Response to Additional Questions
Do Not Call: Combating Robocalls and Caller ID Spoofing

Chairman Latta, and Members Burgess and Bilirakis,

Thank you again for the opportunity to present testimony before the Sub-Committee on Digital Commerce and Consumer Protection. It was an honor and privilege to participate, and I appreciate the opportunity to provide feedback to your follow-up questions in this document.

Thank you,
Ethan Garr
RoboKiller.com
Chief Product Officer

Response to questions from: The Honorable Robert E. Latta

1. Today, our RoboKiller mobile app has over 210,000 customers. Following a one-week free trial period, users can either pay $2.99 per month or $24.99 per year.
2. RoboKiller works by putting Answer Bots, which are time wasting robots to work against the invasive spam and telemarketing calls we block for our users. Using an advanced algorithm that blends technologies including machine learning and audio-fingerprinting, we are able to maintain a comprehensive and dynamic global block list of more than 200,000 known spammers. We use Apple's CallKit technology to block these calls from ringing on our customer's phones, but then, using a call forwarding methodology, we are able to answer the calls we block with Answer Bots. These robots, which users either record themselves, or choose from our library, are trained to reach the human telemarketers behind robocalls to waste their time with extended conversations. While these conversations are entertaining and give our users the satisfaction of getting even with telemarketers, they also serve an important purpose: every minute of a telemarketer's time we waste, is a minute they cannot use to scam someone else, whether that is one of our customers, or someone's unsuspecting grandmother. By wasting telemarketers' time, RoboKiller is able to interfere with the spammer's business model, which ultimately will put them out of business.
3. Once a subscriber downloads and successfully sets up RoboKiller, they are immediately protected from more than 200,000 known spammers and from the majority of neighbor-spoofed calls (telemarketing calls that appear to be coming from a local caller ID). These calls will no longer ring on their mobile phones, but the service will answer these calls with Answer Bots. When a telemarketer calls one of our user's phone numbers, our customer only receives a push notification indicating that RoboKiller has protected them from the intrusion. Their phone does not ring. Most users will experience a 90% reduction in spam calls when they use the service. Users are also given the opportunity to provide feedback when we block calls on their behalf, to help our service better protect them and all of the users in our ecosystem. Users can also manually whitelist

and blacklist numbers, and we use data from these interactions to help us train our blocking algorithm.

4. We estimate a false-positive rate of less than 1.5%, and give our users the ability to provide feedback if we incorrectly identify and block a numbers so that we can update the service for them and for other users appropriately.

5. For RoboKiller, if Apple continues to expand the functionality of its CallKit service it will help us improve our call blocking service. If the equipment manufacturers added call blocking without our app it would limit our ability to use Answer Bots on behalf of our users and likely exacerbate the robocall epidemic as a whole. We contend that unless we can impact spammer's bottom line, the problem will only get worse. Blocking calls alone, just means that spammers skip over savvy users who are unlikely to fall victim to scams, to more efficiently reach their more vulnerable, intended targets.

6. We are not currently sharing call complaint data with the FTC, but we are certainly open and willing to do so. We have not discussed this with the FTC in a long time, but when we did (a few years ago), it did not seem like they had an easy way to ingest data that we could provide. We do include data from the FCC in our call blocking algorithm, but this data is not real time, which makes it a less valuable source for us. From our own efforts, we have found that call data that is even a few hours out of date is less useful for the purposes of curating our global block list, so we are only able to use this data as a secondary point of verification. If the FTC can provide a live feed of this data that we can consume it will substantially improve its value and usefulness for our purposes. Also, if the FTC can give us a method of providing large batches of data we collect, we would be happy to do so. We also feel our users would get great benefit and appreciate it if we could give them an option to share complaint data directly from the app or our website to the FTC.

7. Our system is self-correcting in that our users provide feedback about the calls we block for them both directly and indirectly, and then we use that information to correct our global block list. If we see users providing feedback, or blacklisting, or whitelisting numbers in a manner that is inconsistent with how we are marking those callers, our algorithm will consider that and adjust as appropriate. In rare cases we will make manual changes based on feedback we receive through our support channels.

8. Audio-fingerprinting, as we are using it, should not impact privacy as the only calls we are fingerprint are recordings of calls such as voicemails or interactions between our Answer Bots and robocalls, as directed by our users to improve the quality of their service. Audio-fingerprinting only looks at the recordings as audio data and makes comparisons between sets of data, so it should not impact privacy for any party.

Response to questions from: The Honorable Michael C. Burgess

1.
    a. We are not sure if this question is specifically meant for RoboKiller, as we have not been part of, nor have we been asked to comment, on this rulemaking process. Generally speaking, RoboKiller looks to block all

unwanted calls a user might receive, and allow only wanted calls to ring through. Whether or not a call is legal or illegal, is not the question our users are asking RoboKiller to discern, they are looking for the service to block calls they feel are unwanted. We do recognize that different users will have different opinions as to whether a call should or should not be blocked, and therefore, we notify users whenever we block a call so that they can decide if they agree with our system's decision. Users can blacklist or whitelist any number to ensure that the calls we block or do not block are appropriate.

    b. Yes, if our users believe calls are legitimate and should not have been blocked, our system is self-correcting. If we see users providing feedback, or blacklisting, or whitelisting, numbers inconsistent with how we are marking callers, our algorithm will consider that and adjust as appropriate. In rare cases we will make manual changes based on feedback we receive through our support channels. However, we feel strongly that our users should determine what is a wanted versus unwanted call.

2. Most companies, like RoboKiller, use their blogs to speak to users about such issues. I think if government entities like the FTC, FCC, and IRS reach out directly to companies like us with specific information about scams and issues, we would be happy to share that content with our users. We are always looking to help consumers better understand the threat and the scope of the problem, but it is difficult for us to know, without a central channel, what information the Government would like us to share with our audience.

3. Because RoboKiller answers the calls it blocks and then allows users to listen to these calls the way they would listen to voicemails, we don't believe our solution threatens legitimate companies ability to conduct business. Consumers should be able to decide what calls they wish to ring through to their phones, and our service provides that ability without risk that important calls will be discarded. Furthermore, our system's self correcting nature ensures that through user feedback, RoboKiller will adjust to allow wanted calls to ring through.

Response to questions from: The Honorable Gus Bilirakis

1. Pre-paid mobile users are more vulnerable to scams. They are no more likely to get robocalls and telemarketing calls than people with unlimited plans, as the spammers have no way to target one over the other, however, most mobile carriers do not provide pre-paid plan subscribers with access to conditional call forwarding, which is a feature we need to provide the RoboKiller service to customers.

2. To be clear, I feel that robocall blocking tools that do not make efforts to engage spammers and consume their time do exacerbate the problem by allowing scammers to quickly skip over savvy consumers to reach more vulnerable targets. RoboKiller's Answer Bots are specifically designed to waste spammers' time, and therefore they do protect consumers in your district (even if they don't have RoboKiller) who are less tech savvy, and are less able to protect themselves. So, encouraging those in your district to

use our service should help protect both the tech savvy and less tech savvy populations. Beyond that I do think it is important to take steps to educate your constituents about the dangers that lurk behind a ringing phone. Encouraging them not to answer unknown calls, to always demand any request for personal information in writing via certified mail, and to report any suspicious calls to government agencies is a useful effort. The best ways to do this is likely through media campaigns, public service campaigns, etc.

Thank you again,
Ethan Garr