

## **Re: Written comments on Consultation Paper on Review of Telecom UCC Regulations**

We are enclosing our written submission in regard to the Consultation Paper on Review of Telecom Unsolicited Commercial Communications dated 11<sup>th</sup> May 2010.

While there are no two views that Unsolicited Commercial Communications cause a high level of irritation and hence must be controlled, it is necessary to differentiate between (i) voice calls handled by human beings and (ii) other types of Unsolicited Commercial Communications calls which do not require a human intervention from the telemarketer. Globally, most, if not all, countries make this differentiation and have separate rules for them. It is possible, that by clubbing the two together in India, the rules have become ineffective and hence there is need to segregate the two and mandate rules etc separately for them.

It is known and accepted that there are a substantial number of telemarketers who have not registered with DoT including Direct Sales Agents (DSAs) and that a large number of Unsolicited Commercial Communications calls are made by these entities. However, no effort appears to have been made to bring such telemarketers under the umbrella of registration – thereby ensuring that they are made to follow laid down rules and regulations. The crux of the matter is that some telemarketers are “breaking the law” by either not registering themselves or not scrubbing their calling lists as required.

Additionally, unless sequential dialling is stopped, no amount of rules and regulations will be able to curb Unsolicited Commercial Communications. Sequential dialling also results in calls being routed to classified numbers, unlisted numbers, emergency lines etc, which is totally avoidable.

A Survey indicates that a vast majority (as stated in TRAI's Consultation paper) of customers do not want to receive Unsolicited Commercial Communications. However, a very small proportion of customers have actually signed on to the NDNC Registry, less than 11% of subscribers. Hence, an effort should be made to ascertain why is it that the vast majority of customers do not wish to receive Unsolicited Commercial Communications but the number of subscribers who have registered themselves on NDNC is very small. This is despite publicity given to NDNC and simplifying the process for registration.

The solution for addressing the malaise of Unsolicited Commercial Communications is not by curtailing the entrepreneurial spirit and commercial enterprise as well as job creation opportunities but to have more effective and rigorous implementation of the rules and penalties. Taking such a step as is being envisaged, by mandating opt-in for all Unsolicited Commercial Communications is akin to throwing the baby out with the bath-water. This will sound the death knell of the voice based telemarketing industry in India.

It also needs to be mentioned that the domestic voice based telemarketing industry directly employs approx 2 lakh people and an even larger number indirectly; hence curtailing the growth of this industry would severely impact job creation. This is at a stage when the

industry is likely to witness good growth prospects. Job creation in this segment will continue to be linear i.e., jobs will rise in direct proportion to the increase in business.

Finally, options should be explored to make NDNC a self sustaining effort as it is in the US. We advocate stronger enforcement of regulations to control Unsolicited Commercial Communications. At the same time it is also imperative that, like in most countries in the world different laws and controls be made applicable to Unsolicited Commercial Communications that are voice based (which have a human being handling the call from a telemarketer) and those that are not voice based.

Thanking you,

Yours faithfully,

R Bhatnagar  
Vice President

## **Written submission in regard to The Consultation Paper on Review of Telecom Unsolicited Commercial Communications dated 11<sup>th</sup> May 2010.**

There is no doubt that any reference to Unsolicited Commercial Communications in the Indian context raises strong emotions and there is near unanimity that these should be stopped forthwith.

Intuitively it appears that the opt-in option is better at controlling the unwanted communication that is received by subscribers. However, there is very little data or information to support this approach i.e., opt-in would be a better alternative to the currently followed opt-out process. Further no country has actually moved on to an opt-in approach for voice calls which have a human being handling the call. Hardly any empirical studies have been done to test out this hypothesis. We have, however, identified one study carried out in the US in this direction by

- **Prof. Michael Staten**, Distinguished Professor and Director of the Credit Research Centre, The Robert Emmett McDonough School of Business, Georgetown University; and
- **Prof. Fred Cate**, Distinguished Professor and Ira C. Batman Faculty Fellow, Indiana University School of Law-Bloomington and Senior Policy Advisor, Hunton & Williams Centre for Information Privacy Leadership

The study examines the impact of opt-in on MBNA Corporation, a diversified, multinational financial institution. The authors demonstrate that opt-in would

- raise account acquisition costs,
- lower profits,
- reduce the supply of credit,
- raise credit card prices,
- generate more offers to uninterested or unqualified consumers,
- raise the number of missed opportunities for qualified consumers, and
- impair efforts to prevent fraud.

**Excerpts from this study are enclosed in the Annexure to this representation.**

However, three fundamental aspects which are overlooked in this emotionally charged argument where levels of irritation consequent to frequent telemarketing calls are taking the shape of forcing a significant scaling down, if not a complete shut-down, of telemarketing centres. These aspects are listed below as items 1, 2 and 3. Additionally this submission contains two more sections (listed below as items 4 and 5)

1. Globally no country uses opt-in for voice calls.
2. Regulations exist in India but the enforcement is poor to non-existent
3. Telemarketing activity (voice based calls) creates considerable job opportunities specially for the economically weaker sections of society
4. Specific aspects contained in TRAI Consultation Paper on which we have a variance of views
5. Annexure with extracts from study conducted in the US referred to above

These aspects are explored below.

### **1. Globally no country uses opt-in for voice calls.**

Most, if not all, countries have made a clear distinction between Unsolicited Commercial Communications handled by human beings and Unsolicited Commercial Communications handled in an automated manner.

The appended table highlights the existing scenario in various countries

*(Text of relevant provisions has been made bold and in Red font with the intent to highlight the focus of the directives / legislative intent / broad approach adopted by that country)*

Name of Country / Geographical Area + Summary of system followed (specially for voice based calls)	Relevant provisions for Unsolicited Commercial Communications  Or  Summary of what the legislative intent states in individual countries
<b>Australia</b>  Follows a Do Not Call Registry System	<b>The Do Not Call Register Act, 2006</b> covers the scope of the Do Not Call Register in Australia and also provides for penalties etc to be imposed by the civil courts. An independent authority (Australia Communications and Media Authority) manages the DNC Registry and enforces the Act, mentioned above. Telemarketers are also allowed to contact persons who are on the DNC Register but fall under the category of “Inferred Consent” – where a telemarketer believes that the person would be willing to receive a telemarketing call.
<b>Canada</b>  Follows a Do Not Call Registry System	Rules have been laid down by the Canadian Radio-Television and Telecommunications Commission (CRTC) for controlling telemarketing calls. These rules are called National Do Not Call List Rules – The Telemarketing Rules and Automatic Dialling-Announcing Device (ADAD) Rules.
<b>China</b>  Only internet and email services are regulated. Does not cover voice calls or fax	The Regulations on Internet E-Mail Services aims to regulate Internet email services and to protect end-users. <i>No commercial emails can be sent without prior consent from the recipients.</i> Voice calls are not covered by this legislation at all.
<b>Egypt</b>  No mandated Do Not Call Registry, but individual can opt – out by telling the telemarketer	There are no separate laws dealing with Unsolicited Commercial Communications or telemarketing calls. The process followed is that when a User receives a call from a telemarketer, he can ask the company to take him off the calling list. In effect telemarketing calls can be made to anybody. However, an individual can opt-out by telling the telemarketing company that he does not wish to receive such telemarketing calls.
<b>European Union</b>  Follows a Do Not Call Registry System for voice based calls  Extracts from relevant Acts / provisions have been indicated alongside.  Opt – in (equivalent of a Do call Registry) is used <b>only</b> for messages emanating from automated calling machines, telefaxes and e-mail including SMS / MMS messages	Directive 2002 / 58 / EC; <i>Recital (40): Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes and e-mail including SMS messages. .... For such form of unsolicited communications for direct marketing, it is justified to require that prior consent of the recipients is obtained before such communications are addressed to them.</i>  Article 13 – Unsolicited Communications <i>Para 1: The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. (amendment 131 of the Parliament provides clarification that MMS and similar technologies are covered by the definition of “electronic mail” given in Article 2 (h))</i>  e Privacy Directive requires Member States to apply an “opt – in” system as a general rule, to unsolicited communications (or spam) produced by means of <i>automatic calling machines, fax machines and electronic mail (including SMS messages). .... For other types of direct marketing practices, the Member States can choose to apply an opt – in or an opt – out system.</i>
<b>Italy</b>  Follows a Do Not Call Registry System  Opt – in is for non voice interactions like use of automated calling systems etc	Addressed through “Personal Data Protection Code, Legislative Decree No 196” In regard to Unsolicited Communications the Decree states that <i>the use of automated calling systems without human intervention for the purposes of direct marketing or sending advertising materials, or else for carrying out market surveys or interactive business communication shall only be allowed with the subscriber's consent and shall also apply to electronic communications performed by e-mail, facsimile, MMS- or SMS-type messages or other means for the purposes referred to therein.</i>
<b>Japan</b>	Only emails sent for advertisement purposes are covered by laws. This law

<b>Only emails covered</b>	controls spam disseminated by senders. Other types of Unsolicited Commercial Communications are not covered by any specific law.
<b>New Zealand</b>	New Zealand has the Unsolicited Electronic Messages Act 2007, which deals all with electronic messages except voice call and Fax. It mandates that all commercial electronic messages must contain functional unsubscribe facility. For telemarketing calls currently reliance is on a voluntary code of practice, promoted by the New Zealand Direct Marketing Association.
<b>Covers only electronic messages. Does not cover voice calls or fax</b>	
<b>Pakistan</b>	Controlled by the Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communications Regulation, 2009.
<b>Follows a Do Not Call Registry System</b>	Operators are required to establish standard operating procedures to control spamming, to control fraudulent communications and to control unsolicited calls and ensure registration of Telemarketers. Operators are also required to maintain a Do Not Call Registry (DNCR) to incorporate all registered Telemarketers and to provide access to registered Telemarketers to the central DNCR maintained by the operators.
<b>South Africa</b>	Mainly governed by the Electronic Communications and Transactions Act (ECTA) among other aspects this states that <i>any person who sends Unsolicited Commercial Communications to consumers must provide the consumer with the option to cancel his or her subscription to the mailing list of that person. The ECTA leaves it to the recipient to opt to cancel communication of unsolicited communication.</i>
<b>No mandated Do Not Call Registry, but mail etc must provide an option to opt – out</b>	
<b>U S A</b>	The Telephone Consumer Protection Act of 1991 (TCPA) authorised Federal Communication Commission (FCC) to establish and operate a single national data base listing telephone numbers of residential subscribers who object to receiving telephone solicitation. In December, 2002 the Federal Trade Commission (FTC) went beyond the FCC's company specific approach in dealing with Unsolicited Commercial Communications and <i>adopted a National Do Not Call Registry based on authority granted to the FTC under the 1994 Telemarketing Consumer Fraud and Abuse Prevention Act .</i> The penal provisions in the US are stringent and even carriers (service providers) are penalised. Penalties for telemarketers for service providers are USD 120,000 per violation (capped at USD 1.2 Million) and for others including telemarketers penalty is USD 11,000 per violation (capped at USD 87,500)
<b>Follows a Do Not Call Registry System</b>	
Service providers face larger and stiffer penalties for violations by telemarketers	
<b>United Kingdom</b>	The Privacy and Electronic Communications (EC Directive) Regulations 2003 ( <i>mentioned above under EU</i> ) provide the legal framework for controlling Unsolicited Commercial Communications. The UK Government's Office of Communications (Ofcom) is responsible for maintaining and keeping up-to-date the <i>Registers to be kept for opting – out by consumers from receiving unsolicited communications for direct marketing by means of facsimile machine and public electronic communications service.</i> <i>Those who want to market by text, picture and video message do not need to screen against the Telephone Preference Service (TPS), but they need to get prior consent of the customer before sending such messages i.e., opt – in for getting such messages.</i> TPS is the Do Not Call Register for individuals.
<b>Follows a Do Not Call Registry System</b>	
DNC applies only to direct marketing messages from fax machines and public electronic communications services	

Most countries where Unsolicited Commercial Communications are commonly used have the following additional aspects

- Communication (voice or non voice) must contain a toll free number at which the sender (not the telemarketer) can be contacted
- Time windows between which such communication (voice or non voice) can be made. This usually is between 0800 hours and 2000 or 2100 hours. Some additional restrictions are there such that communication (voice or non voice) is not made on declared public holidays
- Sequential dialling is not permitted, since this bypasses the DNC requirements completely.
- Pre-recorded calls making a marketing pitch are also not allowed since they are not classified as voice calls.

## **2. Regulations exist in India but the enforcement is poor to non existent**

### **Overview**

In India Unsolicited Commercial Communications is a generic term used collectively to cover all types of interactions like unsolicited calls (including live voice calls and canned / recorded messages), SMS, MMS, etc., whereas voice calls and non voice messages comprising Unsolicited Commercial Communications are categorised separately in most, if not all, other countries

Current definition of Unsolicited Commercial Calls in India

*“any message through telecommunication service, which is transmitted for the purpose of informing about or soliciting or promoting any commercial transaction in relation to goods, investment or services which a subscriber opts not to receive, but does not include, -*

- (i) Any message (other than promotional message) relating to a service or financial transaction under a specific contract between the parties; or*
- (ii) Any messages relating to charities, national campaigns or natural calamities transmitted on the directions of the Government or agencies authorised by it for the said purpose;*
- (iii) Messages transmitted, on the directions of the Government or any authority or agency authorised by it, in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality.”*

A literal interpretation (keeping in mind the approach that most countries have taken internationally) would mean that telemarketing applies to messages and not conversations. The difference between a message and a conversation can be briefly states as follows –

- A message is a communication which conveys information etc **but does not allow** the caller and called party to enter into an on line or simultaneous exchange of thoughts or ideas on the information being provided. Each can only communicate in tandem or one at a time i.e., one starts the communication, completes it and then the other starts his or her message. Such messages could encompass several types like; SMS, MMS, email, Fax, recorded message playback by automated calling machines etc
- A conversation, on the other hand, is a communication which conveys information etc **but allows** the caller and called party to enter into an on line or simultaneous exchange of thoughts or ideas on the information being provided. Each can communicate simultaneously i.e., one does not have to wait to complete his / her communication – both can exchange information simultaneously

### **Requirement for telemarketers to register**

There is a requirement for all telemarketers to register themselves.

However, it is known and accepted that there are large numbers of telemarketers who provide telemarketing services or perform telemarketing activities but have not registered themselves with DoT including Direct Sales Agents (DSAs). A large number of Unsolicited Commercial Communications calls are made by these entities. However, no sustained effort appears to have been made to bring such telemarketers under the umbrella of registration – thereby ensuring that they are made to follow laid down rules and regulations. The crux of the matter is that such entities are “breaking the law” by either not registering themselves and / or not scrubbing their calling lists as they are required to do.

### **Penalties in regard to telemarketing and ineffective implementation thereof**

*“To discourage the telemarketers who make calls to the numbers registered in Do Not Call List, a provision has been made whereby Rs.500/- shall be payable by the telemarketer to the service provider for every first unsolicited commercial communication (UCC) and Rs.1000/- shall be payable for subsequent UCC. There is a provision for disconnection of the telemarketer telephone number / telecom resource if the UCC is sent even after levy of Rs.500/- & Rs.1000/- tariff. In case of non-compliance to the Telecom Unsolicited Commercial Communications Regulations, 2007, the Service Provider is also liable to pay an amount by way of financial disincentive, not exceeding Rs.5000/- for first non-compliance of the regulation and in case of second or subsequent such non-compliance, an amount not exceeding Rs.20,000/- for each such non-compliance.”*

It is also stated in the TRAI Consultation Paper that

- a. There are a substantial number of telemarketers who have not registered with DoT including Direct Sales Agents (DSAs) and that a large number of Unsolicited Commercial Communications calls are made by these entities.
- b. Service providers are not interested in disconnecting telecom resources of telemarketers as they are generally valued subscribers and pay good revenue to service providers.
- c. The penalties envisaged for violations are nominal. Further, given the importance (from a revenue generation and profitability perspective for the access service provider) it is likely that access service providers may not be keen to help enforce the requirements.
- d. Even if penal action is taken by disconnecting the telecom resource, there is no mechanism to ensure that the “disconnected” telemarketer does not get a fresh connection and restart his telemarketing activities in an unregistered manner, and
- e. While the vast majority of customers do not wish to receive Unsolicited Commercial Communications they have not taken the step to register themselves on the NDNC Registry, thereby reducing the likelihood of their receiving such calls.

It is essential that appropriate steps be taken to identify telemarketers thereby ensuring that they register and are brought within the ambit of existing regulations. Once identified it is likely that it will be easier to get such telemarketers to register. However, apart from giving even more publicity for the NDNC Registry and making it easier for customers to register for it, no structured efforts seem to have been undertaken to ensure that all telemarketers **actually** scrub their calling lists before making outbound calls. As and when penal action by disconnecting telecom services is undertaken, thereafter, a mechanism must be evolved whereby repeat offenders are not able to get fresh telecom connection to continue telemarketing in an unauthorised manner.

If what is stated in the Consultation Paper is correct i.e., “*Service providers are least interested to disconnect telecom resources of telemarketers as they are generally valued subscribers and pay good revenue to service providers*”, very clearly enforcement is lax. Service providers continue to violate existing regulations but appropriate penal action to ensure enforcement does not appear to be taken.

Some mechanism needs to be evolved whereby streamlining of maintenance of lists can be achieved. Some suggestions in this regard are

- Each service provider needs to continue to maintain a DNC list for its subscribers
- Service providers need to continue to provide, maybe on a monthly basis, their updated DNC List to a nodal agency, which compiles and maintains the NDNC.
- Telemarketers should subscribe to this list and be allowed to access it so that they can undertake the scrubbing exercise by themselves and hence be responsible and accountable for any contacts that are made with subscribers whose numbers appear on the NDNC

Some initial suggestions on identifying telemarketers and ensuring that they do not access fresh connections after having been disconnected are as follows

#### **Identification of telemarketers**

It should be possible to create some filters which would enable identification of telemarketing organisations by service providers themselves. Some suggestions in this regard are given below which used in combination could facilitate identification of a greater number of telemarketers –

- Large proportion of outbound calls, maybe around 80 to 85% - threshold would need to be determined
- Large volumes of calls
- Multiple lines are issued – (also true for large organisations but is a feature of telemarketers)
- Large billing proportion per connection (average billing per connection would be uniformly high)
- Service providers could be mandated to recheck subscribers exhibiting such characteristics and if found to be telemarketers, access providers may be empowered by TRAI to insist that they must register themselves as telemarketers
- TRAI or an appropriate body could seek periodical (quarterly or half yearly) confirmation from service providers that they have examined call patterns of their clients and those that have been suspected to be in the telemarketing space have been registered or found not to be involved in telemarketing. Details of such checks can be required to be sent to TRAI / NIC if needed for a data base to be built up.

It may not be desirable to restrict the number of calls being made in order to contain the issue of telemarketing.

#### **Reconnection mechanism to be tightened.**

- Seek details of the company and the promoters / shareholders behind it as well when taking connection for telemarketing or when identified (as mentioned above or by other means) and made to register

- Upon receipt of complaints, the investigation into the complaint (or repeated complaint) must include a check / confirmation that there is a formal process in place ensuring that the telemarketer scrubs their calling lists. This can be done by a check on historical call lists which have already been dialled out.
- Repeated complaints against such telemarketers would result in disconnection of telecom facilities.
- Any such disconnection that is made by the access providers needs to be communicated to TRAI / NIC as need may be. A thought could be given to placing names and details of such violators on TRAI web site so that such information is in the public domain and other service providers may be required to check this list prior to issuing a new telephone connection for purposes of telemarketing.

#### **Making booking of complaints more effective**

A mechanism should be evolved whereby whenever a complaint is lodged there is a unique ticket number generated (this could be unique for each service provider and not across service providers) which is then tracked through till closure. Most telecom service providers use this system for their customer service complaints and hence it should not be too difficult to extend such a system for UCC complaints as well.

It has been suggested, in the Consultation Paper, that both telemarketers and the agency on whose behalf the telemarketer is making calls should be held accountable for making Unsolicited Commercial Communications calls. Options should be considered whereby the entire chain involved in making Unsolicited Commercial Communications calls would come under the scanner for purposes of enforcing regulations. The entire chain here would mean (i) the telemarketer; (ii) the agency on whose behalf the telemarketer is making the call; and (iii) the service provider who is facilitating making of the call. Suitable boundary provisions would need to be drawn such that the negligence on part of one link in the chain does not impinge in an unwarranted manner on another link. Illustratively, if a telemarketer makes a call to a number registered on NDNC, the telemarketer should be penalised and not the service provider, since the service provider would not have any control over such a call being made. However, if the telemarketer is unregistered then it would be logical to extend the penal action, when such Unsolicited Commercial Communications calls are made, to the service provider as well.

#### **Reaching out with renewed vigour to subscribers and understanding their psyche**

A Survey indicates that a vast majority (as stated in TRAI's Consultation paper) of customers do not want to receive Unsolicited Commercial Communications. However, a very small proportion of customers have actually signed on to the NDNC Registry, less than 11% of subscribers. Hence, an effort should be made to ascertain why is it that while the vast majority of customers do not wish to receive Unsolicited Commercial Communications but they haven't made the effort to register themselves on NDNC. This is despite publicity given to NDNC and simplifying the process for registration. Such an analysis might provide insights on how more subscribers (who would like to opt-out) can be made to register on the NDNC.

It has also been stated in the Consultation Paper that many subscribers do not know where and how to register themselves for the NDNC. The solution to this obviously is to give greater publicity and, if possible, further simplify the registration process and of course more effective enforcement against violations / violators.

Several of the suggestions that have been made in respect of Do Call Registry to make it effective can also be implemented on the Do Not Call Registry. These would go a long way in ensuring that Unsolicited Commercial Communications are minimised. Illustratively the following could be applied for NDNC as well –

- Timings of calls can be specified so that calls are not received at odd hours
- Creation of a separate telephone number level for telemarketers
- Introduction of an IVR menu option which when accessed would automatically register the subscriber on NDNC
- Setting up of an agency for maintaining the NDNC list and enforcing regulations, etc.

### **3. Telemarketing activity (voice based calls) creates considerable job opportunities specially for the economically weaker and backward sections of society**

The voice segment in the domestic telemarketing industry generates considerable employment. While this is still a nascent industry, it already provides employment to about 2 lakh employees directly and an even larger number indirectly.

There are several unique features in regard to the type of employment generated and the cross sections of the social fabric that this segment touches.



- Domestic voice based service centres are increasingly being located in Tier 2 and Tier 3 towns, mainly because of cost pressures in Tier 1 towns and lower price points in the domestic market. As a consequence they are creating most of the job opportunities in Tier 2 and Tier 3 towns.
- Most of the calls are simple and are usually scripted calls i.e., the flow of the call is pre-determined and usually a script is provided as a guidance to the employee making the call from the telemarketing unit. Handling calls like these enables the employee handling the call to increase his / her self-confidence.
- Most calls are in the regional languages and hence these jobs are accessible to even those who are not fluent in or unfamiliar with English. There is a high probability, that employees handling these calls would be from non English medium schools and possibly more from the economically backward sections of society.

**4. Specific aspects contained in TRAI Consultation Paper on which we have a variance of views**

Section reference in TRAI Consultation Paper	Statement in Consultation Paper	Alternate view
Introduction: Page 1, para 2	... but the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy". .....	Unsolicited Commercial Communications whether calls or SMS etc do not intrude onto the telephone conversations of individuals. While this can be said to intrude into one's personal time but it does not interfere with the holding of a telephone conversation
Introduction: Page 11, para 19	..... apart from nuisance and inconvenience to customers, these SMSs can eat the memory space of the handsets resulting in non delivery of important messages .....	As stated that these messages are unwanted by the vast majority of subscribers, most subscribers would promptly delete these messages and hence it is unlikely that they would continue to reside on the handsets taking up memory space.
Introduction: Page 11, para 20	..... Telemarketers make huge payments to acquire the subscriber telephone number database illegally.....	India does not have any laws in regard to data privacy and hence any information pertaining to individuals, like telephone numbers, can be collated and sold. While this action is avoidable and undesirable, but in the present circumstances cannot be termed illegal.
Chapter 2: para 2.6 Bullet No 2	..... Most of the countries like Australia, United Kingdom and Canada initially adopted the approach of Do NOT call registry or Opt-out approach, but effectiveness of such framework is found to be low. ....	The countries mentioned alongside continue to use the Opt – Out approach i.e., Do Not Call Registry and have continuously strengthened their enforcement mechanism to effectively control the Unsolicited Communications
Chapter 2: para 2.6 Bullet No 2	..... Many of the countries like China, Japan, Italy, United Kingdom and European Union prefer —Opt-in□ approach in their e-privacy directives. Australia has also started discussions to curb Unsolicited Commercial Communications and considering —opt-in□ as one of the options. .....	Each of these countries mentioned does not use the Opt – in approach for voice based calls, as has been mentioned earlier. <b>China:</b> Unsolicited Communications laws cover only commercial emails. Voice based calls are not covered at all. <b>Japan:</b> Unsolicited Communications laws cover only emails. Voice based calls are not covered at all <b>Italy:</b> Opt – in is for non voice interactions like use of automated calling systems without human intervention only are allowed with the subscriber's consent (Opt – in) and also covers electronic communications like e-mail, fax, MMS / SMS etc <b>UK and EU:</b> Opt – in is only applicable to automated

		calling machines, fax, email etc. voice based calls are not covered by laws in these countries.
Chapter 2: para 2.8.1	<p>..... the right to privacy has been held to be part of fundamental right to personal liberty and freedom guaranteed under Articles 19 and 21 of the Constitution. Any responsibility placed on the phone user to register him to restrict unwanted calls would mean denying his privacy and breach of confidentiality. ....</p> <p>.....Any telemarketer using data other than provided by authorized source for telemarketing will be guilty of invading privacy of the subscriber. ....</p>	<p><b>Please refer to the annexure below.</b></p> <p>A US District Court in similar circumstances had held that the Federal Communications Commission's (FCC) opt-in rule for the use of telephone subscriber information was unconstitutional and was violative of the First Amendment whereby the telemarketer's freedom of speech was curtailed. The Appellate Court upheld the District Court's interpretation and the US Supreme Court declined to review the judgement in appeal. The opt – in rules were held to be presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the opt – in rules were necessary to prevent a “specific and significant harm on individuals,” and that the rules were “no more extensive than necessary to serve [the stated] interests.</p>
Chapter 2: para 2.8.3	<p>..... It may not be out of place to mention that Mobile telephone subscribers' directory has not been published. As such no information about any mobile subscriber is available in public domain. Procurement of any mobile subscriber data by telemarketers without the consent of the subscribers, is breach of privacy and can be prosecuted. ....</p>	<p>In terms of privacy it is immaterial whether a mobile subscriber's directory is published or not. If a subscriber gives his mobile number to a third party without seeking the assurance that the third party will not further circulate his / her number, there would be no illegal act committed if such third party were to collate such data and commercially exploit it. Currently, the laws in India do not preclude such activity.</p> <p>It should also be borne in mind that privacy laws in India are virtually non-existent and hence an inference that procurement of mobile subscriber data by telemarketer from a secondary source (i.e., other than the mobile telephony service provider or the subscriber him/herself) would not constitute a breach of privacy</p>

## **Annexure with comparisons between “Opt – In” and “Opt – Out” Options**

Extracts from a Case study of MBNA analysing  
**The Impact of Opt-In Privacy Rules on Retail Credit Markets**

By  
**MICHAEL E. STATEN<sup>1</sup>**  
**FRED H. CATE<sup>2</sup>**

A common theme that implicitly runs through both federal and state laws in the United States is that governmental privacy protections are only permitted when they target specific types of information and providers and where a balancing test can be reasonably construed to warrant government intervention. The Supreme Court has struck down many ordinances that would require affirmative consent. The words of the Court – involving a local ordinance that banned door-to-door solicitations without affirmative householder consent—are particularly apt:

*Whether such visiting shall be permitted has in general been deemed to depend upon the will of the individual master of each household and not upon the determination of the community. In the instant case, the City of Struthers, Ohio, has attempted to make this decision for all its inhabitants.<sup>3</sup>*

The Tenth Circuit reached precisely the same conclusion in 1999, when the court struck down the Federal Communications Commission’s (FCC) opt-in rule for the use of telephone subscriber information.<sup>4</sup> The appellate court found that the FCC’s rules were subject to First Amendment review because, by limiting the use of personal information when communicating with customers, they restricted U.S. West’s speech. Although the court applied intermediate scrutiny, it determined that under the First Amendment, the rules were presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were necessary to prevent a “specific and significant harm on individuals,” and that the rules were “no more extensive than necessary to serve [the stated] interests.”

*Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest for it is not based on an identified harm.*

The court found that for the FCC to demonstrate that the opt-in rules were sufficiently narrowly tailored, it must prove that less restrictive opt-out rules would not offer sufficient privacy protection and it must do so with more than mere speculation:

*Even assuming that telecommunications customers value the privacy of [information about their use of the telephone], the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy. The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.*

The court found that the FCC had failed to show why more burdensome opt-in rules were necessary and therefore struck down the rules as unconstitutional. The fact that the information was being used for purposes other than publication was irrelevant. The Supreme Court declined to review the case.<sup>5</sup>

---

<sup>1</sup> Distinguished Professor and Director of the Credit Research Center, The Robert Emmett McDonough School of Business, Georgetown University.

<sup>2</sup> Distinguished Professor and Ira C. Batman Faculty Fellow, Indiana University School of Law-Bloomington; Senior Policy Advisor, Hunton & Williams Center for Information Privacy Leadership.

We thank MBNA America for its participation in this case study and all of the MBNA employees who shared their time and expertise throughout the project. In addition, we received helpful comments and suggestions on earlier versions of this Article from Martin Abrams, Dan Jaffe, David Klaus, Mark MacCarthy, Harriet Pearson and Michael Turner. This project was supported by a grant to Georgetown University from the Privacy Leadership Initiative.

<sup>3</sup> Martin, 319 U.S. at 141.

<sup>4</sup> U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999).

<sup>5</sup> US West Communications, Inc. v. FCC, 528 U.S. 1188 (2000).

For purposes of this study three examples are studied that illustrate the impact of three distinct and successively more restrictive opt-in regimes. The three regimes described below are points along a continuum of rules that range from no restrictions on the sharing of personal information at one extreme to explicit consumer permission for the use of any kind of personal information at the opposite extreme.

**1. Opt-In Regime One Third-Party-Sharing Opt-In.** The least restrictive set of rules are opt-in laws that would permit an organization's internal use of personal information about customers or members, but would require opt-in consent before personal information can be disclosed to third parties outside the organization. This type of opt-in can be found in bipartisan proposals that would amend the privacy provisions of the Gramm-Leach-Bliley Financial Services Modernization Act (the GLB Act) that cover the use of personal information by financial institutions.<sup>6</sup>

**2. Opt-In Regime Two Affiliate Sharing Opt-In.** Moving toward the more restrictive end of the spectrum, the second opt-in regime would limit the sharing of personal information across corporate affiliates within the same organization, as well as with third parties. Affiliate sharing of personal information is a key issue in proposed amendments to the GLB Act and in proposed legislation in many states. In essence, the debate centres on whether separate affiliates under a single corporate umbrella should be treated as third parties. At present, most U.S. privacy laws (including the GLB Act) do not apply an opt-in standard to information sharing among affiliates.

The rationale for putting fewer limits on data-sharing among affiliates reflects two significant considerations. **First**, the responsible sharing of information among affiliates creates demonstrable benefits for the customer, as illustrated by the examples below. **Second**, as a practical matter, consumers expect different divisions of the same company to know them and to offer services and benefits based on that knowledge. A consumer's decision to do business with a company carries an implicit approval (and expectation) of information-sharing under the corporate umbrella. The expectation of information-sharing is especially true if affiliates are all operating under the same brand name, such that the affiliate distinction is invisible to the consumer.

An affiliate opt-in regime would restrict the sharing of personal information about prospects and customers across these corporate divisions, all of which operate under the MBNA brand name and under its direct management, despite the fact that customers are likely unaware of the legal distinctions that make certain divisions "affiliates."

**3. Opt-In Regime Three: Blanket Opt-In.** In the most restrictive of the three scenarios, opt-in consent would be required for any internal use of personal information subject to exceptions specified in the law (such as for collecting debts, performing requested services, or providing product recall and safety notices). The FCC adopted this type of opt-in system when it prohibited telephone companies from using information about their customers' calling patterns for marketing new services without first obtaining those customers' explicit consent.<sup>7</sup> The impact of blanket opt-in will obviously depend upon the scope of information uses for which opt-in consent is required (and the companion list of exemptions), but blanket opt-in limits what a business or other organization can do with information it already legally possesses.

**B. The Differential Impact of Opt-In versus Opt-Out.** Proponents of opt-in claim that requiring explicit consent for the use of personal information gives consumers greater privacy protection than an opt-out system.<sup>8</sup> But, in fact, both opt-in and opt-out give consumers the final say about whether their personal information is used. Neither approach gives individuals greater or lesser rights than the other. Under both systems the customer makes the final and binding determination about data use. **However, there is a stark difference between the opt-in and opt-out systems in terms of their cost.**

A pipeline analogy is helpful in thinking about how opt-in versus opt-out rules affect the flow of personal information through the economy. An opt-out system sets the default rule governing use of personal

---

6 Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501-527, 113 Stat. 1338, 1436-50 (1999) (codified at scattered sections of 15 U.S.C.). The list of organizations covered under the GLB Act as financial institutions is broad. It includes regulated financial companies such as banks, securities firms, insurance companies, insurance agencies, thrifts and credit unions, as well as other institutions "the business of which is engaging in financial activities." 15 U.S.C. § 6809(3)(A) (2000), such as finance companies, mortgage brokers and check cashers. So, for example, retailers with credit programs are covered under the GLB Act.

7 Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, 63 Fed. Reg. 20,326, 20,327 (1998).

8 Consumer Protection: Hearings Before the S. Comm. on Banking, Housing and Urban Affairs, 107th Cong. (2002), 2002 WL 31105436 (statement of the Honorable Mike Hatch, Attorney General, State of Minnesota); id. (statement of James M. Kasper, North Dakota House of Representatives); Internet Privacy: Hearing Before the S. Comm. On Commerce, Sci. and Transp., 107th Cong. (2001), 2001 WL 771617 (statement of Marc Rotenberg, Executive Director of the Electronic Privacy Information Center); id. (statement of Jason Catlett, President and CEO, Junkbusters Corp.); Commerce, Trade and Consumer Protection: Hearings Before the House Comm. on Energy and Commerce, 107th Cong. (2001), 2001 WL 338574 (statement of Ed Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group).

information to “free flow.” In essence, opt-out presumes that consumers do want the benefits (greater convenience, wider range of services and lower prices) facilitated by a free flow of information and then allows people who are particularly concerned about privacy risks to remove their information from the pipeline. In contrast, an opt-in system sets the default rule to “no information flow,” under the presumption that consumers harbor greater concern about the risk of information usage than the loss of benefits consequent to shutting off the flow. Under an opt-in system, those benefits evaporate unless consumers explicitly grant permission for information about them to flow in the pipeline.

By setting the default rule to “no information flow,” an opt-in system restricts the information lifeblood on which today’s economic activity depends. Companies that seek to use personal information to enter new markets, target their marketing efforts and improve customer service must restore the information flow by contacting one customer at a time to gain their individual permission to use information. Consequently, an opt-in system for giving consumers choice over information usage is always more expensive than an opt-out system. Opt-in requires that every consumer be contacted individually to gain an explicit consent. In contrast, opt-out is less costly because it infers permission if consumers do not explicitly object. Information about consumers who are either indifferent about the usage or for whom it matters so little as to not be worth the trouble of responding remains in the pipeline.

How large a drag does an “explicit-consent” system impose on economic efficiency? According to the U.S. Postal Service, 52 percent of unsolicited mail country is never read.<sup>9</sup> If that figure translates to opt-in requests, then more than half of all consumers in an opt-in system would lose the benefits or services that could result from the use of personal information because the mandatory request for consent would never receive their attention. Moreover, even if an unsolicited offer is read, experience with company-specific and industry-wide opt-out lists demonstrates that less than 10 percent of the U.S. population ever opts out of a mailing list—often the figure is less than 3 percent.<sup>10</sup> **Indeed, the difficulty (and cost) of obtaining a response of any sort from consumers is the primary drawback of an opt-in approach.**

Under an opt-out system, the failure of consumers to respond does not limit either the use of information about them in the market or the benefits that flow from such use. Under opt-in systems, however, the failure to respond makes the collection and use of personal information illegal (in the US) in the absence of explicit consent. To the extent that consumers do not respond to requests for opt-in consent whether due to the failure to receive or read them, lethargy, confusion, or the competing demands of modern life their inaction amounts to a total prohibition on the collection and use of information about them.

In addition, because opt-in requires specific, individual contact with each consumer, such a system imposes higher costs that may make the proposed use of information and the services and products that depend on that use, economically untenable even for those consumers who would have opted in. In 1997, U.S. West (now Qwest Communications), one of the largest telecommunications companies in the United States, conducted one of the few affirmative consent trials for which results are publicly available. In that trial, the company sought permission from its customers to utilize information about their calling patterns (e.g., volume of calls, time and duration of calls, etc.) to market new services to them. The direct mail appeal for permission received a positive response rate between 5 and 11 percent for residential customers (depending upon the size of a companion incentive offered by the company).<sup>11</sup> Residential customers opted in at a rate of 28 percent when called about the service.<sup>12</sup>

When U.S. West was actually communicating in person with the consumers, the positive response rate was three to six times higher than when it relied on consumers reading and responding to mail.<sup>13</sup> But even with telemarketing, the task of reaching a customer is daunting. U.S. West determined that it required an average of 4.8 calls to each consumer household before they reached an adult who could grant consent. In one-third of households called, U.S. West never reached the customer, despite repeated attempts. In any case, many U.S. West customers received more calls than would have been the case in an opt-out system and despite

---

9 Briefs, CIRCULATION MGMT., May 1999, [http://www.circman.com/ar/marketing\\_briefs\\_7/index.htm](http://www.circman.com/ar/marketing_briefs_7/index.htm) (referring to the U.S. Postal Service’s 1997 household diary study).

10 Internet Privacy, supra note 7 (statement of Fred H. Cate, Professor, Indiana University School of Law-Bloomington).

11 Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, 63 Fed. Reg. 20,326, 20,330 (1998); Brief for Petitioner and Intervenor at 15, U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (No. 98-9518) (“[T]he outbound mail campaign produced affirmative consents in the range of 6–11%. The offering of incentives appeared to have no material impact on the frequency with which consents were provided.”); Ex parte letter from Kathryn Krause, Senior Attorney, US West, to Dorothy Attwood, Senior Attorney, Common Carrier Bureau, Federal Communications Division at 11 (Sept. 9, 1997), in the proceeding In re Implementation of the Telecommunications Act of 1996 (on file with the Duke Law Journal).

12 U.S. West, Inc. v. FCC, 182 F.3d 1224, 1239 n.12 (10th Cir.1999). Interestingly, when an opportunity to consent was presented to the customer at the conclusion of a call that the customer initiated, 72 percent opted in. Id. at 1239.

13 Ex parte letter from Kathryn Krause to Dorothy Attwood, supra note 64, at 9–10.

repeated contact attempts, one-third of their customers missed opportunities to receive new products and services. The approximately \$20 cost per positive response in the telemarketing test and \$29 to \$34 cost per positive response in the direct mail test led the company to conclude that opt-in was not a viable business model because it was too costly, too difficult and too time intensive.

### **The Study draws the following Conclusion**

The practice of offering consumers a choice over many uses of their personally identifiable data is now well accepted in both the public policy and business communities. If a way could be devised such that consumers could register their preferences regarding personal data usage at no cost to themselves or to businesses, then the debate over whether to impose an opt-in versus opt-out rule would largely disappear. However, in the absence of a costless method of registering consumer preferences, an opt-in system remains significantly more restrictive than an opt-out system, because non-response is treated as disapproval, even if it arises from consumer inattention or indifference to the choices.

To briefly summarize the impact on MBNA, we found that mandatory opt-in requirements on MBNA's operations would impair MBNA's affinity group business model, raise account acquisition costs and lower profits, reduce the supply of credit and raise credit card prices, generate more offers to uninterested or unqualified consumers and raise the number of missed opportunities for qualified consumers and impair efforts to prevent fraud and identity theft.

A third-party opt-in rule would drastically affect MBNA's central business model that has built a cardholder base of over 50 million customers around the affinity marketing strategy. Access to member lists for organizations such as professional associations and alumni groups allows MBNA to identify likely cardholder prospects and tailor a product for them that builds on their affinity for the organization. This strategy implodes with loss of access to member records.

Opt-in would also raise account acquisition costs and lower profits. Target marketing efficiency deteriorates under opt-in rules. Both third-party and affiliate-sharing opt-in regimes would dramatically limit MBNA's ability to acquire and use the information necessary to determine which of the 800 million annual "leads" it receives are appropriate candidates to receive card offers. By reducing its ability to cull prospect lists, these opt-in rules would boost MBNA's cost-per-account-booked via direct mail by 22 percent. Moreover, the accounts booked would have lower revenues and higher losses relative to the more precisely targeted group, yielding an 8 percent reduction in net income over the first five years of experience.

Because opt-in restrictions of the type analyzed above would impact all credit card issuers (not just MBNA), the reduction in supply (from both incumbent firms and new entrants) consequent to higher production costs would inevitably impact all cardholding consumers through higher prices, limits on card features or reduced access to credit cards.

Finally, it should be noted that although legislation may impose practical limits on business access to personal information, it does not change the underlying value of that information. MBNA has an economic incentive to improve its targeting efficiency in either an opt-in or opt-out environment. Legal restrictions on the collection of useful data simply boost the incentives to devise proxies for the attributes the restricted data were useful for measuring. These proxies are necessarily less accurate and/or more expensive (or they would have been used in the first place) and quite possibly more intrusive and less equitable. For example, if individually specific data is no longer available, MBNA and other card issuers might adopt rougher proxies for an individual's attributes based on census tract data for the person's neighbourhood.

Movement in this direction as a consequence of opt-in rules, especially in the context of credit and financial services markets, is a step backward from the broad "democratization of credit" experienced over the past generation.