Authenticated Caller ID Plus Regulatory Changes

By Vincent A. Lucas, Ph.D.

Presented to the FTC Robocall Challenge

This paper provides solutions to two problems faced in the enforcement of the Telephone Consumer Protection Act (TCPA).

Problem 1: False Caller ID information

The monetary penalties provided under 47 USC § 227(b)(3), (c)(5), and (g) plus the FTC Do-Not-Call complaint registry would provide an adequate deterrent to illegal robocalls *if* consumers could reliably identify the originators of the illegal calls. However, the current Caller Identification system is not designed to be reliable[1], and consequently illegal telemarketers can avoid prosecution by sending false Caller ID information ("spoofing") and refusing to otherwise identify themselves. For example, in the "Rachel from Cardmember Services" scam[2], robodialers send out millions of prerecorded messages identifying the caller only as "cardmember services". The telemarketer's live agents are instructed to not give out the true identity of the company.[3] If the telemarketer spoofs the Caller ID, the consumer cannot determine who the telemarketer is. If the consumer files a complaint but cannot provide the true telephone number or name of the telemarketer, law enforcement cannot do much to follow up on the complaint. A reliable caller identification system is necessary for the enforcement of the TCPA.

Solution: Authenticated Caller ID

The image submitted with this paper is a diagram of the system. When a telephone call is initiated:

1. The caller's communications service provider (CSP) establishes a connection with the CSP for the destination telephone number. The caller's CSP must be the communications service

[1] Caller ID is easily spoofed using VoIP or PRI lines. See http://en.wikipedia.org/wiki/Caller_ID_spoofing. A Google search for "caller ID spoofing" shows many commercial websites claiming to offer Caller ID spoofing, e.g. http://www.spoofcard.com

[2] http://www.ftc.gov/opa/2012/11/robocalls.shtm

[3] I know this from personal experience in attempting to get "Rachel's" live agents to reveal the name of the company they represent.

provider associated with the caller's telephone number according to records maintained by the Number Portability Administration Center (NPAC)[4].

2. After establishing the connection, the caller's CSP sends a data message digitally signed[5] by the caller's CSP. The data message contains:

- the source (i.e. caller's) telephone number,
- the name of the person or organization to whom the source telephone number has been assigned according to the records maintained by the caller's CSP,
- the destination telephone number, and
- a timestamp.

This data message is the Authenticated Caller ID information.

3. The destination's CSP rejects the data message if:

- The digital signature is not valid;
- The company that signed the data message is not the CSP associated with the source telephone number according to the records maintained by NPAC; or
- The timestamp is more than 30 seconds[6] later than the time when the destination's CSP received the data message.

4. If the data message is not rejected, the destination's CSP permits the call to go through to the destination telephone. The source telephone number and name in the data message is displayed as the caller's phone number and name on the destination telephone's Caller ID device. If the data message is rejected, the call is terminated; the destination telephone does not ring and the callee is not otherwise alerted to the fact that someone attempted to call him/her.

[4] NPAC (http://www.npac.com) administers records that show what CSP a telephone number is assigned to. If a country other than the United States or Canada wants to provide Authenticated Caller ID information for calls originating from that country, the applicable regulatory agency in that country would need to use an organization similar to NPAC.

[5] Digital signatures are commonly used in computer science to establish that a message comes from a particular author and that the message has not been altered. For example, Android applications must be digitally signed by the author before they may be sold on the Android Market. For more information on digital signatures, see e.g. H. Delfs and H. Knebl, "Introduction to Cryptography, Principles and Applications" (2nd ed. 2007); http://en.wikipedia.org/wiki/Digital_signature

[6] The timestamp check is done so that the data message cannot be reused for a different call. A value other than 30 seconds could be used, but the value must be longer than the time required to transmit the message from the caller's CSP to the destination's CSP. On slow networks, one could also create a protocol to permit multiple attempts to retransmit the message if it is rejected only because of the timestamp.

Responsibilities of the caller's CSP

The person or organization to whom the CSP assigned the telephone number is called herein the "account holder". The CSP shall maintain records that show the name and address of the account holder (and any other information designated by the FTC that would be useful to law enforcement in tracking down the account holder). The CSP should not send a digitally-signed Authenticated Caller ID data message unless:

- For telephone numbers associated with a landline or cell phone, the call originates from the landline or cell phone associated with the account holder's telephone number;
- For telephone numbers associated with VoIP, the CSP has authenticated that the account holder, or someone authorized by the account holder, is the person originating the call, for example, the caller has logged into his account over a SSL connection using a reasonably strong password and then originates the call using the account[7].

This is not a comprehensive list. The CSP can send the digitally-signed Authenticated Caller ID data message under other circumstances in which there is high certainty that the call originates from the account holder, someone authorized by the account holder, or the account holder's telecommunication equipment.

A CSP that intentionally or repeatedly does not adhere to these responsibilities should be prohibited from being assigned telephone numbers by NPAC.

Business callers that wish to display a common Caller ID

Some business callers may wish to call from numerous telephone numbers but display on the Caller ID a single telephone number. E.g. calls from numbers 212-555-01xx all display as 212-555-0100 which is the customer service number for the business. This can be permitted, as long as the call originates from one of the telephone numbers assigned to the business, and as long as this is otherwise permitted by regulation.

Handling calls that do not contain Authenticated Caller ID information

A call might not have Authenticated Caller ID information if the caller intentionally blocked the transmission of Caller ID information or the call originates from a region in which Authenticated Caller ID has not been implemented yet (e.g. a foreign country). Telephone

[7] For VoIP accounts associated with a specific landline, for example, a VoIP account from a cable company that is associated with the account holder's cable line and in which the CSP expects calls to originate only through the cable line, the CSP should send the Authenticated Caller ID data message only if the call originates from the landline.

consumers should be provided, free of charge, options for how to handle such calls. At least the first two of the following options should be provided:

1. Automatically reject the call. The callee is not alerted to the fact that a call was attempted. The caller hears a message saying that the call cannot be completed without Authenticated Caller ID information.

2. Permit the call to go through. Some businesses may prefer this over call rejection. If unauthenticated Caller ID information is available, display a warning on the Caller ID device that the Caller ID information is not authenticated.

3. Use some other system to decide whether to permit the call. For example, allow the call only if the caller successfully completes an audio CAPTCHA,[8] or permit the call if it contains unauthenticated Caller ID information and the caller's number is on a list of numbers provided by the consumer. This option would be particularly useful to consumers who expect to receive calls from family and friends in regions where Authenticated Caller ID has not been implemented.

The consumer should be able to choose one of these options when setting up his/her telephone account, and should be able to change the option later.

*99 to file a complaint of illegal telemarketing

Some consumers do not have Caller ID display devices. A system should be provided so that these consumers can file a complaint of illegal telemarketing that contains the telemarketer's Caller ID information. For example, if the consumer dials *99 immediately after a call, the consumer is sent to an Interactive Voice Response system that the consumer can use to register a complaint, and the Authenticated Caller ID number of the alleged telemarketer will automatically be put into the complaint.

<u>Problem 2: Use of facilitator companies</u>

Another way that telemarketers have been evading prosecution under the TCPA is by using facilitating companies who "loan" their telephone numbers to them.[9] The telemarketer, often through an intermediate company located outside the U.S.A., obtains permission to use a large number of the facilitator company's telephone numbers. The number displayed on the

[8] http://en.wikipedia.org/wiki/CAPTCHA

[9] *Cellco Partnership d/b/a Verizon Wireless and Onstar, LLC v. Dealers Warranty, LLC, et al.*, NJ Dist. Ct. Case No. 3:09CV1814; *Astrahan v. Pacific Telecom Communications Group*, C.D. Cal. Dist. Ct. Case No. SACV 12-02184; *Lucas v. Pacific Telecom Communications Group*, S.D. OH Dist. Ct. Case No. 1:12CV630.

Caller ID is a real telephone number, but it is the number of the facilitator company, not the telemarketer. The facilitator company says that it is not the originator of the calls and so it claims it is not liable under the TCPA for the calls.

Why do this instead of just spoofing the Caller ID? One reason is in order to obtain additional profits from Caller ID Name (CNAM) database queries. The presentation from Telephone Management Corporation (TMC), available at http://telemarketerspam.wordpress.com/2012/05/19/about-pacific-telecom-communications-group/pacific-telecom-communications-group-f-antone-accuardi-_01/, describes the scheme. (See also http://www.slideshare.net/CNAM/cnam-revenue-share). The facilitator company maintains various Caller ID Name databases. When a consumer receives a call with one of the facilitator's telephone numbers, the consumer's telephone company looks up from one of these databases the name that should be displayed on the Caller ID. The facilitator company is paid by the consumer's telephone company each time that the name is looked up from the facilitator's database. The facilitator company has a revenue-sharing agreement in which the telemarketer is then paid a portion of revenue received from the CNAM database lookups. Hence, the telemarketer profits from the call even when the callee does not answer the phone. These revenue-sharing plans obviously encourage the telemarketer to call over and over even if the consumer has previously rejected the telemarketer's offer. Sadly, in recent years, many other companies have copied TMC's revenue-sharing plan.[10]

Solutions

1. Authenticated Caller ID

Authenticated Caller ID eliminates the use of the facilitator companies' CNAM databases. The name displayed on the Caller ID comes directly from the records of the caller's CSP, and the destination's CSP is not charged a fee for this information. Facilitator companies no longer derive profit from selling CNAM database access to telephone companies, and therefore cannot share this profit with telemarketers. Therefore, this eliminates one financial incentive for telemarketers to call over and over. This also eliminates the problem that consumers do not receive the Caller ID name information when their telephone company is not willing to pay for access to the facilitator companies' CNAM databases. Furthermore, facilitator companies and telemarketers are not able to tamper with the Caller ID name information.[11] The

[10] For example, Google search "dipfee revenue"

[11] Slide 6 of the TMC presentation claims that its service allows their customers to "instantly change the message that appears" as the Caller ID name.

current unreliable Caller ID system allows the telemarketers to display Caller ID name information that is false, misleading[12], or does not correctly identify the company that is calling.

2. Regulatory/statutory changes

A. Strict liability under the TCPA for companies who "loan" their telephone numbers to others

The rule should be simple and unambiguous. If a company "loans" out its telephone number, that company is liable for any violation of the TCPA made using that telephone number, regardless of whether the facilitator knows that the number is being used for illegal telemarketing. These facilitators should be liable to the same extent that they would be if they were the actual telemarketer.

The strict liability rule has many advantages. This rule would eliminate the burden on plaintiffs of attempting to prove the facilitator knew or "consciously avoided knowing"[13] that their number is being used to violate the TCPA. It was originally envisioned that consumers would be able to sue under the TCPA representing themselves in small claims court[14]. However, any time that a plaintiff needs to prove that a defendant "knew" or "consciously avoided knowing" something, the lawsuit is too complex for most consumers to handle without an attorney.

A strict liability rule would put the burden on the facilitator company to thoroughly check the trustworthiness of any company before granting the company permission to use its telephone numbers. Additionally, facilitator companies can contractually require the telemarketer to indemnify them for any TCPA liability so that the telemarketer ultimately pays for the TCPA violation.

[12] For example, in the "Rachel" scam, the telemarketer often displays "Card Services" as the Caller ID name, which misleads some consumers into believing that the call is from customer service for a bank that they already have a credit card with.

[13] 16 CFR § 310.3(b)

[14] "The . . .[TCPA] contains a private right-of-action provision that will make it easier for consumers to recover damages from receiving these computerized calls. The provision would allow consumers to bring an action in State court against any entity that violates the bill. … [I]t is my hope that States will make it as easy as possible for consumers to bring such actions, preferably in small claims court. . .
Small claims court or a similar court would allow the consumer to appear before the court without an attorney. The amount of damages in this legislation is set to be fair to both the consumer and the telemarketer. However, it would defeat the purposes of the bill if the attorneys' costs to consumers of bringing an action were greater than the potential damages." Remarks of Sen. Hollings, 137 Cong. Rec. 30821-30822 (1991).

B. Nationwide service of process for claims under the TCPA

This simply means that consumers and law enforcement can sue facilitator companies in the federal judicial district where the call was received. In *Cellco Partnership v. Dealers Warranty*, the court dismissed the claims against TMC based on lack of personal jurisdiction.[15] According to this ruling, a lawsuit against TMC for facilitating illegal telemarketing would need to be filed in Oregon[16] instead of the location where the consumer received the call. This ruling, if followed elsewhere, would lead to the absurdity that a single telephone call could lead to lawsuits in multiple district courts. In fact, there might need to be a separate lawsuit in a separate district court for each facilitator used by the telemarketer. This would impose an enormous burden on anyone suing under the TCPA and would also be a waste of judicial resources. A statute which authorizes nationwide service of process for TCPA claims would allow a plaintiff to sue the facilitators in the venue where the call is received.[17]

The proposed solution meets the Robocall Challenge Criteria

Does it work?

I do not believe it is possible with existing technology to create hardware or software that can accurately distinguish between illegal sales solicitation calls and lawful calls, such as charitable solicitations, lawful debt collection efforts, and political calls. Instead, I believe the best strategy to prevent illegal robocalls is to accurately identify the originators of the calls and impose financial penalties on them. Therefore, to enforce the TCPA, at a minimum, consumers need the real telephone number of the telemarketer. I believe that Authenticated Caller ID and the proposed regulatory changes, combined with the monetary penalties already provided by statute, would deter nearly all illegal telemarketing. The proposed solution would not prevent legally permitted calls, since the monetary penalties do not apply to legal calls. If the consumer chooses to block all calls that do not have Authenticated Caller ID data, a small number of wanted calls may be blocked. These are calls where the caller intentionally blocked transmission of Caller ID information or calls from a region where Authenticated Caller ID has not been implemented. I believe however that for consumers that choose to block all calls without the Authenticated Caller ID information, the number of blocked wanted calls would typically be very low, and most of these consumers will consider the benefit of blocking to far outweigh the drawbacks.

Is it easy to use?

The consumer does not need to do anything to benefit from the proposed solution. The

[15] *Id.*, Opinion dated Sept. 17, 2010, Docket entry 142.
[16] Or some other state that TMC has sufficient "contact" with
[17] Federal Rule of Civil Procedure 4(k)(1)(C).

consumer may optionally configure how calls without Authenticated Caller ID information should be handled and may use *99 to report illegal telemarketing. Otherwise, there is nothing for the consumer to learn.

Can it be rolled out?

A Caller ID system that reliably provides the real telephone number of callers could readily be implemented using existing technology. The current, easily-spoofable Caller ID system must be replaced with a reliable system. However, the government would need to mandate the replacement of the current Caller ID system within the United States. Authenticated Caller ID does *not* need to be implemented worldwide in order for consumers in the United States to receive benefit from implementing it in the United States.