of keyword spam) SymRank (H. K. Bokharaei, A. Sahraei, Y. Ganjali, R. Keralapura, and A. Nucci, You can SPIT, but you can't hide: Spammer identification in telephony networks, 2011 Proceedings IEEE INFOCOM, pp. 41–45, 2011).

Almost all of these are explicitly based on models very similar to Bayesian filtering of email as used by ISPs; almost all of these also have the same upsides and downsides as with UCE filtering. Basically, they can be useful for catching SPIT that manages to make it through a blacklist, and (in conjunction with consumer reporting to the FTC) can be used to compile a blacklist, but (depending on sensitivity) can result in false negatives or false positives. (SpamAssassin, an existing UCE filter similar to SPIDER, can have its sensitivity adjusted per site needs.)

In addition, whilst all of these are proof-of-concept, almost all testing so far has been on the German PSTN and for business use, not on a consumer level and not on the NANP PSTN (which uses different signaling techniques). In my opinion, these would be best used on a telco or business level, not at the consumer level (much as Bayesian filtering systems are implemented primarily at the ISP level, not at the end-customer level). These DO have the advantage of being one of the few approaches really implementable at a business PBX level, however.

6) A second line of defense that may show particular promise in stopping robocalling in particular is (in conjunction with a known whitelist of exempt users) the use of voice fingerprinting to drop a call. Probably the farthest-along development is with VIAT (http://viat.fh-koeln.de/) at Cologne University, but other approaches have been proposed (documented in D. Lentzen, G. Grutzek, H. Knospe, and C. Porschmann, Content-based Detection and Prevention of Spam over IP Telephony - System Design, Prototype and First Results, IEEE International Communications Conference (ICC) 2011 and Y. Rebahi, S. Ehlert, and A. Bergmann, A SPIT detection mechanism based on audio analysis, in Proceedings of 4th International Mobile Multimedia Communications Conference MobiMedia 2008: July 7-8, 2008, Oulu, Finland. ICST; ACM, 2008 respectively--Y Rebahi in particular has worked extensively on mitigation of SPIT).

Again, though, this is only the barest proof-of-concept at the moment and has only been tested on European telephone networks, and would be more useful in comprising a trustworthiness base--basically another form of Bayesian filtering, though one which may be particularly useful in dropping robocalls (versus other forms of SPIT).

7) A related technical-regulatory angle to 3) is to record which particular companies are providing VoIP/dedicated line/satellite service to "leaky PBX's" as these tend to be either front companies of illegal telemarketing operations or may be operating as small-time "pink telcos" and to allow regulatory action against companies known to provide services to illegal telemarketers. (This is probably the model under which TMC--the suspected perpetrator of the "Rachel at Card Member Services" calls--may be operating.)

8) Likewise, a regulatory angle may well involve an FTC registry (possibly coordinated with the FCC) of known VoIP providers with an entry or exit point for VoIP connections in the US--this would, again, make it potentially easier to track which VoIP providers are acting as "pink telcos" and allow appropriate enforcement action.

9) Change the present laws on telemarketing to no longer have violations merely be a civil offense, but to raise the status of violations of telemarketing law to felony violation of law. (This is one of the biggies--largely because it gives the FTC a powerful tool for getting at the worst of the phish farms; being able to extradite people. This is also why a number of states actually have violations of telemarketing law as felonies--mere fines weren't cutting it, and they needed the tool of felony conviction to enable international extradition of 'bad actors'.)

10) Change the present laws on telemarketing to not only allow going after the telemarketing companies acting as "bad actors", but also "pink telcos" (as accessories to violations of telemarketing law and/or accessory to a felony--if DNC violation is raised to a felony, the possibility of seizure of assets under RICO comes into play) and the companies hiring the "pink telcos" and telemarketing companies. (Yes, I'll say it--perhaps it's time to unleash civil forfeiture laws and RICO on the companies in question, because they keep setting up shells even as the FTC knocks them down. The "Rachel from Card Member Services" scam has gone on from TMC-associated shell companies since at least 1999 and the FTC has not been able to knock it out entirely; if they could go after TMC itself, that MIGHT nuke the operation.)

11) One underappreciated private action that can be taken against telemarketers--and, other than soliciting info to the FTC, really the only one that's feasible for non-business consumers--is lawsuits under the TCPA ($500 per offense, $1500 per willful offense) but the small claims limits in some states make TCPA lawsuits difficult (in Kentucky, for instance, small claims is limited to $1500 and it is not uncommon for states to have limits of $3000-5000 for small claims court). The FTC could encourage states to increase the monetary limits for lawsuits under small claims court.

Yes, this is even a relevant solution for SPIT spam--until the passage of CAN-SPAM, many anti-spam activists were having success in the courts in shutting down spammers and "pink providers", and it's generally been through the courts where the worst offenders have finally been shut down. Sanford Wallace, who was singlehandedly responsible for passage of the anti-junk-fax provisions in the TCPA as well as California's anti-spam laws, finally ended up in prison after a 20-year history of near-sociopathic behaviour in spamming just about every way he could--it took a lawsuit from Facebook to finally shut him down, but he'd been driven off other forms of spamming before by successful lawsuits resulting in millions of dollars in damages.

Arguably, there may have been a recent case of SPIT robocalling that has been shut down by the mere threat of a class-action lawsuit (the "Celebration Cruise Line" phish, which purported falsely to be a pro-Republican political survey and was a resurrection of a similar "free cruise" phish that was linked to predecessor company Imperial Majesty and targeted British as well as US telephone customers; after the announcement of a class-action lawsuit against the perpetrators this particular phish seems to have shut down) and it may be that that giving customers better legal tools may be a surprisingly large portion of the solution.

12) Similarly to 1) and 2) above, refuse to route calls from an international outbound call center to cell phones, as this is already illegal; consider any attempt to call a cell phone a prima facie violation of telemarketing laws. (In fact, cell phones--like fax machines--are legally under an "opt-in only" model; as more Americans go to cell phones for their primary phone service, violations have become more common.)

13) The FTC should begin the compilation of a "Bad Actors List" (not saying it doesn't already, but the FTC mechanism could use some help) including not only being able to submit calls but known companies known to be "bad actors". (Private investigations by people on anti-telemarketing forums have found, among other things, that a "Free Home Security System" phishing scam and the "Rachel Phish" are both related to TMC of Portland, Oregon and likely shell company Pacific Telecom.)

This is one of those areas where private consumers are most likely to be helpful, as an aside; one way to encourage compilation is to make it easier for customers to conduct call tracing (allow call trace without charge--some companies charge as much as $5.00 per trace) and specifically allow the FTC to be considered law enforcement in cases of call traces related to telemarketing fraud.

14) Consider ANY forgery of CID by a party not registered with the FTC as a prima facie violation of telemarketing laws (this is already illegal but needs much more teeth) and instruct telcos not to route the call. (Capability already exists with telcos, and again would have little to no real effect on legitimate telephone solicitation or legitimate (inbound) offshore call centers.)

15) Probably one of the largest impediments is that a number of VoIP "pink telcos" offer anonymous equivalents of "bulletproof hosting"--going after the telcos (7) is helpful in this, as would a similar regulation to that concerning USPS post office boxes--that any VoIP connection used for business must have an owner on record which must be provided upon request to law enforcement for said VoIP operator to operate legally in the US. (This would not affect private individuals or legitimate businesses--but it would make it much easier to trace "phish farms" operating via VoIP-based PBXs.)

Honestly, this is probably what it's going to take to stop illegal telemarketing without going to a full-on "opt-in" model (such as what was in place for email in California until CAN-SPAM, and what is in place nowadays re junk calls to fax machines and cell phones). Even the RFCs on this issue acknowledge a multipronged approach including technical, regulatory, and educational fixes will be necessary--and frankly the problem of SIP spamming may ultimately be as difficult as email spamming to fully mitigate, but telephony does have the advantage of a limited number of ingress and egress points usable by an abusive SPITter and—with a multipronged approach, having learned lessons from dealing with other forms of Internet spam—hopefully the “War on SPIT” can have better results.

Respectfully,

P. Bailey-Stine

Private individual and anti-spam activist