Spam Flagging and Call Blocking and Its Impact on Survey Research

AAPOR Ad Hoc Committee

David Dutwin, SSRS (Chair)

Micheline Blum, Baruch College

Kennon Copeland, NORC

Howard Fienberg, Insights Association

Chris Jackson, IPSOS

Eric Jodts, Westat

Olga Koly, U.S. Census Bureau

David Malarek, Marketing Systems Group

Gerry Holzbaur, Marketing Systems Group

Stephanie Marken, Gallup

Joe Matuzak, University of Michigan

Carol Pierannunzi, Centers for Disease Control

Jamie Ridenhour, RTI International

David Sheppard, U.S. Census Bureau

Michele Ernst Staehli, Fors

Lynn Stalone, HR Research

John Thompson, COPAFS

Sanjay Vrudhula, Recon MR

Introduction

Recently, cellular telephone operating systems, cellular carriers, and third party app builders have begun to provide features for cell phone owners that block incoming telephone numbers or warn users that incoming numbers are from potential scammers, fraudsters, or spammers. The algorithms used to flag numbers as fraud, spam, or otherwise warranting blockage vary, but in whatever form, generally utilize a threshold on the volume of calls originating from a specific number, review logs of complaints, or both. As a result, many of these features are blind to whether, in truth, the originating caller is indeed a telemarketer or otherwise attempting to spam or defraud the caller. We refer to these features collectively as "blockers."

While the goal of reducing robocalling and telemarketing on cellphones is laudable, the rise of spam flags and automatic blockers is a direct threat to legitimate survey research organizations. Many survey research organizations have reported to this committee that their phone numbers have been flagged by these blockers. It seems likely flagged numbers will experience lower response rates and lower productivity metrics, driving up costs and potentially increasing nonresponse bias.

The goal of this report is to provide all relevant information on the issue of cellular telephone flagging and blocking to inform the AAPOR membership of the full scope of the issue. As this report is published, this committee and AAPOR Executive Council are considering recommendations for potential actions by AAPOR to this issue.

The Development of Spam Blocking Software and Apps

There are three principal sources of blocking and spamming: operating system providers such as Apple (iOS) and Google (Android), cellular telephone companies such as AT&T and Verizon, and 3rd party apps such as Truecaller. Third party apps began to appear in 2013, after the Federal Trade Commission (FTC) announced its first FTC Robocall Challenge, offering a prize of $50,000 and an FTC Technology Achievement Award to the developer creating the best tool to deter robocalling. In April, it split the prize between two approaches, one of which was Nomorobo, which quickly became available, and as of this writing claims to have stopped almost half a billion robocalls.

Since that initial contest, the FTC has continued to host similar contests with differing approaches. The 2015 winner was another app that is now available for download, "Robokiller" to engage spam and robocallers and waste their time while gathering an "audio fingerprint" of scammers voices in order to block them.

The FTC now makes all consumer complaint data about robocalls available to developers and to the public via its website. Because of caller ID spoofing[1], the reported phone number and caller names may

[1] The illegal use of an owned phone number for caller identification purposes without the owner's consent, see appendix for more information

not be accurate, something the agency takes pains to point out. Because of caller ID spoofing, the reported phone number and caller names may not be accurate. Further, differing approaches to detection can lead to differing results on the same number. Both of these issues are of great concern for researchers as they increase the challenge of reaching intended respondents, associate our calls with potential illegal activity, and result in a potential respondent experience that could vary without our knowledge.

Third Party Applications

Third party applications for smartphones are available from dozens of providers across the various mobile platforms. Many of these apps are free or cost only a few dollars. These applications typically use proprietary methods and algorithms to block calls or display warnings on the smartphone during incoming calls. Typical methods for determining which calls to block or warn rely on call volume and/or online ratings and complaints for the originating number. Some applications allow the user to designate certain numbers for blocking or allowing. In addition, some applications upload the user's contact list to be allowed. Others allow the user to designate the type of calls blocked. For example, many apps allow one to block all numbers not in a user's contact list and/or social media connections. Apps can also block based on geographies and/or area codes. Some applications offer additional features. For example:

- reverse call look-up, providing data on incoming numbers (e.g., online reviews or search engine results) - some offer a delayed ring allowing you to evaluate the information before deciding to answer or block
- blocking of unwanted texts (note: Android policy does not allow third party apps to block text messages but Apple does)
- logging the number of calls received from a specific phone number
- silent ringers for unknown callers

Some applications offer choices about how to respond to an incoming call. For example, users can send a prewritten text message to the caller or file a complaint with the FTC. Third party apps can produce a number of outcomes for the receiver as well as the caller. In the extreme, apps can fully block calls, where phones will not ring or notify the user of a blocked call. Some will allow for calls to transfer directly to voicemail without ringing, pick up and hang up automatically, or just mute the ringer. Other apps notify the user of blocked calls, allowing them to review, sort and classify numbers after the fact as legitimate or not. Still others will allow incoming calls, but provide warning messages that a given number is spam, scam, a survey, or other flags. These warnings may or may not include qualifiers such as "possible," "likely," or "suspected."

There are numerous third party applications currently available including Hiya, NoMoRobo, Safest Call Blocker, Mr. Number, Call Control, Extreme Call Blocker, Sync.me, Robokiller, TrueCaller, and Callblocker. The end of the report gives a more complete list.

One example of a third party application that can be used on both Android and Apple devices as a blocker is Hiya. Hiya has partnered with Samsung, AT&T, T-Mobile, and others to include Hiya's services on the companies' devices. They have both Hiya Cloud which operates at the network level and the Hiya Client, which is the third party application a user would download from the App Store or Google Play. Hiya is available in many different countries and has been in operation since 2016. It provides more options for what a call can be flagged as than just spam or scam. The user can tell Hiya whether a call was general spam, not spam, telemarketer, IRS scam, debt collector, scam or fraud, political, survey, or nonprofit. Hiya is in part powered by its users in that it uploads a user's contacts to its database for the purpose of identifying likely not-spam calls – an end user is unlikely to save a spam call to their phone book. Below we give an example of what a possible spam call may look like on an Android device when flagged by Hiya. The identification in the purple box is how Verizon identified the caller whereas the orange box is Hiya's overlay of how it identified the caller.

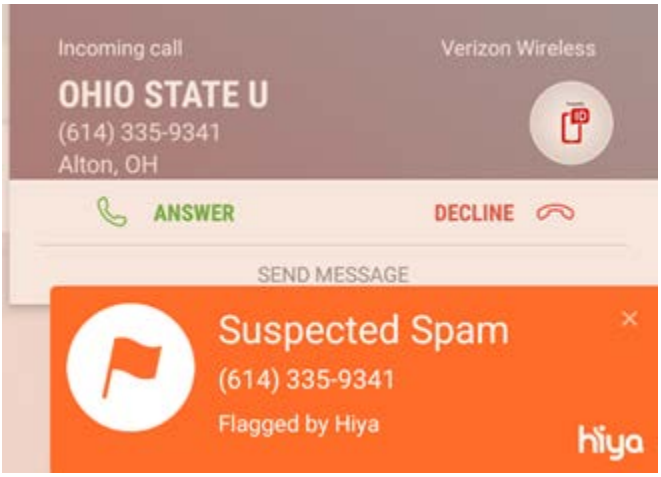


Image 1: Hiya Incoming Call Example

Hiya also makes the reports of other Hiya users available inside the app so the user can see how what others have said about the caller:

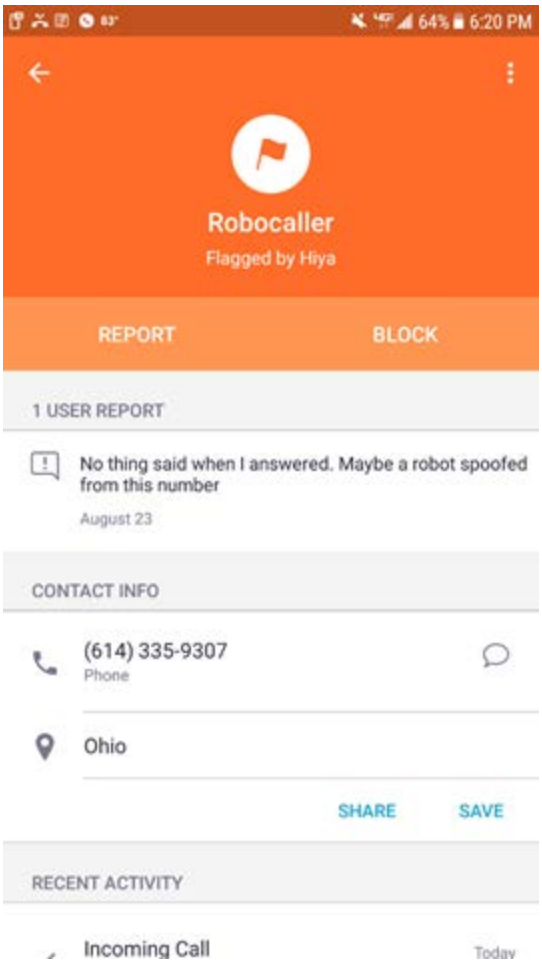


Image 2: Hiya Incoming Call Example with User Report

While testing out the Hiya application, a cellular number of one of the authors was selected by the National Immunization Survey (NIS). According to the Hiya app some users reported calls from the NIS number as spam, others reported it correctly as a CDC survey. The CDC website verified that this was a legitimate NIS call[2] and we reported to Hiya that the designation should be 'survey' as shown below:

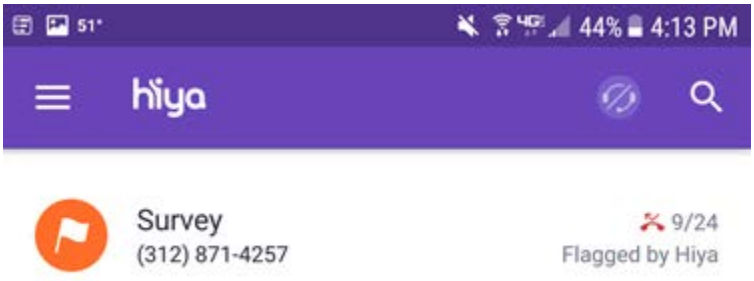
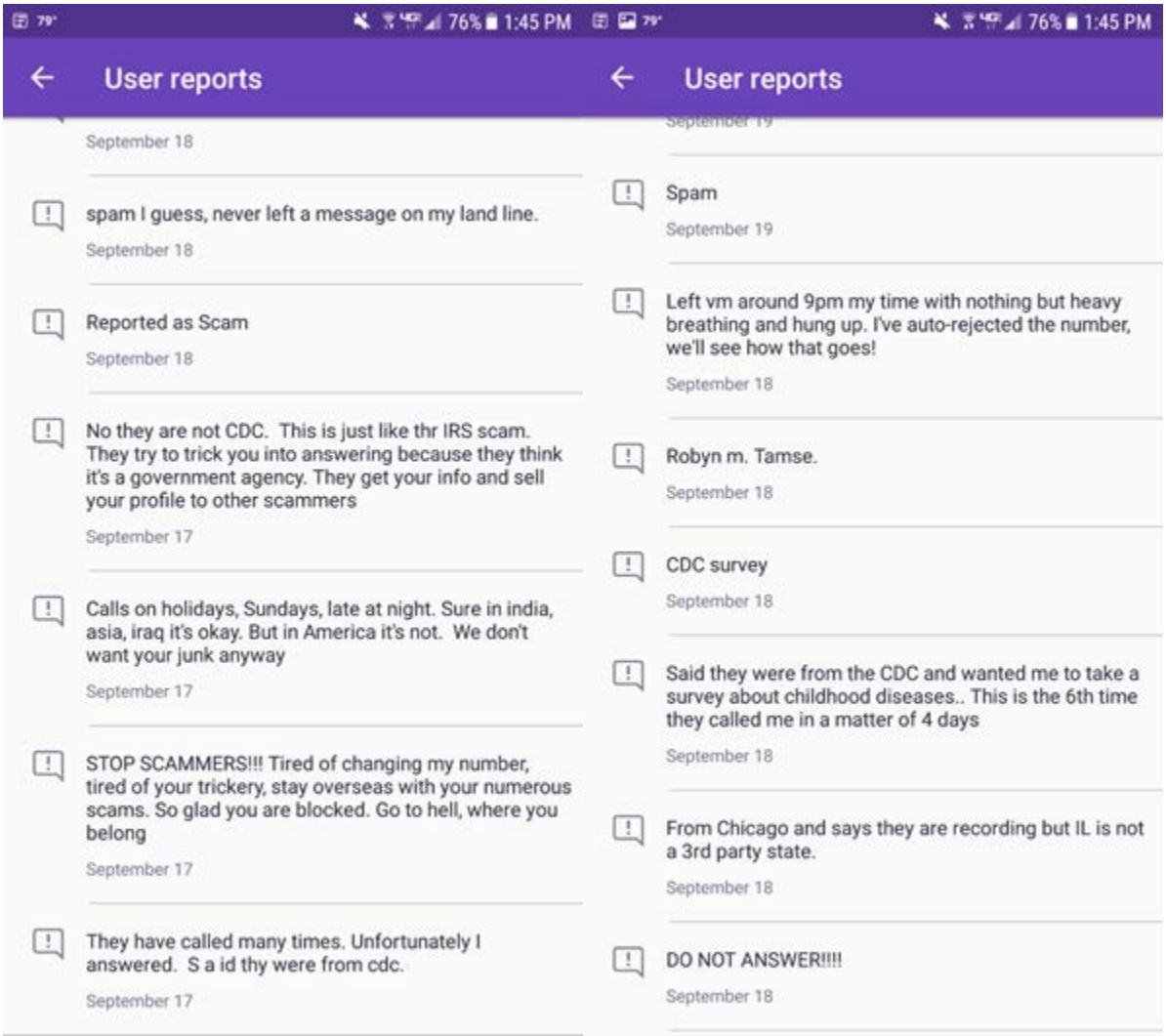
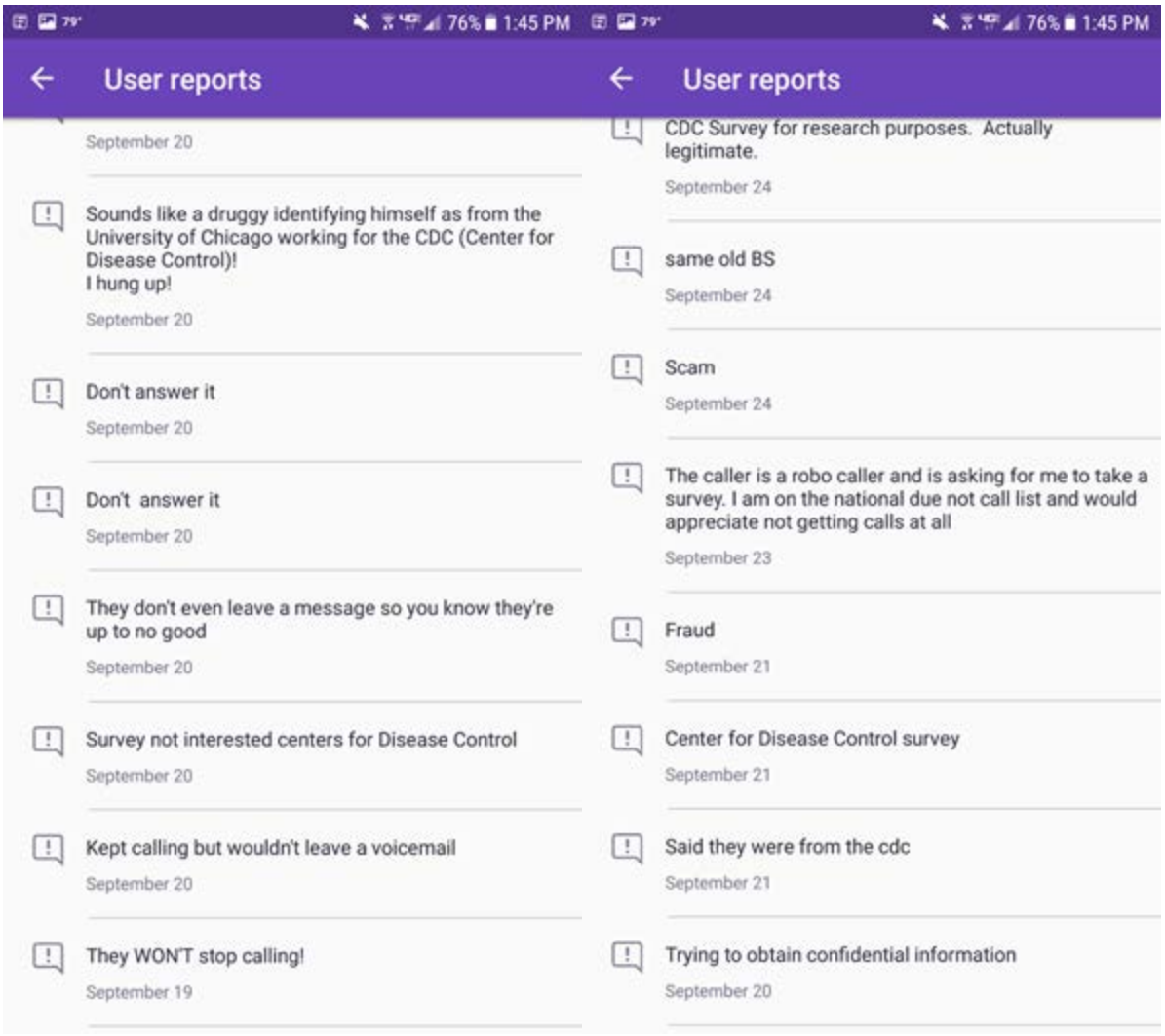


Image 3: Hiya Incoming Call With Survey Flag

[2] https://www.cdc.gov/vaccines/imz-managers/nis/participant/index.html

For the average cell phone user who is likely less familiar with survey research then a co-author of this report, the reports from various Hiya users in the app about this caller could be a deterrent to answering a future call from this number or calling it back to participate in the survey (examples below).





Images 4 and 5: Hiya Example User Reports

Cellular Telephone Carriers

Similar to 3rd party applications, cellular telephone companies can block suspect calls. For example, T-Mobile now offers a service called "Scam ID." T-Mobile will compare the number to a database of known numbers used by scammers and, if they find a match, the caller ID will display as "Scam Likely." In addition, T-Mobile will allow subscribers to block all such calls from ever showing up on their cell phone. However, customers will need to actively opt in to this blocking service, as T-Mobile recognizes that they may inadvertently block legitimate calls. AT&T offers a similar service called "Call Protect" that block robocalls at the network level and alerts customers to suspicious calls, but also comes with a companion app for iOS and Android that provides additional call blocking and/or categorization features. Verizon's service is called "Caller Name ID" and provides alerts on incoming spam calls and allows users to report or block calls. These services are currently only offered to customers of the respective carrier. Most are

free to subscribers, while Verizon charges a monthly fee for its service. Many of these carriers also offer similar products for landline phones either through hardware add-ons or partnerships with services like Nomorobo.

Operating System Providers

The latest players to enter the game of spamming notifications are the operating system providers. Google and their Android unit are the largest ecosystem for smartphones in the world today, accounting for over 2 billion units worldwide by some estimates. Globally, Android-based smartphones make up the significant majority of sales, estimated at over 80% of the market share in 2016[3]. In the United States, there is one Android system phone for every three citizens[4].

The Android system functions as an operating system for smartphones governing the overall function and user interface. The current version as of this publication is "8.0 Oreo" released in July 2017.

Google allows Android phone users to install third-party software to their devices. The vast majority of these come through the Google "Play" Store which provides over 1 million applications for sale or free download. Among these are hundreds of different call blocking and spam blocking apps.

In addition to allowing call blocking apps, Google provides a spam block service with the core operating system. The Android system provides two different levels of call screening to users.

The first essentially blocks calls from any and all phone numbers not in the user's digital "phone book" contained either in the device or the Google cloud. The second allows users to log phone numbers from received calls as "spam" and they are blocked from further contacts. Additionally, the system scans the "Google My Business" listing for information to display as part of the caller ID screen.

Beyond these features, which must be set by the end user, the default phone application in Android operating systems automatically provides spam warning for any incoming calls it deems as potential spam. This feature started rolling out in July of 2016. Calls are flagged as potential spam based on the volume of outbound calls from a particular telephone number and by cross-referencing available blacklists. Rather than the default blue screen for an inbound call, incoming calls will show on a red screen with language such as "suspected spam" or "possible scam." In some instances, users can swipe down to confirm that a number is indeed spam. Even if the call is ignored, the call log in the phone app will list the call as potential spam and provide users to flag calls from that number as spam.

[3] http://www.gartner.com/newsroom/id/3609817

[4] https://www.statista.com/statistics/232786/forecast-of-andrioid-users-in-the-us/

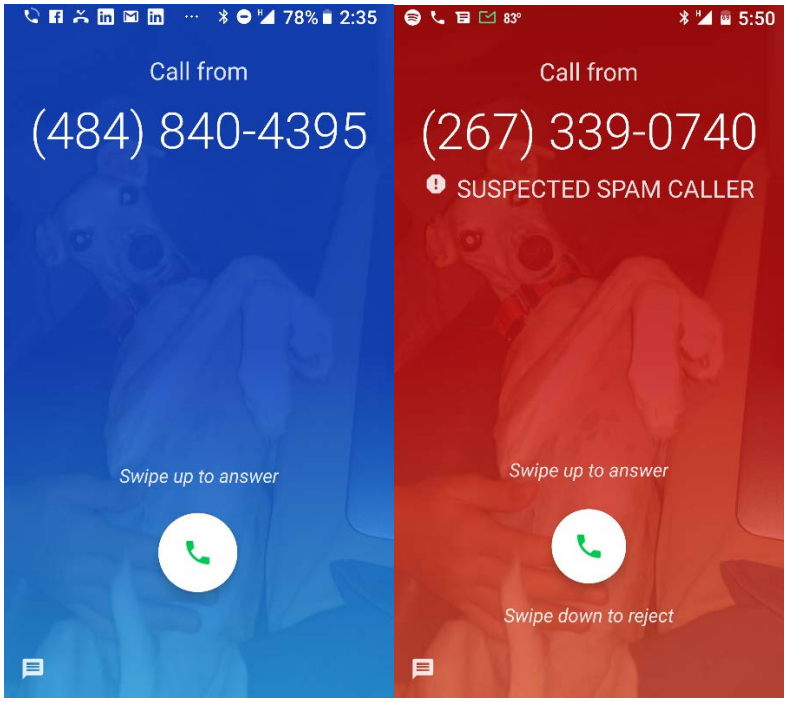


Image 6 and 7: Android Incoming Calls: Normal Versus with Spam Warning

If a user defines a telephone number as spam, they will no longer be notified of calls from that number and it will be permanently blocked on that phone. Google then utilizes that input from the end user to confirm or deny that a call is spam and use that information for calls to other users.

Apple developed such features later than Google, only recently rolling out spam and blocking features. With the release of iOS 10 in September 2016[5] Apple introduced CallKit which allows for third party applications to work with the Phone application to check numbers for likely spam or scam calls. Apple allows for more than one of these applications to be installed and for the user to specify the order in which the applications are used. As of October 2017 the support information[6] available on Apple's website for blocking spam calls only mentions the installation of third party applications and does not indicate whether Apple is developing its own capability in this arena. We have reached out to Apple but have not received additional information at this time.

Impact on Survey Research

The emergence of blockers has the potential to reduce the effectiveness of telephone surveys. While the use of such apps may decrease productivity, increase costs, and reduce telephone survey response rates, and potentially to a significant degree, perhaps more concerning is the explicit linkage of scientific

[5] https://en.wikipedia.org/wiki/IOS_10
[6] https://support.apple.com/en-us/HT207099

research organizations with the growing number of organizations that use deceptive and unethical practices to harass respondents.

The growing availability of spam warning and call blocking apps is due in a large part to the growing number of telemarketing calls to cellular telephones. Cell phone owners are becoming increasingly frustrated by such practices, thereby creating a demand for apps that will allow users to avoid such calls. The methodology underlying such apps will often not distinguish legitimate survey research calls from telemarketing. When this situation occurs, potential respondents who have an app will be alerted that a survey research call is potential spam, and in most cases will avoid the call.

Many legitimate survey research organizations include some type of identification associated with the call number(s) they use to conduct their telephone surveys. When such scientific surveys are lumped together with telemarketers, it increases doubts about the legitimacy of the organizations conducting the research. This can easily become a serious problem, particularly when social media is used as a forum to disparage the survey organizations.

In addition, potential research sponsors may grow concerned that spam flagging will result in telephone survey research that will have response rates too low to produce acceptable results.

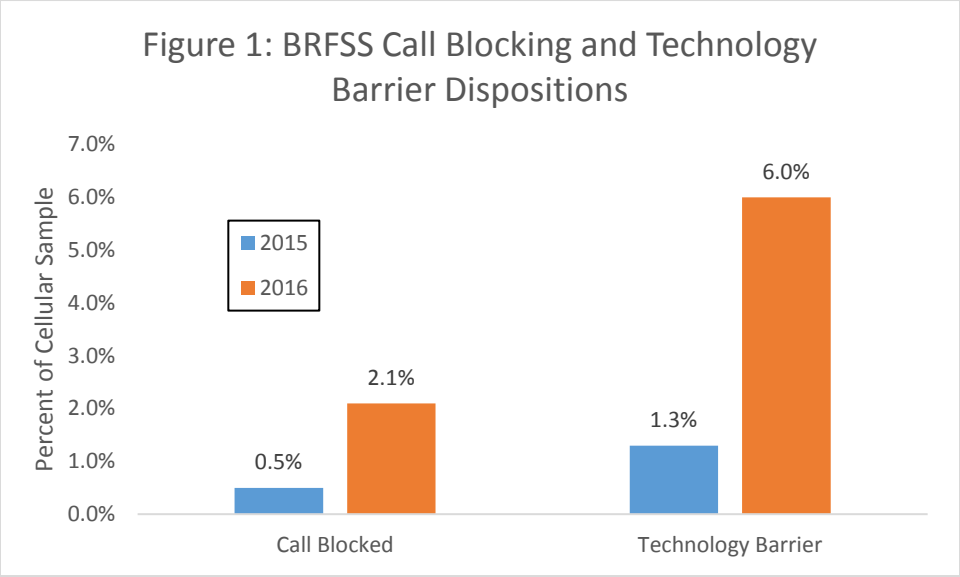
Assessing the Impact on Response

Overall, it is difficult to ascertain the impact of screening/blocking apps on cell phone sample calling distributions. In many instances, calls screened by apps would be coded as no answer or as sent to voicemail by potential respondents. The observation of changes in the proportions of dispositions from one year to the next could be due to a variety of causes, and would not necessarily be a result of widespread use of screening apps within cell phone samples. It is also unclear what the person placing the call would hear on the line when a call is flagged as spam and blocked from ringing.

The Behavioral Risk Factor Surveillance System (BRFSS) provides one case study. The BRFSS is a large scale, state-based system of health surveys conducted by state health departments with the assistance of the Centers for Disease Control and Prevention (CDC). Each state designs a dual frame sample. The BRFSS uses a standard calling protocol and calculates response rates[7] based on AAPOR RR#4. Two BRFSS call disposition codes may provide evidence as to the impact of the call screening apps: Call Blocked is assigned (after up to 15 attempts) if the interviewer detects a call blocking device, is asked to provide a PIN in order to be connected, or is connected to any message (produced by the potential respondent or by the provider) that indicates that the call may have been blocked; Technological Barrier is assigned (after up to 6 attempts) if the call repeatedly does not connect properly or is connected to a number of circuit messages. In 2016, 22,146 numbers were given a final disposition of “call blocked,” and 100,348 were assigned the code “technological barriers.” As these numbers reflect, this is a relatively small portion of the cell phone sample, overall. The small number may be a reflection of the fact that in most instances, the interviewer is unaware that a call is being blocked or screened. Indeed, historically these

[7] Behavioral Risk Factor Surveillance Stems 2016 Summary Data Quality Report. https://www.cdc.gov/brfss/annual_data/2016/pdf/2016-sdqr.pdf Accessed October 10, 2017.

numbers have little consequence as a share of total cell phone dispositions; here we show them as the proverbial canary in the coalmine with regard to the potential larger impact of call blocking on participation. And in fact, the rise in the numbers of these dispositions in the combined states' cell phone samples from 2015 to 2016 is notable (see Figure 1[8]).

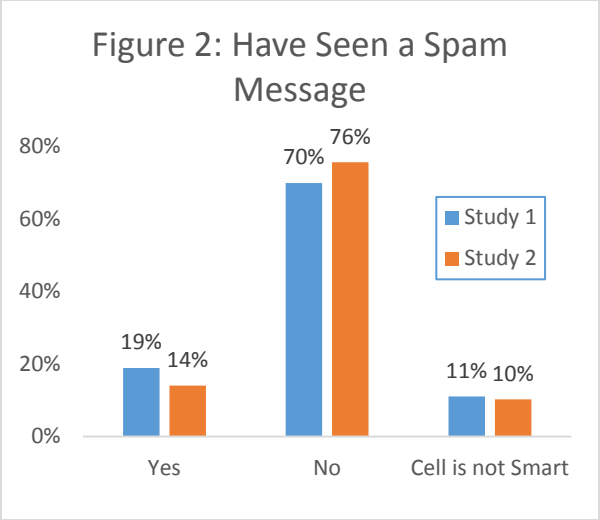


As was noted earlier, the interviewer in most instances is not aware that a potential respondent has blocked or screened incoming calls. The call blocking disposition has only been assigned to a small proportion of the sample, and interviewers are trained not to assign call blocking as a disposition unless they have reason to suspect blocking or screening by respondents, and not by other causes.

While at the time of publishing this report we do not have nationwide figures for the 2017 BRFSS, there are enough state data to suggest that the trend has continued into 2017. For data we do have in six states (ND, IN, ID, NY, TX, ME), the number of call blocking dispositions has doubled from the prior year. In total there is about an eightfold increase in call blocking dispositions in the two year period from 2015-2017.

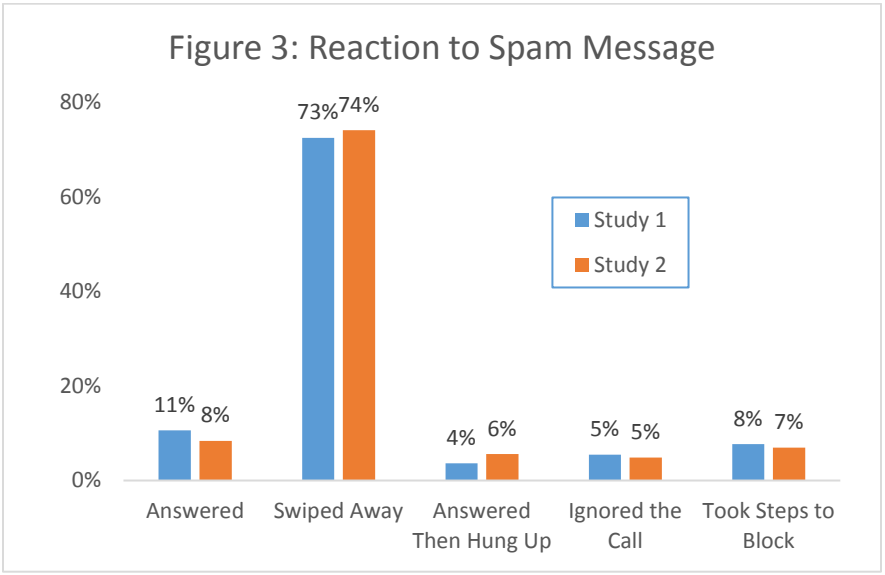
In an attempt to further assess the impact on nonresponse, SSRS fielded a number of questions in the SSRS Probability Panel. SSRS first ascertained whether the respondent had a cell phone and whether it was a smartphone. If they owned a smartphone, they were shown image 7 in this report and asked if they had ever seen it or some similar type of spam warning on their phone. Respondents were then asked how they reacted to the warning if they recalled seeing one. These questions were administered in two separate general population surveys in December 2017 and January 2018 (N = 1,016 and 1,452 respectively).

[8] Behavioral Risk Factor Surveillance Stems 2016 Summary Data Quality Report. https://www.cdc.gov/brfss/annual_data/2016/pdf/2016-sdqr.pdf Accessed October 10, 2017.



As shown in figure 2, 19 percent and 14 percent respectively said they had seen a message. While this is a low number, one must take these figures with a grain of salt given the possible challenge in recalling such a message, or the possibility they did not connect the spam image from Image 7 to whatever particular spam message they saw (and also to consider, this is among people willing to be part of a probability panel). SSRS did not see any way in which they could validate this measure and thus resolved to take it at face value. But they note that if there is error in this metric there seems to be a rationale to argue that it underestimates the number of cell phone owners who have seen a spam warning.

Unfortunately to the survey research industry at large, just under three out of four respondents who reported seeing a spam warning said they swiped the call away (rejecting the call) while still others eventually hung up. Some reported simply ignoring the call while others actually took action to specifically block the number in the future. In all, only about one in ten actually fielded the call. In short, the data show that the vast majority of receivers take the spam warning at face value, and in some manner, reject the call (see figure 3).



Assessing Whether Your Firm is Impacted

There are several means for survey research organizations to determine if spam warning or call blocking apps are affecting their telephone surveys. Survey organizations are encouraged to acquire spam warning and call blocking apps on phones purchased solely for detecting the flagging of telephone numbers as spam. Researchers would then seed the numbers of these phones in every study they carry out, and find ways to call these numbers as frequently (optimally, daily) as possible to determine if a survey is being targeted as potential spam or telemarketing.

Due to the difficulty of assessing whether a particular outbound number is being identified and labeled as spam through a comprehensive report, one way to measure the level of potential mislabeling is through manual in-house testing. Although this process does not provide a full scope of the degree to which a given number may be flagged by all the types of carriers, operating systems, and 3rd party apps, it can give an idea as to what percent of the outbound calls are being labeled as spam on specific systems, carriers and apps. Furthermore, a periodic retesting using this method, might indicate trends in call blocking (i.e. are more and more of the organization's calls being blocked?).

A possible model for an organization might involve acquiring two test phones (Apple iPhone and Google Android), downloading several blocking apps to these devices, placing test calls to the phones, and documenting the results. A test without any apps downloaded would also reveal the current status of the research firm phone numbers with the cellular service provider and operating system providers in combination. It may be more challenging to determine whether it is the service provider or the operating system provider is blocking a call unless there is a number of phones being tested with different combinations of these two factors.

A quicker, but less revealing way to assess the level of the call blocking issue of a research firm is to review calls that have been reported through the Federal Communications Commission (FCC) Consumer Complaints. The following website provides FCC open data for Consumer Complaints Data on Unwanted Calls[9]. One can filter this data and search for the phone numbers used by the research firm.

Some apps also provide a "reverse lookup" service. For example, Hiya app, allows customers to key in phone numbers and provides a caller ID info label without the actual phone call. Some apps, such as Call Control, rely on sister sites to identify calls that need to be marked as spam. Https://www.everycaller.com/ allows users to key in phone numbers and provides an output with information about that particular number. It provides info such as Caller (Name), Caller Type (Scam, Telemarketing, Robocall, Collection Agency, Phishing, etc.), and provides a list of comments from call recipients. As such survey researchers could use this service to gain some insight as to whether at least Hiya is flagging their numbers as spam.

[9] https://opendata.fcc.gov/Consumer/Consumer-Complaints-Data-Unwanted-Calls/vakf-fz8e

Government Involvement

FCC Involvement

The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the Commission is the federal agency responsible for implementing and enforcing America's communications law and regulations[10]. In its role, the FCC coordinated development and implementation of the Telephone Consumer Protection Act (TCPA) of 1991, which, among other rules, "Prohibits any call made using automated telephone equipment or an artificial or prerecorded voice to … a cellular telephone …"

In August of 2016, the FCC commissioned an industry-wide Strike Force to address the increasing number of consumer complaints about robocalls and telemarketing calls being made to both landlines and cellphones. In October of 2016, the FCC issued a report detailing the commission's initial findings and next steps.[11] The Strike Force consists of nearly three dozen major telecommunication and technology companies working to curtail the billions of pre-recorded phone calls made each year.

The Strike Force acknowledged that there is currently no single solution to robocalls that spans wired and wireless communication networks. As it relates to the wireless users, the Strike Force encourages service providers to offer call blocking solutions – either with standalone applications or with a network based solution. The Strike Force is also encouraging the industry, including third party entities, to come up with collaborative and creative solutions. The Strike Force continues to focus on a number of different aspects, including developing technology to verify exactly where a call originates.

The Strike Force stated that success would require action in three areas: source authentication; network and consumer blocking tools; and effective enforcement with the power to trace and shut down offending accounts. Among the features recommended by the Strike Force was creation and maintenance by the FCC of a "Do Not Originate" database of numbers to be blocked network-wide.

The FCC also recommended that outbound calls be segregated into a number of different business categories, including Survey Research. This would provide additional information to consumers about who was calling and assist them with how they would manage or control the incoming call. The call categories the FCC recommends are:

· Telemarketing
· Survey Research
· Political
· Charities/Non-Profit
· Informational

[10] https://www.fcc.gov/about/overview
[11] https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf

· Emergency/Public Service
· Collection
· Healthcare
· Basic/Personal
· Trusted Entity
· Spoofing
· Suspected fraudulent call

The FCC will not build nor maintain whitelists or blacklists. However, one of the Strike Force's recommendations is to encourage network operators and third-party developers to develop whitelists, something that is occurring today.

Further, both the FCC and FTC release call complaint data to the public quarterly. The releases contain originating numbers, but it is not clear what verification goes into those complaints before the data is shared, nor do the agencies separate out actual illegal telemarketing calls from any other. Providers of call blocking or tagging are known to add the numbers to their own blacklists.[12]

> "Even if providers use objective standards, there might be some situations in which legitimate calls would be blocked. For example, high-volume calls that properly obtain prior express consent might run afoul of call-per-minute restrictions even though all calls made are legal. This might occur if a call center lawfully spoofs the Caller ID on outgoing calls to utilize the business's toll-free number that consumers can use to call back or that might be familiar to consumers in a way that helps to identify the caller" ("FCC Fact Sheet: Advanced Methods to Target and eliminate Unlawful Robocalls: Notice of Proposed Rulemaking and Notice of Inquiry – CG Docket No. 17-59", "Protections for Legitimate Callers" p. 12)

The Commission is considering setting up regulations to avoid blocking of legitimate calls, "Specifically, should we require providers to "whitelist" legitimate callers who give them advance notice? Should we establish a challenge mechanism for callers who may have been blocked in error?" ("FCC Fact Sheet: Advanced Methods to Target and eliminate Unlawful Robocalls: Notice of Proposed Rulemaking and Notice of Inquiry – CG Docket No. 17-59", "Protections for Legitimate Callers" p. 12).

[12] The Insights Association told the FCC that, "Delivering all those originating numbers from disparate and unverified consumer complaints to voice service and call blocking service providers will probably do more to disrupt legitimate dialing than to combat illegal robocalls." http://www.insightsassociation.org/article/fcc-should-white-list-research-callers-insights-association-response-robocall-proposals

The FCC adopted and released on March 23, 2017 a Notice of Proposed Rulemaking and Notice of Inquiry on the topic of Advanced Methods to Target and Eliminate Unlawful Robocalls (2017 Call Blocking NPRM and NOI)[13], which were intended to "begin a process to facilitate voice service providers' blocking of illegal robocalls." The FCC was seeking comments on proposed rules which would provide service providers greater latitude in blocking potentially illegal calls, including : 1) "facilitate[ing] the sharing of such [subscriber-originated] requests among providers where, for example, the subscriber asks the provider that serves the number at issue to disseminate its request throughout the industry"; 2) "how and when such blocking [of calls originating from unassigned numbers] should be permitted and on whether there are other categories of numbers that should be considered to be unassigned"; 3) "what methods providers and third-party call blocking service providers employ in order to determine that a certain call is illegal"; and 4) "what blocking practices and objective standards should be covered by any safe harbor."

The FCC's Consumer Advisory Committee (CAC) issued on May 19, 2017 a set of 11 recommendations[14] in response to the 2017 Call Blocking NPRM and NOI, which included "Explore making complaint data available to third parties on a near-real time basis in order to maximize its usefulness for companies whose robocall analytics engines use the data to identify telephone numbers that may be candidates for blocking or providing alerts to consumers."

The FCC followed up the 2017 Call Blocking NPRM and NOI with a July 14, 2017 Notice of Inquiry in the matter of Call Authentication Trust Anchor (2017 Call Authentication NOI)[15], seeking to "explore how we can further secure our telephone networks against these activities by facilitating use of methods to authenticate telephone calls and thus deter illegal robocallers." The NOI calls out the two frameworks for authentication of legitimate telephone numbers documented in the April Strike Force report (STIR and SHAKEN), a governance approach, and criteria for designating certification authorities.

The FCC CAC met September 18, 2017[16] and made seven recommendations, including to "Encourage voice providers to offer consumers optional tools to block robocalls beyond the four categories mentioned in the NPRM and NOI and make information about those options easily available to current and potential subscribers." This recommendation appears very broad in terms of options which voice providers could offer. A summary of the meeting prepared by Paranorma Services, Inc.[17] provides the perspective "that while this NPRM/NOI seems to contemplate some of the right questions and the wheels of the rulemaking process are turning, blocking by voice carriers has already begun — absent any of the contemplated protections for legitimate callers."

[13] https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-24A1.pdf
[14] https://apps.fcc.gov/edocs_public/attachmatch/DOC-344985A1.pdf
[15] https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-89A1.pdf
[16] https://apps.fcc.gov/edocs_public/attachmatch/DOC-346767A1.pdf
[17] http://panoramalegal.com/2017/09/25/fcc-committee-meets-about-unwanted-robo-calls-makes-more-recommendations/

In its most recent action, the FCC on November 17, 2017 released the Report and Order and Further Notice of Proposed Rulemaking on Advanced Methods to Target and Eliminate Unlawful Robocalls[18] with a comment date of January 23, 2018. The proposed rules would allow "providers to block calls from phone numbers on a Do-Not-Originate (DNO) list and those that purport to be from invalid, unallocated, or unused numbers." The rules would "encourage providers who block calls to establish a means for a caller whose number is blocked to contact the provider and remedy the problem." This appears to stop well short of one of the lines of inquiry in the 2017 Call Blocking NPRM and NOI to establish "a mechanism, such as a white list, to enable legitimate callers to proactively avoid having their calls blocked."

Experiences from Europe

In Europe, government entities have in some cases also gotten involved in identifying legitimate callers. In Switzerland, for example, call blockers concern not only cell phones but also landline phones. Limiting the access to telephone-interviews through such practices makes it difficult to fulfill the scientific requirements of high quality surveys. Different countries have experienced differing levels of effect. Following Swiss telecommunication law (Fernmeldegesetz, FMG), the main national operator Swisscom has to protect their clients from unfair mass advertising (art. 45a). Swisscom therefore mandated a private company (katia.ch) to develop a call filter for landline and cell phones. In addition, clients can configure their own filter through an online portal. If nothing can be done against individual filters, the Swiss Association of Social and Market Research (vsms-asms.ch), a member of ESOMAR and EFAMRO, is fighting to get their member organization's phone numbers whitelisted from the general filter. The main argument for whitelisting is that following the same telecommunication law, Social and Market Research cannot be considered as unfair mass advertising. The Swiss Federal Statistical Office (bfs.admin.ch) already obtained such a whitelisting of their numbers. Katia built up an interface where they can add the numbers used for their surveys. However, the fight for the vsms members is still open (as of December 2017).

Current Mitigation Strategies and Possible Future Actions

There are a range of potential mitigation strategies the field of survey research and survey researchers can use to lessen the impact of call blocking and spamming.

Changing Numbers

One specific strategy survey research can enact immediately is the swapping of a blocked outbound number to a new telephone number. Ideally, the new number would be a number not yet used for other purposes; survey researchers have experienced situations where new numbers are immediately flagged as spam because they are already exist on blacklists from a prior use. Numbers can be purchased directly from the telecom provider that the organization already works with for an additional cost per

[18] https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-151A1.docx

phone number. This cost is typically minimal, but will vary based on the volume of numbers purchased each month.

One example is a recent state survey; this survey has found it necessary to rotate the outgoing number (i.e., the number that shows up on the phone of the person being called) on a daily basis and to recheck, on a monthly basis, the status of all of the numbers in the rotation to see if they are currently flagged as a high likelihood of spam. While there are no published results, the firm administering this survey found large variation in what a number was flagged as depending on the service provider, operating system, and presence of third party applications, even when calls were received within 30 minutes of one another.

Still, this strategy is viewed as a temporary solution to an ongoing problem since the use of these applications continue to increase and there are added costs associated with regularly changing outgoing numbers. Further, survey researchers have reported that numbers can get flagged as spam in as little as 24 hours. As such, close monitoring is required to ensure numbers are quickly replaced once identified as spam. Additionally, this strategy is not viable for organizations who have to preprint the outgoing phone number associated with an upcoming call on a pre-notification. While changing phone numbers and relying more heavily upon local presence dialing can improve productivity in centers, it should not be viewed as a long-term solution for survey researchers. Additionally, firms should be aware that there are patent applications pending for local presence dialing methods and applications.[19] There are concerns as well with the legitimacy of such a practice when a survey organization or its sponsor has no presence in the footprint of a given local telephone number.

Development of Outside Whitelists

Another possible solution to call blocking of survey research calls is the establishment of a whitelist. Unlike blacklists which list telephone numbers of known spammers, a whitelist would be used for legitimate businesses such as survey research firms. As a call is being routed to an individual cell phone, the respective provider would perform a look up to the white list to see whether or not the call can continue. Telephone numbers contained on a whitelist would not be blocked, even if they were previously flagged as a nuisance call by certain end users of databases.

There are some challenges in order for whitelisting to work. A single network based whitelist that all providers would check would be the ideal solution. However, there is no single network- based whitelist at the moment. Managing and maintaining the list is also a challenge. Some sort of validation process would need to be established to verify who gets placed on the whitelist. A likely scenario going forward is for a third party to develop and maintain such a list.

There are more questions than answers when it comes to creating a global whitelist. Here are some of these questions from the FCC Notice of Proposed Rule Making and Notice of Inquiry:

[19] https://www.google.com/patents/US9398148, https://www.google.com/patents/US9338289

> "First, we seek comment on establishing a mechanism, such as a white list, to enable legitimate callers to proactively avoid having their calls blocked. Should we specify the mechanism or mechanisms to be used or administrative details, such as the type of evidence providers might require of such legitimate callers? If so, what should we require? Should we specify a timeframe within which providers must add a legitimate caller to its white list? How should white list information be shared by providers? Is there anything the Commission can do to ensure that white list information is shared in a timely fashion such that legitimate callers need not contact each and every provider separately? Is Commission action needed to guard against white lists being accessed or obtained by makers of illegal robocalls? What is the risk that a caller could circumvent efforts to block illegal robocalls by spoofing numbers on the white list? Is this risk mitigated by the SHAKEN and STIR standards for authenticating Caller ID if, for example, the white list requires that all calls from the white listed telephone number be signed—once those standards have been implemented? Finally, we seek comment on any other relevant issues." ("FCC Fact Sheet: Advanced Methods to Target and eliminate Unlawful Robocalls: Notice of Proposed Rulemaking and Notice of Inquiry – CG Docket No. 17-59", "Protections for Legitimate Callers" p. 13)[20].

Another possibility is to classify incoming calls to cellphones by type of business (i.e. survey research vs. telemarketing). This is one of the points made by the FCC Robocall Strike Force. Some applications and providers are already providing this functionality. To be effective though, a single network solution would need to be established.

Applying a nuisance scoring to cellular telephone sample is yet another possible solution. Samples of telephone numbers could be run through a scoring algorithm to append a nuisance score. The score would indicate the likelihood the respondent would report the incoming call as spam or as nuisance call. These numbers could be handled separately or purged all together from the sample.

The owners of the operating systems control the terms of service for all applications. It is theoretically possible, then, for those operating systems to include provisions to allow for certain phone numbers to remain unblocked by their applications. This would require negotiations and separate agreements with Apple and Google.

Conclusion

The development of call blocking techniques has a reasonable goal: to limit the amount of illegitimate spam calls and illegal telemarketing calls on cell phones. Just as the practice of bottom netting in fishing causes considerable the collateral damage to other species and the ecosystem as a whole, the practice

[20] https://transnexus.com/solutions/stir-and-shaken/understanding-stir-and-shaken

of call blocking and spam filtering in telephony is, in the process of surely reducing illegal calling, also causing great harm to survey research and surely other legitimate domains.[21]

AAPOR is currently considering action to encourage developers of cell phone operating systems, carriers, and 3rd party apps to modify their techniques to avoid harm to legitimate businesses. These actions may include the encouragement of official whitelists, legal avenues of remediation, or both, and perhaps in concert with other impacted organizations and industries. While these efforts are undertaken, survey researchers can take steps to reduce the impact in production and respondent cooperation. Survey organizations should acquire spam warning and call blocking apps on phones used to detect call blocking and spam filtering. Researchers should then check all numbers they use for outbound calling on these phones, daily if possible. When numbers become blocked or otherwise flagged, organizations are encouraged to retire those numbers and acquire new, "clean" numbers.

Researchers are further encouraged to attain more data on the empirical impact of call blocking and spam filtering. The survey research industry has faced many challenges in its past, and looks forward to an eventual resolution of the deleterious impact of call blocking and spam filtering.

Appendix

Links to Lists/Description of Apps

There are numerous articles and lists online describing and evaluating various call blocking apps. These are easily found in search engine results for call blocking apps. The most comprehensive list of applications available by operating system (Android, iOS, Blackberry and Windows) seems to be at: https://www.ctia.org/consumer-tips/robocalls. There are links to lists by OS at the bottom of the page. The data were last updated in April 2017 and yet list 56 apps for Android, 23 for iOS, 13 for Blackberry and 9 for Windows.

Some Specific Apps

a. Safest Call Blocker

b. Mr. Number[22]

c. Call Control

d. Extreme Call Blocker

[21] As one example, a colleague overhead a conversation where a patient was complaining about not getting alerted about an upcoming appointment, only to then realize they did see a number of incoming calls from the doctor but ignored them because they were flagged as spam.

[22] Mr. Number is linked to Hiya. On their website, you can choose to relabel your caller ID. https://hiya.com/manageyourcallerid

e. Nomorobo[23]

f. Hiya[24]

g. Sync.me

h. Robokiller

i. TrueCaller

j. Callblocker

k. Callblock by Rocketship

l. CallApp

m. PrivacyStar[25]

n. Should I Answer?[26]

o. UMail[27]

n. CallControl

[23] Nomorobo can be run on iPhone, Landlines, and soon will be available on Android. It also has a tool for blocking SMS spam text messages. Nomorobo uses a feature known as "Simultaneous Ring". When simultaneous ring is enabled, your phone will ring on more than one number at the same time. The first device to pick it up gets the call and the other phones stop ringing. When the Nomorobo number is enabled as a simultaneous ring number it is the first number to screen the call. If it's a legitimate call, the call goes through to your number. If the call is an illegal robocaller, Nomorobo intercepts the call and hangs up for you. Your phone will ring once letting you know that the robocall has been answered and stopped." (http://www.nomorobo.com/nomorobo101). Reaching out in attempt to "whitelist" selected numbers, through a "Submit a Request" page on the nomorobo website, proved to be very effective. An email request was routed to company founder, Aaron Foss, who was able to 'whitelist" all numbers requested. Moreover, the numbers were said to have been permanently whitelisted, so there is no risk of them ever getting stopped again by this company.

[24] "Hiya Caller ID and Block" can be run on both iPhone and Android. Reaching out to the main support email (support@hiya.com), with a request to "whitelist" legitimate numbers proved to be effective. Hiya support was able to "whitelist" the requested numbers by removing the spam label and adding the proper Caller ID. Hiya analyzes phone number traffic behavior and classifies whether the numbers are spam or not based on those behaviors. "Hiya analyzes more than 3.5 billion incoming mobile calls per month globally and then leverages its proprietary rule-based algorithm to identify these calls for consumers. Hiya's Robocall Radar is calculated by extrapolating the total number of unwanted robocalls detected among Hiya's user base as compared to the entire US mobile subscriber base. Growth in total call volume and the numbers involved with these calls will vary month to month." (https://hiya.com/robocall-radar).

[25] PrivacyStar can be run on both iPhone and Android. The company has agreed to whitelist the numbers for the U.S. Census. They requested that numbers are entered in to the www.calltransparency.com website.

[26] Should I Answer? can run on Android. This app is respondent reported based on positive, neutral, or negative ratings, but the company can override to force neutral labels to prevent call blocking or making as spam. After reaching out to this company, U.S. Census numbers were "whitelisted" with a forced "neutral rating" and will not be blocked even if negative user reviews are accumulated.

[27] Youmail can run on both iPhone and Android. Principals have expressed interest in working with AAPOR regarding whitelists.