On the Effectiveness of the National Do-Not-Call Registries

Merve Sahin, Aurélien Francillon,
EURECOM, Sophia Antipolis, France
{merve.sahin, aurelien.francillon}@eurecom.fr

***Abstract*—Voice spam is a significant problem worldwide. In this paper, we observe some aspects of the voice spam ecosystem in Europe using a telephony honeypot with 800 phone numbers from 8 European countries over a period of 3 years. Unlike previous honeypots, the numbers were never assigned to a real user before being added to the honeypot.**

The specific nature of this honeypot allows us to focus on illegitimate calls. Indeed, as the numbers were never used by real users, no consent to telemarketing has ever been given.

In particular, we present an experiment we conduct on National *Do-Not-Call* (DNC) lists and the effects of registering to such lists. We find that the phone numbers added to DNC lists receive a lower number of spam calls both in Spain and the UK. However, we also show anecdotal evidence that the DNC list in the UK is abused by spammers. Finally, we discuss the effectiveness of DNC lists by reviewing various implementation challenges and comparing the existing approaches.

I. Introduction

Unwanted phone calls may take many forms, both in terms of call content (e.g., telemarketing campaigns, market research and surveys or various scams) and in terms of call format (e.g., calls from live agents, calls playing pre-recorded messages, one-ring (ping) calls, abandoned (silent) calls).

Such calls have been a major problem in many countries since years, and have impelled governments and regulator bodies to take countermeasures to protect consumers' choices for their privacy and peacefulness [8], [20], [28], [30]. However, despite these countermeasures the amount of unwanted calls have been on the rise, leading to millions of consumer complaints [19], [29], [36].

A common initiative that is adopted by many countries is the establishment of a National *Do-Not-Call* list – an opt-out mechanism for consumers– to avoid unsolicited telemarketing and sales calls. These lists are often enforced by regulations, and the companies that violate the DNC lists (i.e., calling a phone number registered to the DNC list without consent) are fined [22], [25], [31]. Unfortunately, this countermeasure is only effective against legitimate telemarketing campaigns, whereas scammers (especially from overseas call centers) and other abusive and illegitimate companies usually ignore the DNC list or find ways to avoid regulations (such as using 'front' companies or spoofing caller ID) [21], [22], [25], [39]. Moreover, DNC lists have been frequently subject to dispute and criticism about their effectiveness [24], [27], [42].

There were even cases where the DNC lists were leaked to 3rd parties, invading the privacy of thousands of users [10], [25]. Indeed, some consumers report that registering a number to the DNC list increases the amount of spam it receives [13], [32]. However, it is often difficult to identify if this increase is only a perception, if there is a real correlation, or finally, if the registration to the DNC list is the cause of the increase of unwanted calls (as some users seems to believe).

In this paper, we make an overview of the current DNC list practices in Europe, and present our findings from a telephony honeypot that we have been operating for the last 3 years. Our honeypot is made of 800 fixed phone numbers from 8 European countries which are directed to an Asterisk server. Our honeypot did not receive a high volume of calls because of its particular nature: unlike previous honeypots, the numbers were never assigned to real users before being added to the honeypot. However, this made possible to perform an experiment designed to test the effectiveness of DNC lists. In particular, while we show that, overall, the phone numbers registered to the DNC list receive a lower amount of spam, we also observe a clear abuse of the DNC list in the United Kingdom. We then study the different DNC list implementation choices in Europe and conclude that such abuses can be prevented with better practices in relation to the distribution, maintenance and the coverage of the lists.

In summary, we make the following contributions:

- We deploy the first telephony honeypot that aims to observe voice spam in Europe, in particular unwanted calls performed without user consent. Our honeypot covers 8 countries and has been running for 3 years.
- By registering some of the honeypot numbers to the DNC list of their respective country, we analyze the effectiveness of these lists, and, in particular, we identify a clear effect in Spain and UK.
- We give a comparative analysis of the DNC list practices in 6 of the 8 countries, and discuss the possible problems.
- Finally, we present our observations on two spam campaigns (one in Spain and one in UK) that are captured by our honeypot.

II. Honeypot setup

Telephony honeypots aim to collect data on the incoming phone calls received by a set of phone numbers. The phone numbers are usually directed to an IP based telephony server (IP-PBX) that uses a set of phone lines to receive calls and allows to process them (e.g., answer, record, forward). As opposed to the spam call complaints reported by consumers,

telephony honeypots provide complete data with high accuracy on the time and metadata of the call [35].

The phone numbers that will be assigned to a telephony honeypot can be chosen in different ways, depending on the purpose of the honeypot. For instance, the phone numbers that have been returned by consumers due to high spam volume (also called *dirty numbers*) would allow the honeypot to collect high number of calls, especially the calls targeting various telemarketing lists. On the other hand, use of *clean* phone numbers (that were never assigned to a user) may allow to observe calls that are randomly targeted. Note that, it is always possible to 'seed' (i.e., advertise) the clean phone numbers in various platforms (e.g., online social networks, questionable websites [34]) to attract more calls from spammers, however, we did not perform this. In addition, a telephony honeypot can be either interactive (i.e., responding to the call and interacting with the caller) or low/no interaction (i.e., not responding to the calls, or passive response).

In our experiment, we deploy a no interaction honeypot with 800 phone numbers from 8 European countries. The phone numbers were provided by Voxbone[1] via a SIP trunk linked to our telephony server. Each country has a *consecutive* range of 100 numbers, which are all fixed phone numbers belonging to the same geographical area (Table I). In other words, our honeypot numbers differ only by the last 2 digits in their respective countries.

Incoming calls that are received at the honeypot are first answered with a ring tone that continues for 12 seconds. Afterwards, a busy signal is emitted for 10 seconds and the call is terminated. Note that the calls can also be terminated by the calling party before termination on our side, and the related information will be logged.

As all our honeypot numbers are clean (i.e., they had never been used after their allocation by the regulator), no one ever gave consent to any telemarketing or advertisement calls. Therefore the numbers should not be in any telemarketing list. However, we expect that our honeypot may receive several type of calls:

- Telemarketing calls that target phone numbers without user consent (cold-calls).
- Calls that do not require user consent (e.g., in some countries, calls from non-profit organizations or survey calls).
- Calls that aim to scan phone numbers and identify if the numbers are currently in use.
- Calls intend to scam phone users (e.g., ping or callback scam, technical support scams, vacation scams).

We also inspect the phone number allocations at each country, in order to find if our honeypot numbers are part of a large or a small block of phone number allocation. This may have an effect as the larger the allocated number range is, the more likely nearby numbers would be used by real users and be registered for telemarketing. A possibility is that, telemarketers would then target the whole range. Table I shows that in Germany our honeypot is part of a much smaller allocated number range compared to other countries.

[1] www.voxbone.com

TABLE I. GEOGRAPHICAL AREA, SIZE AND DATE OF THE ALLOCATED NUMBER RANGE THAT CONTAINS OUR HONEYPOT NUMBERS. DATA WAS OBTAINED FROM REGULATOR'S DECISIONS DOCUMENTS OR HTTPS://WWW.WHITEPAGES.COM.

Country	City	Allocated block size	Allocation date by the regulator
Luxembourg	Luxembourg	10.000	>2011
Belgium	Ghent	10.000	2007
UK	Leeds	10.000	2007
Italy	Florence	N/A	2010
Germany	Stuttgart	1.000	N/A
France	Nimes	10.000	2010
Netherlands	Tilburg	10.000	N/A
Spain	Toledo	10.000	N/A

A. Do-Not-Call List Experiment

The clean phone numbers in our honeypot were not advertised (seeded) in any way, however, in 6 of the 8 countries (except Italy and Luxembourg), we registered 10 randomly chosen phone numbers to the Do-Not-Call (DNC) lists of the corresponding countries. Registration dates were from January 16 to 21, 2015[2].

The aim of this experiment is twofold. First, we want to see if registering to DNC lists work as intended (i.e., reduces the number of spam calls), and second, we want to see if DNC lists are abused by fraudsters as 'calling lists'. As our numbers are clean, we can observe the abuse of DNC lists with higher confidence, because we avoid most of the noisy spam calls that are not related to DNC list registration. We will discuss this experiment and results in Section IV.

III. OVERVIEW OF COLLECTED CALLS

From January 2015 to March 2018, our honeypot received 2770 calls to 800 numbers. However, some of these calls were possibly misdials, as also observed in [18], [35]. We assume that, if a source number has called only a single destination number (during the lifetime of the honeypot), but the calls occur multiple times in the same day, these calls are likely to be misdials from genuine users who repeatedly try to reach the callee. Eliminating those leaves us with 1978 calls, where 55 of them have anonymized caller IDs.

As seen in Table II, our honeypot did not receive a large number of spam calls, probably because it is a small honeypot only made of clean numbers. However, distribution of calls over the week look similar to previous studies [35], [45], concentrated on working days and hours (Figure 1). Moreover, we notice large scale spam campaigns in Spain and in the United Kingdom, as we will discuss next.

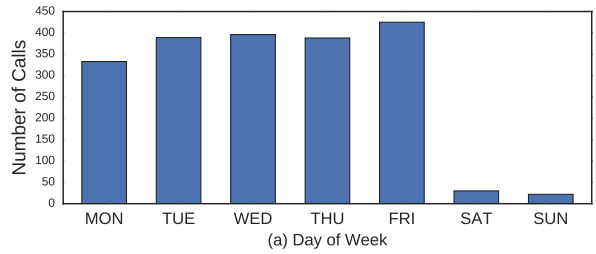
A. Observations on two spam campaigns captured by honeypot

1) Spain: The calls we received from Spain were initiated from 122 distinct source numbers to 95 honeypot numbers. However, most of the source numbers (97) actually generated less than 10 calls. On the other hand, 2 source numbers were responsible for the 20% of the calls. These were landline numbers from Balearic Islands and belong to the same number range except the last 2 digits. Moreover, our honeypot has

[2] In France, our numbers remained registered to the DNC list ('Pacitel') only until February 2016, due to the introduction of a new DNC list ('Bloctel') on this date.

TABLE II. NUMBER OF CALLS RECEIVED BY THE HONEYPOT PER COUNTRY.

Country	Number of calls received	Ratio of domestic calls	Ratio of calls with same area code
Germany	3	100%	0%
Italy	14	78%	0%
Netherlands	33	60%	0%
Luxembourg	59	36%	0%
France	73	77%	3%
Belgium	162	72%	25%
United Kingdom	216	96%	82%
Spain	1418	99%	1%



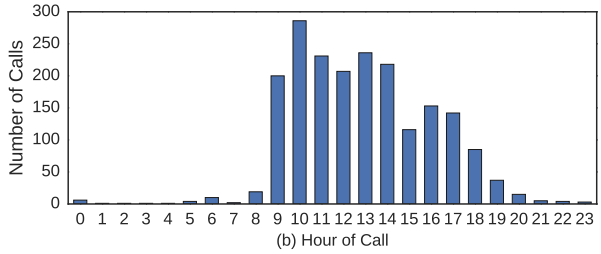


Fig. 1. Day and time information for all received calls. (Calls in each country are considered in their corresponding time zone.)

received calls from these numbers for more than two years (since June 2015). While the originating numbers may be spoofed, the fact that the same numbers have been used for such a long period strongly indicates that those calls belong to the same call campaign.

The voice call graph of these two source numbers (Figure 2) shows that most of their target destinations were in common. As another interesting finding, all the calls were terminated either on the 6th or the 7th second of the 12-second ringing period. By looking up the numbers on the online complaint websites[3], we found many fraud complaints, which indeed mention one-ring calls and silent calls.

As the source numbers are domestic and do not belong to premium rate number ranges, these calls are not likely to aim for callback scams [44]. However, it is possible that the spammers are scanning certain number ranges to identify the phone numbers that are currently in use. This information can, for example, be used to create target lists for scam calls, or to determine which domestic number ranges are unused and can be abused for international revenue share fraud [44].

2) United Kingdom: In the United Kingdom, we observe a 2-week call campaign (07/24/2015 to 08/06/2015) where a single source number made 174 calls to 40 honeypot numbers (on average 4.3 calls per number). This source number share

[3]such as http://stopting.es, www.responderono.es, www.guiatelefonicainversa.es

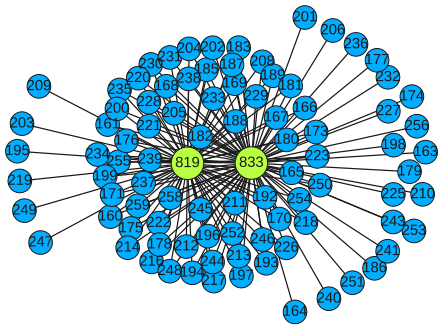


Fig. 2. Voice call graph of a spam campaign observed in Spain. The two green nodes represent the source numbers, blue nodes represent the honeypot numbers. Node labels represent the last 3 digits of the respective phone number.

the same area code with the honeypot numbers, which is a common technique used by spammers to increase the probability of the call to be answered [14], [16], [17], [23]. We also found online complaints about this source number in the same time frame, such as [12]:

> Advertisement asking if you're the homeowner [...] in reality they're claiming to be a electrical company asking you to pay a delayed bill completely fake do not answer or call back

We then check the owner of the source number [40] and find out that the company provides phone services for banking, insurance, health and other professional services. As our honeypot numbers were not assigned to any user, and thus cannot be registered to any business or telemarketing list, these calls are indeed very likely to be abusive.

IV. THE DNC LIST EXPERIMENT

As our honeypot received only a small number of calls, our DNC list experiment did not yield statistically significant results in most of the countries, except in in Spain[4] and UK[5] where we observe that DNC list numbers receive significantly lower number of calls. However, in the United Kingdom, we also observed a case where the DNC list was abused and there were calls specifically to the numbers we registered to it.

A. *Effectiveness of DNC lists*

Table III shows the statistics for calls that are received by DNC list and non-DNC list numbers in Spain and UK. Performing a t-test on the statistics shows that there is a statistically significant difference between the amount of calls received by these group of numbers (for the significance level of 0.05, $p < 0.0001$ and $p = 0.0079$ for Spain and UK[6] respectively). In fact, in Spain, 5 honeypot numbers that have never received any calls, were among the DNC list numbers.

[4]Lista Robinson, www.listarobinson.es

[5]Telephone Preference Service, www.tpsonline.org.uk

[6]In this t-test, we exclude the abuse event observed in the UK (Table IV).

TABLE III. EFFECTIVENESS OF DNC LISTS IN SPAIN AND UK.

	Avg # of calls to numbers and (95% Confidence Interval)	
	in DNC list	not in DNC list
Spain	0.9 (±0.8)	15.5 (±0.6)
UK	1.6 (±0.3)	2.1 (±0.4)
UK (excl. event from Table IV)	0.2 (±0.2)	″

B. Abuse of DNC list in the UK

In the United Kingdom, we registered 10 randomly chosen honeypot numbers to the Do Not Call list on January 16, 2015. Approximately 2,5 years later (on July 7, 2017), we observed a sequence of consecutive calls targeting all those numbers in order (but none of the numbers that were not registered) in an half an hour period. As the numbers registered in DNC list were randomly selected, a coincidence is highly unlikely (both probabilistically, and in terms of being a simple number range scanning attempt). Note that, except single calls to 2 of the phone numbers, these honeypot numbers did not receive any calls previously. Moreover, during this half-hour period, there was no other call to the rest of the 90 numbers.

As shown in Table IV, all the calls were ringing for a maximum of 2 seconds and were only separated by a few minutes from each other. Moreover, 4 months after from this incident, another batch of calls were made to a subset of the DNC list numbers.

An interesting observation is that, the calls originate from different caller IDs (7 unique caller IDs in total). However, all the caller IDs belong to the allocated ranges of the same telecom operator [40]. It is possible that the spammers use multiple caller IDs (and maybe caller ID spoofing) to reduce the number of complaints (from DNC list subscribers) per source number in an attempt to avoid attracting the attention of the regulator [37].

These calls may also intend to identify active phone numbers (i.e., assigned to a user). Again, we found several online complaints[7] about the originating numbers, reporting missed calls and silent calls, especially in the early morning hours. In fact, some users were not able to make sense of the calls, for instance, one user states the following[8]:

> Has called a few times at 5am, but why, I'm not going to buy anything at that time, is it a faked Caller ID who hasn't bothered to check the actual time in the UK?

Such ping calls are very difficult evade since the fraudsters can use autodialers and VoIP technology to generate large number of calls with very small cost [46]. Moreover, they can spoof the caller ID to avoid detection [43].

Although our experiment only provides anectodal evidence on the abuse of DNC lists, there are several factors that relate to the DNC list implementations, which may prepare the ground for such abuses. In fact, from a fraudster's point of view DNC list numbers are interesting, as users may not expect to be a victim of fraud, or may be less accustomed to it, and they may have a higher likelihood of calling back.

[7]From websites such as www.tellows.co.uk, http://findwhocallsyou.com, www.shouldianswer.co.uk.

[8]Comment collected from digcaller.co.uk.

TABLE IV. SEQUENTIAL CALLS RECEIVED BY THE HONEYPOT NUMBERS THAT WERE REGISTERED TO THE DO NOT CALL LIST.

Date	Caller ID	Honeypot number	Ring dur. (seconds)
07/07/2017 06:19:35	44124XX29132	44113XXXX563	2
07/07/2017 06:23:02	44162XX70017	44113XXXX576	0
07/07/2017 06:26:26	44190XX90242	44113XXXX581	0
07/07/2017 06:29:59	44161XX80876	44113XXXX589	2
07/07/2017 06:33:13	44120XX65019	44113XXXX601	1
07/07/2017 06:36:43	44208XX91314	44113XXXX613	1
07/07/2017 06:40:29	44208XX91314	44113XXXX623	0
07/07/2017 06:43:58	44208XX91314	44113XXXX637	0
07/07/2017 06:47:10	44124XX29132	44113XXXX645	1
07/07/2017 06:50:30	44124XX29132	44113XXXX654	1
11/09/2017 16:25:23	44208XX91314	44113XXXX563	0
11/09/2017 16:27:50	44190XX90242	44113XXXX589	0
11/09/2017 16:32:20	44208XX53765	44113XXXX645	0
11/09/2017 16:33:08	44124XX29132	44113XXXX654	0

In the next section, we will analyze the implementation challenges of DNC lists, and compare the practices employed in several European countries.

V. ANALYSIS OF NATIONAL DO-NOT-CALL LIST PRACTICES

Consumers tend to have a number of expectations from national DNC lists. For instance, they often think that the list is maintained by the government, and registering to the list will protect them from all types of unwanted calls. Another common misconception is that the DNC list provides a system to block calls, whereas it's just a list of numbers that telemarketers should refrain from calling. Thus, DNC list implementations may not always match the expectations of the consumers, especially if the implementation details are not clearly understood.

Some of the design choices that need to be considered while establishing a national DNC list are:

- **List maintainer:** The national DNC lists are often enforced by government's regulatory bodies, however, they may not always be maintained by the same entity. Instead the maintenance of the list can be assigned to an independent organization (which may have commercial interests), or to a non-profit third party.
- **Coverage of the list:** As we mentioned earlier, DNC lists cannot prevent all unwanted calls, as the illegitimate parties will ignore them anyway. However, there are usually further restrictions on the coverage of DNC lists.
- **Access to the list:** Often, users subscribing to the DNC list are requested to give various personal information such as name, home address and email, in addition to the phone numbers. As all this information is stored in the DNC list, distribution of the list therefore becomes a sensitive issue. In many countries, telemarketing companies are allowed to download the whole DNC list, for a few thousand Euros per year. On the other hand, some countries employ the 'list washing' technique [25], where telemarketers send their phone number lists and the DNC list maintainer cleans (or highlights) the numbers that should not be called.
- **Membership renewal:** DNC lists may require the renewal of membership periodically, or make the registration permanent (unless the user explicitly removes the number from the list).

TABLE V. COMPARISON OF DNC LIST PRACTICES IN SIX EUROPEAN COUNTRIES.

	Coverage	Maintainer	Distribution of the list	Time to take effect	Membership renewal
United Kingdom [9]	Direct and live telemarketing calls	Private sector, enforced by regulator	Download	28 day	Not required
Spain [6]	Commercial communications	Private sector, enforced by data protection agency	Download	3 months	Not required
France [1]	Calls intended to offer or sell a product	Private sector, enforced by regulator	List washing	Within 1 month	Every 3 years
Belgium [5]	B2B and B2C telemarketing	Private sector, enforced by government	Download	5 working days	Not required
Germany [3]	Unwanted advertising	Non profit organization based on federal data protection act	List washing	N/A	Not required
Netherlands [4]	Commercial, ideological or charity calls	A third party organization	Download	6 weeks	Not required
USA [7]	Sales calls (incl. robocalling)	Federal consumer protection bureau	Download	31 days	Not required
Canada [2]	Telemarketing calls (incl. robocalling)	Private sector, enforced by regulator	Download	31 days	Not required

- **Time to take effect:** Depending on how frequent the telemarketers receive the DNC list updates (or has to "wash" the list), a user may need to wait for a certain time before his registration takes effect.
- **Penalty on violation:** Violation of the DNC list usually results in a penalty to be imposed on the company. However, regulators may not always deal with all the consumer complaints they receive about DNC violations. Moreover, it is often difficult to identify the bad actors from user complaints. Even when they are identified, the penalties may not be enough to deter them from calling the DNC list numbers.

Table V gives an overview of the different DNC list implementations around Europe, and also in the US and Canada for comparison. First, we can see that most of the DNC lists (except in Netherlands) only protect against commercial telemarketing calls, excluding opinion surveys, donation calls and market research. Moreover, in the UK, the coverage is only limited to live telemarketing calls, while robocalls that deliver prerecorded messages are not included. On the other hand in Belgium, business phone numbers are also allowed to be registered to the DNC list.

Second, in most of the countries DNC lists are maintained by private sector (usually by an organization called the 'digital marketing association', an association of telemarketing companies), although regulatory bodies handle the consumer complaints and the legal enforcement of the list. However, there may always be a conflict of interest between such marketing associations and regulators [15], [26], which may decrease the effectiveness of DNC lists. In addition, as the regulatory body may not be able to process all the consumer complaints, there is often a gap between complaints and lawsuits, and consumers may find the complaint process inefficient [33].

Another common practice is to make DNC lists downloadable by telemarketing companies. This practice could put consumers' privacy at risk, as the lists often also include additional information about consumers. The DNC list regulations usually state that the disclosure or sale of the list to external parties are not allowed [11]. However, this may be very difficult to detect and prevent, if the lists are downloadable by third parties. While the second option, list washing, seems to be a better alternative to provide access to the DNC list, it can still be abused. For instance, a company with a very large target phone number list may abuse the list washing process to actually identify the DNC list numbers.

Overall, we believe that careful consideration of these issues may help to improve consumers' DNC list experience, and reduce possible abuses like the one we observed in our honeypot. Moreover, employing telephony honeypots to observe the calls received by DNC list numbers may help the regulators notice significant violations in a faster way, and to take action before waiting for consumer complaints.

VI. RELATED WORK

Telephony honeypots have been frequently used to observe and better understand the voice spam landscape. Gupta et al. uses a no interaction honeypot located in the US, which received 1.3 million calls from 250K source numbers to 39K honeypot numbers over 7 weeks [35]. The calls are not answered, but directly terminated with a busy tone. As the honeypot uses 'dirty' numbers, seeding of the numbers is not required. By correlating the source numbers with other complaint datasets, authors identify and analyze calling patterns of different spam types. They also find that the number blocks that have been allocated for a longer duration receive more spam calls compared to the newly allocated blocks. Another work [18] uses a mobile phone honeypot that received hundreds of fraudulent SMS and phone calls over 7 months. The honeypot is located in China and uses 8 mobile phone numbers from various operators. The numbers are seeded in different ways (via publishing them on social networks, using them with the phones that installed mobile malware known to leak data, and calling phone numbers that are known to be abusive) to compare the efficiency of seeding techniques. Finally, Sahin et al. analyzes the use of chatbots as high interaction honeypots to fight against voice spam [45].

In addition to the honeypot based studies, Tu et al. [46] presents a taxonomy of existing voice spam countermeasures and evaluates them. In [38], authors aim to reveal the techniques used by technical support scammers, by analyzing the phishing websites and interacting with the scammers on the phone. A more recent study analyzes the effectiveness of phone number blacklists that are used by various smartphone applications [41]. Authors find that more than 55% of spam calls in the United States can be prevented by using such blacklists.

On the other hand, our study focuses on the effectiveness of National Do-Not-Call lists that are enforced by regulations.

Our honeypot is also different in the sense that it contains only *clean* phone numbers (as opposed to *dirty*), and it covers 8 European countries (instead of targeting a single country), which allows the comparison of different DNC list practices.

Finally, few studies focus on the factors that affect people's decision in signing up for DNC lists. Varian et al. analyze the demographic patterns of consumers signing up for the national DNC list in the US [47], [48]. Authors find that large households have lower sign-up frequency, whereas households with higher income and education level have higher registration rates. Their study also estimates the economic benefits of the DNC list for consumers, and it concludes that the popularity of DNC list will critically depend on how it is implemented and enforced. A similar study [49] follows up with a larger dataset of DNC list registrations. It shows that the demand for DNC registration increases in regions that have higher heterogeneity in ethnicity, education and religion.

VII. Conclusion

In this paper we studied the effectiveness of the Do Not Call lists, in particular using the data from a 3 year long honeypot deployment with phone numbers from 8 European countries. We reported both positive effects (reduced spam calls) as well as abuses (DNC list used to target calls). We then compare the DNC list implementations among those countries. We believe that repeating this experiment on a larger scale might be an interesting future work. In particular, a larger honeypot with both dirty and clean phone numbers would allow to better compare the telephony abuse targeting all numbers. Also, registering more honeypot numbers, and in particular dirty numbers, to the DNC lists would allow to better evaluate DNC list effectiveness.

VIII. Acknowledgements

This work was partially supported by the Principality of Monaco. We would like to thank Payas Gupta and Mustaque Ahamad for the interesting discussions on the topic. We also thank Voxbone (in particular via Anne-Valerie Heuschen and Laurent Jarbinet) for their collaboration on the honeypot setup. Finally, we thank the anonymous reviewers for their constructive comments and feedback.

References

[1] Bloctel. http://www.bloctel.gouv.fr/.

[2] Canada's National Do Not Call List. https://www.lnnte-dncl.gc.ca/en.

[3] Deutschen Robinsonlisten. https://www.robinsonliste.de.

[4] Het wettelijke Bel-me-niet Register. https://www.bel-me-niet.nl/.

[5] La liste Ne m'appelez plus. https://www.ne-m-appelez-plus.be.

[6] Listas Robinson. https://www.listarobinson.es.

[7] National Do Not Call Registry. https://www.donotcall.gov/.

[8] New TPS Protect App. http://www.tpsonline.org.uk/tps/tps_protect.html.

[9] Telephone Preference Service. http://www.tpsonline.org.uk/tps/index.html.

[10] South africa: Dmasa Do Not Call database leaked. https://www.databreaches.net/south-africa-dmasa-do-not-call-database-leaked-repost/, Jun 2011.

[11] CRTC Unsolicited Telecommunications Rules. http://www.crtc.gc.ca/eng/trules-reglest.htm, March 2014.

[12] who-called.co.uk, August 2015.

[13] Do not sign up to Do Not Call registry! https://800notes.com/forum/ta-db478a8fed34069/do-not-sign-up-to-do-not-call-registry, Jan 2016.

[14] Getting spam calls from numbers similar to my own. https://security.stackexchange.com/, Feb 2016.

[15] Firms face ruin as Ofcom rejects zero tolerance fears. dma.org.uk, JANUARY 2017.

[16] Scam calls from local phone numbers. https://fraudpreventionunit.org/, March 2017.

[17] B.-J. ANTEOLA. Getting calls from numbers that look like yours? It's possibly a scam and here's why. http://www.fresnobee.com/, September 2017.

[18] M. Balduzzi, P. Gupta, L. Gu, D. Gao, and M. Ahamad. Mobipot: Understanding mobile telephony threats with honeycards. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16. ACM, 2016.

[19] C. Brosset and G. Caret. Le demarchage telephonique et vous. available at: https://www.quechoisir.org, January 2017.

[20] A. Burlacu. AT&T starts robocalls crackdown with Call Protect service to block spam phone calls: How it works. available at: http://www.techtimes.com, December 2016.

[21] Canadian Radio-television and Telecommunications Commission. Report on the Operation of the National Do Not Call List for the period April 1, 2013 to March 31, 2014. https://www.crtc.gc.ca/eng/dncl/rpt140930.pdf, September 2014.

[22] CBC News. Bell fined $1.3M for breaking do-not-call rules. http://www.cbc.ca/news/business/bell-fined-1-3m-for-breaking-do-not-call-rules-1.960118, December 2010.

[23] A. Chang. Familiar-Looking Numbers Are The Latest Twist In Robocalls. https://www.npr.org/, July 2017.

[24] A. Condomines. Bloctel, la liste anti-démarcharge téléphonique du gouvernement, gérée par des entreprises de démarchage. https://www.lci.fr/, Jun 2016.

[25] C. Connolly and A. Vierboom. Emerging Best Practice in Do Not Call Registers. http://www.galexia.com/public/research/assets/do_not_call_best_practice_2009/do_not_call_best_practice_2009.pdf, August 2009.

[26] DMA. Ofcom refuses to interpret abandoned calls legislation. dma.org.uk, Feb 2017.

[27] A. Farnham. Fighting telemarketers: When Do-Not-Call list fails, these strategies work. http://abcnews.go.com/Business/best-ways-turn-tables-telemarketers/story?id=21534413, January 2014.

[28] Federal Communications Commission. FCC robocall and caller ID spoofing workshop, Sept 2015. Video recording available at https://www.fcc.gov/events/workshop-focus-robocall-blocking-and-caller-id-spoofing.

[29] Federal Trade Commission. Consumer Sentinel Network Reports. available at: https://www.ftc.gov/enforcement/consumer-sentinel-network/reports, 2008 to 2015.

[30] Federal Trade Commission. Robocalls: Humanity strikes back, 2015. Available at https://www.ftc.gov/news-events/contests/robocalls-humanity-strikes-back.

[31] Federal Trade Commission. Enforcement of the Do Not Call Registry. https://www.ftc.gov/news-events/media-resources/do-not-call-registry/enforcement, 2018.

[32] C. Fredman. How robocalls scam the Do Not Call list. https://www.consumerreports.org/cro/news/2015/04/how-robocalls-scam-the-do-not-call-list/index.htm, April 2015.

[33] J. Graye. Télémarketing: la liste "Ne m'appelez plus" est-elle efficace? www.rtbf.be, Feb 2017.

[34] P. Gupta, M. Ahamad, J. Curtis, V. Balasubramaniyan, and A. Bobotek. M3AAWG Telephony Honeypots: Benefits and Deployment Options, 2014.

[35] P. Gupta, B. Srinivasan, V. Balasubramaniyan, and M. Ahamad. Phoneypot: Data-driven understanding of telephony threats. In *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2014*, 2015.

[36] K. F. Kok. Truecaller insights special report. available at: https://blog.truecaller.com/2017/04/19/truecaller-us-spam-report-2017/, April 2017.

[37] S. Ladurantaye and S. Houpt. CRTC fines Indian telemarketers for violating call list. www.theglobeandmail.com/, MARCH 2017.

[38] N. Miramirkhani, O. Starov, and N. Nikiforakis. Dial one for scam: A large-scale analysis of technical support scams. In *NDSS*, 2017.

[39] C. Miranda. A versatile way to get around the Do Not Call list. https://www.consumer.ftc.gov/blog/2014/03/versatile-way-get-around-do-not-call-list, March 2014.

[40] Ofcom. Ofcom numbering site. http://static.ofcom.org.uk/static/numbering/index.htm, January 2018.

[41] S. Pandit, R. Perdisci, M. Ahamad, and P. Gupta. Towards measuring the effectiveness of telephony blacklists. In *Network and Distributed System Security Symposium, NDSS*, 2018.

[42] Quechoisir. Enquete démarchage téléphonique. https://www.quechoisir.org, January 2017.

[43] B. Reaves, L. Blue, H. Abdullah, L. Vargas, P. Traynor, and T. Shrimpton. Authenticall: Efficient identity and content authentication for phone calls. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 575–592, Vancouver, BC, 2017. USENIX Association.

[44] M. Sahin, A. Francillon, P. Gupta, and M. Ahamad. Sok: Fraud in telephony networks. In *Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P'17)*, EuroS&P'17. IEEE, April 2017.

[45] M. Sahin, M. Relieu, and A. Francillon. Using chatbots against voice spam: Analyzing lenny's effectiveness. In *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, SOUPS'17. USENIX, July 2017.

[46] H. Tu, A. Doupé, Z. Zhao, and G.-J. Ahn. SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam. In *Proceedings of the 37th IEEE Symposium on Security and Privacy*, May 2016.

[47] H. Varian, F. Wallenberg, and G. Woroch. Who signed up for the do-not-call list? 2004.

[48] H. Varian, F. Wallenberg, and G. Woroch. The demographics of the do-not-call list [security of data]. *IEEE Security Privacy*, 3(1):34–39, Jan 2005.

[49] K. Yong Goh, K.-L. Hui, and I. Png. Consumer heterogeneity, privacy, and personalization: Evidence from the do-not-call registry. October 2009.