International Journal of Public Administration in the Digital Age
Volume 6 • Issue 4 • October-December 2019

Public Policy Issues in Direct and Digital Marketing – Concerns and Initiatives:
Public Policy in Direct and Digital Marketing

Pratap Chandra Mandal, Indian Institute of Management Shillong, Shillong, India

ABSTRACT

Companies require information about customers to understand them, know their preferences, and develop relationships with them. Companies employ a number of direct and digital marketing channels to collect information and intelligence about customers. Marketers adopt a number of unfair practices for collecting information through direct and digital marketing and this raises concerns about consumer privacy. The article discusses the various aspects of consumer privacy and the need for protecting consumer privacy. The article further focuses on the various regulations enforced by regulatory bodies and governments of countries to protect customers. Various initiatives taken by companies to protect customers are discussed. Direct and digital marketing channels allow companies to collect information and intelligence about customers and to influence them. However, companies should be sensitive to customer concerns. This will help companies in building long-term customer relationships.

KEYWORDS

Consumer Privacy, Consumer Protection, Customer Relationship, Ethics, Marketing Information, Marketing Intelligence, Phishing, Unfair Practices

1. INTRODUCTION

Companies require collecting information and intelligence about customers for analyzing, understanding their requirements and preferences, and targeting them (Stone & Jacobs, 2007). Success in business depends to a large extent on the mutual relationships between customers and companies. Companies understand the importance of customer satisfaction and developing customer relationships (Martin & Murphy, 2017). Again, companies also need to be aggressive to perform and sustain in the competition. This becomes even more important in direct and digital marketing where the competition is intense. In direct marketing and in digital marketing, company employees or people appointed by companies maintain direct relationships with customers (Duhigg, 2007). Companies collect information and intelligence about customers through different direct and digital marketing channels. Sometimes, direct and digital marketers may adopt aggressive approaches which may not be liked by customers or may even bother or harm customers. Consequently, customers become suspicious and speculative about the intentions of direct and digital marketers and the policies adopted by them (Appuzo & Perlroth, 2014). This may also affect the reputation for the company and for the

DOI: 10.4018/IJPADA.2019100105
This article, originally published under IGI Global's copyright on October 1, 2019 will proceed with publication as an Open Access article starting on February 4, 2021 in the gold Open Access journal, International Journal of Public Administration in the Digital Age (converted to gold Open Access January 1, 2021), and will be distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

industry as a whole (Asllani & Halstead, 2015). Customers may get irritated and frustrated because of the actions of direct and digital marketers (Moraes & Michaelidou, 2017). The actions of direct and digital marketers may in extreme cases result in instances of unfair practices or even outright deception and fraud (Bonfrer & Dréze, 2009). Critics accuse the industry of invading the privacy of customers, breaching the codes of conduct to be maintained while dealing with customers, and threatening the security of customers (Hamidi & Moradi, 2017). The issues of privacy and security of customer information are of prime importance especially in online and digital marketing. Critics accuse that marketers violate the codes of conduct for customer privacy and security in digital marketing (Ikonen, Luoma-aho, & Bowen, 2017).

Direct marketers and digital marketing are convenient and beneficial for customers (Martin & Murphy, 2017). Direct and digital marketers usually enjoy mutually beneficial and rewarding relationships. However, although customers mostly benefit from direct and digital marketing, like various other aspects of marketing, they have a dark side as well. Marketers sometimes adopt aggressive and shady tactics for their selfish motives and these motives can harm customers (Ikonen et al., 2017). Such actions result in a bad reputation for the entire industry. Abuses range from simple excesses that irritate customers to instances of unfair practices. Sometimes, to overcome the competition, direct and digital marketers adopt certain practices which result in outright deception and fraud. The direct marketing industry has also faced growing privacy concerns. Digital marketers must deal with internet and mobile security issues (Martin & Murphy, 2017). It is the responsibility of both marketers and customers to guard against irritating and harmful effects of direct and digital marketing practices (Singer, 2012). The paper focuses on various public policy issues in direct and digital marketing, responsibilities of direct and digital marketers and customers, and various initiatives taken by companies to protect customers against such issues. The discussions in the paper are important from the perspective of public administration because the policies adopted by companies, governments, and regulatory bodies and agencies will have immediate effect on consumers which in turn will affect the general public. The policies implemented require to be regulated. So, the policies will have direct effects on public administration. Also, consumers have access to the internet and all types of informational technologies in this digital age. Consumers are active on the social media, browse through company websites, do much of their shopping online, and access the internet on their mobile phones. Because of all these reasons, the topic is of relevance in the digital age.

The paper is structured as follows.

Section 2 focuses on the issues of irritation, unfairness, and fraud created by direct and digital marketers. Sub-section 2.1 focuses on the concerns of consumers with respect to privacy and security in the digital age. Section 3 discusses the various unfair practices followed by marketers in collection of information from customers. Section 4 focuses on the importance of privacy of consumers with sub-sections 4.1 and 4.2. focusing on invasion of consumer privacy and protection of consumer privacy respectively. Remedial actions are required and the necessity is discussed in section 5. Different initiatives taken by companies are discussed in section 6 with a focus on different forms of communications – direct mail (discussed in sub-section 6.1), telephone marketing (discussed in sub-section 6.2), mobile marketing (discussed in sub-section 6.3), internet marketing (discussed in sub-section 6.1), and e-mail marketing (discussed in sub-section 6.1). Section 7 focuses on the key points discussed in the paper. Managerial implications and contribution of the paper are highlighted in sub-sections 7.1 and 7.2 respectively. Section 8 concludes the paper with sub-section 8.1 focusing on future research directions.

2. IRRITATION, UNFAIRNESS, AND FRAUD

Direct marketers, digital marketers, and their aggressive measures sometimes irritate or offend customers (Atsmon, Child, Dobbs, & Narasimhan, 2012). For example, customers get offended when TV commercials ask for direct responses, are too loud, long, and insistent. Emails sent by

direct marketers are delivered daily and such emails fill the inboxes of individuals. Most of those emails are unwanted junk mails or spam mails. Similarly, mobile phones and tablet screens of individuals flash with unwanted online or mobile display advertisements, pop-ups, or pop-unders (Moraes & Michaelidou, 2017).

Direct marketers take undue advantage of the ignorance of individuals. They target those individuals who can be influenced easily. They target impulsive and less-sophisticated buyers. Critics accuse television shopping channels, enticing websites, and program-long infomercials which target individuals who are addicted to watching television and browsing on the internet (Hamidi & Moradi, 2017). Direct marketers capture the attention of individuals by featuring smooth-talking hosts, elaborately staged demonstrations, "while they last" time limitations, claims of drastic price reductions, and unequalled ease of purchase for individuals. Through such tactics, direct marketers try to influence those individuals who have low sales resistance (Martin & Murphy, 2017).

Nowadays, direct and digital marketers are targeting individuals with fraudulent schemes, such as investment scams. Collections in the name of charity have also multiplied in recent years (Sullivan, 2010). The internet has allowed direct marketers to carry out scams swiftly, conveniently, and sometimes without the fear of getting identified and caught. Internet fraud has become a serious issue. According to the Internet Crime Complaint Center, since 2005, internet scam complaints have tripled and have crossed 275000 per year (Internet Crime Complaint Center, 2016). In 2017, the financial loss incurred due to scams amounted to more than $800 million (Moraes & Michaelidou, 2017).

Phishing is one internet fraud which results in huge loss for individuals. It is a type of identity theft that uses deceptive e-mails and fraudulent online websites to fool users into divulging their personal data (Ikonen et al., 2017). Phishing is not a direct marketing activity. It is an activity which urges individuals to reveal personal information. Although it is not a marketing activity, it is related to the welfare of consumers whose personal information is compromised with. For example, individuals receive e-mails from banks, credit card companies, and other financial institutions stating that their personal information has been compromised and they need to update their information immediately to keep their accounts safe and secured. They are requested to share information like usernames, passwords, and perhaps even their Social Security Number (Martin & Murphy, 2017). Those individuals who share such information become vulnerable because the shared information may be misused by scam artists. Although now-a-days individuals are aware of such scams, it is difficult to detect such scams on the internet. It also damages the reputation of legitimate online marketers who work hard to develop and build their brand image. Scams damage the confidence of individuals in web, e-mail, and other digital transactions (Sullivan, 2010).

2.1. Concerns of Consumers in the Digital Age

Customers are concerned and worried about online and digital security. Customers fear that direct marketers will keep track of their online transactions and social media postings without their knowledge and consent (Ikonen et al., 2017). Direct marketers collect information like bank account details and credit and debit card numbers. Online shopping is common and convenient now-a-days. However, studies reveal that more than 70 percent of individuals are still concerned about safety and security of online transactions. They fear about identity thefts and misuse of their identities to satisfy the selfish requirements of companies. Data breaches are happening in industries like retailing, telecommunication services, and banks to healthcare providers and the government (Moraes & Michaelidou, 2017). Studies show that in 2017 alone, there were 781 major data security breaches in the United States (Moraes & Michaelidou, 2017).

Critics are concerned about vulnerable and unauthorized groups accessing their sensitive information shared on the internet (Moraes & Michaelidou, 2017). Any form of information is readily available on the internet. It becomes difficult for companies to restrict groups of individuals from viewing content on several websites which they are not authorized to access (Ikonen et al., 2017). For example, marketers of adult-oriented materials and sites find it difficult to restrict minors from

accessing contents. Social networking sites like Facebook, Instagram, Twitter, and Snapchat do not allow children under age 13 to open accounts. However, it becomes difficult for such sites to enforce the criteria and all the sites have members who are significantly underaged (Moraes & Michaelidou, 2017). Similarly, it becomes difficult for children to detect issues like identity theft schemes, revealing personal information, negative experiences, and other online dangers. They become vulnerable to such frauds. Critics and national lawmakers are debating about rules and regulations which should be enforced to better protect children online. This requires the development of technology solutions which is difficult. As Facebook puts it, "That's not so easy." (The Drum, 2016)

3. UNFAIR PRACTICES FOR INFORMATION COLLECTION IN DIRECT AND DIGITAL MARKETING

Direct and online marketers may adopt unfair practices for collecting information and this might cause irritation and concern for customers. Some of those practices are perceived as deceptive. Marketers may become aggressive and desperate while collecting customer information. Such actions may result in fraud (Moraes & Michaelidou, 2017).

Sharing of information and intelligence by customers with direct and digital marketers benefits both companies and customers (Byron, 2006). It results in a win-win situation. However, sometimes customers do not favor the aggressive approaches adopted by direct and digital marketers. Buyers fall prey to marketers when they make impulsive buying decisions. Marketers target vulnerable groups of buyers to collect information and to get their products sold. They approach less sophisticated customers like kids, children, and the elderly. It is easy to approach and influence such groups of customers. Critics feel that such marketing practices are unethical (Wilbur & Zhu, 2009).

Individuals dislike TV commercials which try to force the products on to customers. Direct and digital marketers also send unsolicited e-mails to individuals. Many individuals perceive such communications as unwanted junk mails and spam mails. Marketers cause irritation to people when promotions are communicated in the form of display or pop-up advertisements. People might get irritated because they might be engrossed in some important work. Critics feel that such practices are unfair (O'Leary, 2010).

It is easier for marketers to collect information from impulsive or less sophisticated buyers. In the process, they sometimes violate the line of ethics while targeting them (Sullivan, 2010). They target individuals who are addicted to watching television by showing commercials on television shopping channels and program-long infomercials. The programs attract the attention of viewers with the help of smooth-talking hosts and elaborately staged demonstrations. Viewers are influenced by offering drastic prize reductions, excellent product quality, and free offers. They also try to influence viewers to act instantly by mentioning "while they last" limitations (Lohr, 2010). They assure convenient shopping and products with low prices. Marketers of such commercials prepare persuasive communications and write copy intended to mislead buyers (Sullivan, 2010).

Customers are mostly unaware that their personal information is getting stored with companies. Companies maintain customer databases to store the information. Every time a customer orders a product by mail or telephone, apply for a credit card, or take out a magazine subscription, their details like names, addresses, and purchasing behavior are recorded in the company databases (Moraes & Michaelidou, 2017). Critics worry that companies may collect and store a lot of information about customers without the knowledge and consent of customers (Michaels & Lunsford, 2006). Critics also worry that companies may come to know a lot about the personal lives of customers which companies are not supposed to know (Neff, 2006).

Critics accuse that both direct and digital marketers make false claims about their offerings (Wilbur & Zhu, 2009). Direct marketers design mailers and write copy intended to mislead or exaggerate product size, product performance, or the retail price. The Federal Trade Commission (FTC) has

to handle thousands of customer complaints every year regarding fraudulent investment scams and phony charities (FTC, 2009).

Direct marketers are involved in a number of investment scams (Wilbur & Zhu, 2009). Direct marketers persuade customers to donate for charity. The money collected is invested in fraudulent schemes. These types of misleading communications have multiplied recently. The increasing usage and popularity of the internet and the advancement in information technology allow direct and digital marketers to do such communications (Hauser, Urban, Liberali, & Braun, 2009). Some of the most serious issues in recent times include internet fraud, identity theft, and financial scams (Wilbur & Zhu, 2009). In the year 2010 alone, the FBI's Internet Crime Control Center (IC3) received more than 336650 complaints related to internet fraud. This resulted in a monetary loss of $560 million to the U.S. Government (Lohr, 2010).

Consumers share a lot of information on the internet. They fear about the safety, security, and privacy of the shared information. They fear that direct and digital marketers will gain access to the information and use the information unethically without their knowledge. Marketers may come to know a lot about consumers including their personal and sensitive information like credit and debit card numbers, online transaction passwords, bank account details, and mobile numbers (Swartz, 2010). The internet is becoming popular now-a-days because more and more customers are technology-oriented. Online shopping is also becoming popular because of convenience (Clifford, 2010). However, survey suggests that 75% of the participants still do not like their personal or credit card information to be shared on the internet (Vega, 2010). Individuals also worry about security issues and identity thefts which may happen because of attack by annoying and harmful viruses like Trojan, spyware, and other malware and malicious software.

The internet helps in reducing barriers to communication. Although there are checks, it is difficult to restrict individuals from viewing contents which they are not authorized to access. For example, it is difficult for companies marketing adult-oriented products to monitor and restrict minors from visiting their websites (Lohr, 2010). In a survey, out of four children aged between 8 and 12 years admitted to having an account on a social networking website such as Facebook or Myspace. Although such websites do not allow access to children who are less than 13 years old, it is difficult for websites to monitor the activities of children (Steel, 2009). Due to open and unrestricted nature of the internet, it becomes difficult to enforce such regulations in practice. Sometimes, parents may be unaware that their kids are accessing information which they are not supposed to access. One survey found that 17% of the parents did not have the knowledge that their kids are having accounts on social media and that they are accessing them regularly (Learmonth, 2009).

The above example suggests that it is difficult to monitor and control the activities of direct and digital marketers. Such activities of direct and digital marketers may result in increasingly negative customer attitudes and lower response rates. They also result in state and federal regulations (FTC, 2009). Marketers should target their promotions only to individuals who are interested in their offers and who will respond positively to such offers (Ransom, 2010).

4. PRIVACY OF CONSUMERS

Consumers are concerned about the privacy and security of their personal information. This is the toughest public policy issue which the direct marketing industry needs to address (Asllani & Halstead, 2015). Direct marketers collect information about customers and store such information in customer databases. Both direct marketers and customers benefit from the maintenance of such databases. Customers receive offers which match their requirements and preferences. However, critics worry that companies may have access to more information than is actually required. Companies may know a lot about the personal lives of customers. They may use the knowledge to take unfair advantage of customers. Customers fear that excessive usage of customer databases may result in intrusion on

consumer privacy (Verhoef & Lemon, 2013). Customers, now-a-days, share a lot more information about themselves than they used to do previously. However, they are nervous about personal information and preferences shared with marketers via digital and social media. One recent survey found that 92 percent of U.S. internet users worry about their privacy online (Miners, 2014). Another study revealed that 90 percent of Americans feel that they have lost control over the information shared by them with companies on social media sites (Malcolm, 2013).

The advent of big data has made it possible for companies to capture personal information about customers in databases the moment such customers post something on social media sites, enter a sweepstakes, visit a website, apply for a credit card, or order products online or by phone. Companies may then employ data mining and data intelligence for analysis and to "microtarget" their selling efforts (Rafaeli et al., 2012). Direct marketers have become proficient in collecting and analyzing detailed consumer information both online and offline. Even experts are surprised at and worried about the amount of information collected by companies and what they can do with the collected information (Rafaeli et al., 2012). One *Advertising Age* reporter states (Bush, 2010):

I'm no neophyte when it comes to targeting – not only do I work at Ad Age, but I cover direct marketing. Yet even I was taken aback when, as an experiment, we asked the database-marketing company to come up with a demographic and psychographic profile of me. Was it ever spot-on. Using only publicly available information, it concluded my date of birth, home phone number, political-party affiliation. It gleamed that I was a college graduate, that I was married, and that one of my parents had passed away. It found that I have several bank, credit, and retail cards at "low-end" department stores. It knew not just how long I've lived at my house but how much it cost, how much it was worth, the type of mortgage that's on it, and – within a really close ballpark guess – how much is left to pay on it. It estimated my household income – again nearly perfectly – and determined that I am of British descent. But that was just the beginning. The company also nailed my psychographic profile. It correctly placed me into various groupings such as someone who relies more on their own options than the recommendations of others when making a purchase; someone who is turned off by loud and aggressive advertising; someone who is family-oriented and has an interest in music, running, sports, computers, and is an avid concert-goer; someone who is never far from an internet connection, generally used to peruse sports and general news updates; and some who sees health as a core value. Scary? Certainly.

Consumers may be highly vulnerable and open to abuse if information is readily available. Critics argue that credit card companies should not be allowed to make the data of millions of their customers, public. They should also not sell the data to merchants who accept their cards (Verhoef & Lemon, 2013). Similarly, states should also not sell the names and addresses of driver's license holders, along with height, weight, and gender information. This may allow apparel retailers to target individuals with customized clothing. Also, companies in the telecommunications sector should not sell mobile phone usage data to data analytics firms. The firms may sell such data to marketers. Marketers may get customer insights from such data which have not been approved for usage by customers. SAP's Customer Insight 365 unit gleans and sells customer insights from up to 300 mobile calls, web surfing, and text messaging events per day for each of 20 million to 25 million mobile subscribers from data supplied by mobile operators (Kane, 2015). Such actions by marketers are clearly unethical.

4.1. Invasion of Consumer Privacy

Direct and digital marketers are accused of invading consumer privacy and causing security threats. This is the most important public policy issue which needs to be handled by the direct and digital marketing industry (Lohr, 2010). Marketers collect information about customers by applying a number of techniques. They then store the information in customer databases. Companies analyze the stored data to understand customer likes and dislikes, preferences, and psychology. A number of advanced statistical tools like cluster analysis, factor analysis, and predictive analysis are employed

to understand customers and their requirements. Companies then target individuals based on analysis with the help of sophisticated tools like RFM (R – recency, F – frequency, M – monetary value). Based on RFM analysis, RFM scores are calculated for individual customers or customer groups. Companies target those customers or customer groups who have the highest RFM scores (Asllani & Halstead, 2015). Maintaining customer databases has its own benefits. Customers receive relevant offers from companies based on their requirements and preferences. Companies also understand customer requirements better and this helps them to target customers better. Although maintenance of customer databases has its own advantages, critics feel that marketers may come to know a lot about customers which they are not supposed to know. Companies may take unfair advantage of this knowledge. Some of the stored information may be sensitive. Customer information may be stored without the knowledge and consent of customers. Usage of customer information without the knowledge and the explicit consent of customers intrudes on consumer privacy (Ikonen et al., 2017).

Privacy and security issues of customer information are serious concerns because marketers may conduct businesses with the information. Customers swap personal information with companies for customized products (Martin & Murphy, 2017). Customers share personal and sensitive information with the belief and trust that companies will not misuse the information. However, at the same time, customers worry that private information may be used against them for robbing and cheating. They dislike being bombarded with unwanted communications. They also fear that their children may be targeted with promotions (Ohm, 2012). The issues of online privacy, safety, and security are of great concerns for both customers and regulators. Technology allows marketers to collect and analyze all kinds of information (Sullivan, 2012).

Critics have the following comments to make on data privacy:

Make no mistake, your personal data isn't your own. When you update your Facebook page, 'Like' something on a website, apply for a credit card, click on an ad, listen to an MP3, or comment on a YouTube video, you are feeding a huge and growing beast with an insatiable appetite for your personal data, a beast that always craves more. Virtually every piece of personal information that you provide online (and much that you provide offline) will end up being bought and sold, segmented, packaged, analyzed, repackaged, and sold again. (Sullivan, 2012)

Companies are able to store, retrieve, and analyze any information shared by customers with developments in information technology (Martin & Murphy, 2017). The information may include details about visiting a website, applying for a credit card, or ordering products by mail, telephone, or on the internet. The information is stored in customer databases from where direct and digital marketers retrieve the information. With the help of the information and sophisticated analytical tools, direct marketers can "micro-target" their selling efforts. Consequently, customers are concerned about online privacy and security. With the advancement of web tracking technology, digital privacy experts believe that direct marketers will be able to know almost anything about customers without their knowledge (Moraes & Michaelidou, 2017).

Marketers provide a lot of information on their websites. It becomes difficult for customers to assimilate all the information provided on websites (Bussey, 2013). Customers are asked to share their own details after assimilating the information provided. Consequently, some of the information provided by consumers online may make them vulnerable. Companies may take unfair advantage of the shared information (Appuzo & Perlroth, 2014). Critics and policy makers worry that the ready availability of information may leave customers open to abuse. Companies collect information from customers through a number of techniques and without the knowledge of customers. Cookies may be installed on websites and customers may be able to access the websites only after they enable the cookies. Customers are unaware about the information which gets captured because of cookies. Many critics are of the opinion that it is unfair to collect information about customers through such techniques. They also question whether companies are authorized to track the online behavior of customers. They

feel that it is unethical for companies to develop customer databases based on such information and to sell the information to third parties without the knowledge of customers. Because of all these issues, critics voice their support for privacy and security of customer information (Dumenco, 2013).

Information shared by customers with companies may be collected, bought, and sold by the personal data economy, including advertisers, ad networks, website publishers, social networks, marketers, data brokers, and online tracking and targeting companies (Best, 2013). Companies become aware about personal information of individuals like age, race, gender, height, weight, marital status, education level, political affiliation, buying habits, hobbies, health, financial status, vacation dreams, and more (Best, 2013).

The information shared by customers to direct and digital marketers is transparent and it is a matter of concern for customers (Lilien, 2011). Because of all these concerns, individuals, especially older customers are reluctant to share their information online (Ohm, 2012). However, it is difficult for customers to prevent intrusions into their privacy. They are compelled to accept the intrusions, willingly or unwillingly. Customers are unaware about what information they are sharing. They also feel that they do not have any choice but to share the information. Some others feel that the information shared will not really matter. For example, while buying a product like smartphone, customers share a lot of private and personal information. They sign an agreement giving consent to companies to keep track of their every move (Goldfarb & Tucker, 2012). Carrier IQ is a firm which received permission from any purchaser of an EV0 3D HTC smart phone to keep track of every phone call made, text messages sent and received, and websites visited (Acquisti, John, & Loewenstein, 2012). Once the information is shared online, customers do not have any more control over the information shared. The shared information may end up in unexpected places resulting in spam or worse.

It is the right of consumers to know how companies keep track of their online activities. They should be aware about where, when, how, and why they are being watched online. Acxion is a data tracking firm which maintains a database of about 190 million U.S. individuals and 126 million households (Sullivan, 2012). The firm is able to analyze 50 trillion data transactions per year with the help of its 23000 servers. Based on the analysis, Acxion is able to understand and have a 360-degree view of customers by capturing data from offline, online, and mobile sources. The customers of Acxion include banks like Wells Fargo and HSBC, investment services like E*TRADE, automakers like Ford and Toyota, and departmental stores like Macy's (Duhigg, 2012).

It is sometimes unethical for companies to do online profiling of customers. Companies target parents of new-borns with a number of baby products. Such customers are lucrative for companies because they purchase a variety of baby products over a period of time. Companies collect birth records which are public to target such parents. For example, Target analyzed the buying behavior of women who signed up for new-baby registries at its stores. It was revealed that such women bought large amounts of vitamin supplements during their first trimester and unscented lotion at the start of their second trimester (Singer, 2012). Target was able to identify pregnant women and send them offers related to baby products. The offers contained coupons timed to the stages of pregnancy and later baby needs. Critics and analysts were concerned about such unethical targeting of customers (Goldfarb & Tucker, 2012).

4.2. Protection of Consumer Privacy

Consumer privacy is important, and companies should strive to protect it. Laws and regulations are enforced to protect consumer privacy. Governments of countries take initiatives to curb and control unethical practices by companies. Government agencies keep a close watch on not only do-not-call lists but also on do-not-mail lists, do-not-track lists, and can spam legislation. The federal government of the USA enforces a number of legislative actions from time to time. Such actions are taken to regulate and control the aggressive actions which companies adopt to collect information from customers (FTC, 2009). The actions also address the privacy and security concerns of customers. For example, the Congress is drafting legislation which will enable customers to decide how the

information shared by them online will be used by companies. FTC is also taking active initiatives in developing policies for online privacy (FTC, 2009).

Several companies adopt measures to protect consumer privacy even before legislators take preventive actions (Ikonen et al., 2017). Four advertiser groups, the American Association of Advertising Agencies, the Association of National Advertisers, the Direct Marketing Association (DMA), and the Interactive Advertising Bureau from the USA issued guidelines for websites (Magill, 2009). The guidelines are issued for companies so that they follow the government regulations. This will ensure protection of consumer privacy. The guidelines require companies to inform customers whether their online actions are being monitored. The guidelines also require companies to provide customers with an option of opting out from viewing an advertisement and also to inform why the advertisement is shown to the viewer (Magill, 2009). This is especially applicable for behaviorally targeted online advertisements.

Vulnerable groups of customers are easier to target and to get products sold. The most common vulnerable groups are children and kids because they can be influenced easily. Children and kids find it difficult to resist their temptation when they see attractive offers. In 2000, the Congress passed in Children's Online Privacy Protection Act (COPPA) (Kang, 2013). COPPA makes it mandatory for companies targeting children and kids to indicate their privacy policies clearly on their websites. Marketers also require informing the parents of those children and kids that their wards are being targeted. It requires parental consent to target and collect information from children who are below 13. Marketers do online promotions on mobile phones and other new technologies. Such promotions are becoming popular with the advent of new technologies and increasing usage of smart phones. Experts and privacy groups urge the U.S. Senate to extend COPPA and include both new technologies and teenagers. The information which is shared by teenagers online is readily available to third parties. In the age of seamless technologies, this is the main concern regarding privacy because third parties may use the information for their own selfish motives. Also, the privacy and security policies of most of the social networking websites are ambiguous, unclear, confusing, and not very stringent (Moore & Rideout, 2007).

Digital and direct marketers target customers online by providing online advertisements and other means of communications. Direct and digital marketing industry also needs to address the public policy issues (Magill, 2009). Marketers require assuring customers who shop online that their transactions are safe and secured. Towards building the confidence of customers, initiatives are taken by DMA which is the largest association of businesses practicing direct, database, and interactive marketing. DMA members include nearly half of the Fortune 100 companies. DMA launched "Privacy Promise to American Customers" which requires that all DMA members adhere to a specified set of consumer privacy rules. The rules require that customers should be informed about how their information is being used. Permission should be obtained from customers before their personal and private information is made public by selling, renting, or by exchanging with others (Magill, 2009). The rules allow customers to opt out from receiving further communications from companies. Personal information of customers should not also be shared with others without obtaining explicit permission of the concerned customers. The rules require companies to respect consumer privacy and to remove the details of those customers who do not wish to be contacted further through e-mails, phone calls, or any other means of communication (Dumenco, 2013).

The success of direct and digital marketers depends on winning customer faith and maintaining customer relationships. On the other hand, if marketers are insensitive to the wishes and requests of customers, such actions may result in increasingly negative customer attitudes, negative word of mouth, lower response rates, and calls for more restrictive state and federal legislation (Hamidi & Moradi, 2017). Direct and digital marketers should target customers with products and services which are honest, well-designed, and which satisfy customer requirements. The offerings should also be targeted only to the interested individuals and who prefer receiving such communications from companies. Direct and digital marketing is costly and requires investments in terms of money,

manpower, and other resources. Marketers should not waste their resources for those customers who are not interested in the offerings (Clifford, 2009).

5. NECESSITY FOR REMEDIAL ACTIONS

Customers do not encourage direct marketing excesses. Governments and agencies appointed by them take initiatives to curb unwanted intrusions by direct marketers into the lives of individuals. Governments are introducing do-not-call lists, do-not-mail lists, do-not-track online lists, and Can Spam legislation (Moraes & Michaelidou, 2017). The federal government is serious about online privacy and security concerns of customers. It has introduced several legislative actions to regulate how online, social media, and mobile operators obtain and use customer information. Congress is even drafting legislation which will allow customers to have more control on how the information shared by them online is used (Moraes & Michaelidou, 2017). In addition, the FTC is taking a more active role in policing online privacy.

Direct marketers need to be cautious about their activities and should take remedial actions. They should monitor and prevent privacy abuses before legislations take actions. For example, before the government issued regulations, six advertiser groups – the American Association of Advertising Agencies, the Network Advertising Initiative, the Interactive Advertising Bureau, the Direct Marketing Association, the Association of National Advertisers, and the American Advertising Federation issued a set of online advertising principles through the Digital Advertising Alliance (Advertising Age, 2013). Regulations also require that online and mobile marketers be transparent in their actions. Permission should be obtained from consumers before their online viewing data are collected and used for targeting interest-based advertising. Following the regulations, the advertising industry uses an advertising option icon – a little "i" inside a triangle. The icon informs consumers why they are seeing a particular advertisement. The icon also allows consumers to opt out (Advertising Age, 2013).

Direct marketers target vulnerable groups like children. Regulators are strict in protecting privacy rights of children. In 2000, Congress passed the Children's Online Privacy Protection Act (COPPA). The act requires marketers targeting children online to post privacy policies on their websites. Such marketers should notify the parents of children who are being targeted and obtain parental consent before collecting any information from children under age 13 (Kang, 2013). With the subsequent advent of mobile phones, social media, and other digital technologies, in 2013, Congress extended COPPA to include "identifiers such as cookies that track a child's activity online as well as geolocation information, photos, videos, and audio recordings" (Kang, 2013). Critics are concerned about the amount of information obtained from social media by third parties and the manner in which such information is used. Critics are also worried about the ambiguous privacy policies by various social media websites (Hamidi & Moradi, 2017).

Many companies are truly concerned about the privacy and security issues of consumers and have formulated regulations of their own. Some other companies take an industry-wide approach. For example, TRUSTe is a non-profit self-regulatory organization which works in collaboration with multinationals like Yahoo!, Facebook, Apple, Microsoft, AT&T, and Disney to audit privacy and security concerns of customers (Clifford, 2009). It helps customers to solve their privacy and security concerns. The website of TRUSTe says, "TRUSTe believes that an environment of mutual trust and openness will help make and keep the internet a free, comfortable, and a richly diverse community for everyone" (Clifford, 2009). TRUSTe also provides its privacy seal to those websites, e-mail marketing, mobile apps, and other online and social media channels that satisfy its privacy and security standards (Clifford, 2009).

The direct marketing industry understands the public policy issues and is trying to address them (Singer, 2012). For example, it is trying to build confidence about online shopping in the minds of customers. The Direct Marketing Association (DMA) which is the largest association for businesses practicing direct, database, and interactive marketing, including nearly half of the Fortune

100 companies, launched a "Privacy Promise to American Consumers". It makes mandatory for all DMA members to adhere to a set of consumer privacy rules. The members require informing their customers when customer information is exchanged, rented, or sold with third parties. They should also honor the decision of consumers to opt out of receiving solicitations in future. They should not reveal contact information of customers to third parties without the consent of customers (Magill, 2009). Finally, they should abide by the DMA's Preference Service which requires them to remove the details of customers who do not wish to be contacted or do not wish to receive phone, e-mail, or mail offers (Magill, 2009).

Direct marketers realize that customer concerns should be addressed before it is too late. Otherwise, such concerns will lead to increasingly negative customer attitudes, frustration, and lower response rates in future. In extreme cases, such negligence may result in more restrictive and strict state and federal legislation. Direct marketers should realize that customers want honest and well-designed marketing offers. Such offers should be targeted only to those customers who appreciate receiving them. Direct marketing efforts may be too expensive if they are wasted on customers who do not want them.

6. INITIATIVES TAKEN BY COMPANIES

Effective direct marketing channels include telemarketing, mobile marketing, and other forms of direct marketing. Effective direct marketing channels include social media, company websites, and other forms of digital marketing. Direct and digital marketers should use their communication channels effectively. Otherwise, such marketers may experience resentment and backlash from those customers who view such communications as a threat and an invasion of their privacy (Ikonen et al., 2017). Marketers should use their marketing communication channels judiciously to add real value to the interested customers without unwanted intrusions into their security and privacy.

6.1. Direct Mail

Direct mails may be viewed as spam or junk by those individuals who do not have interest in direct mails (Lohr, 2010). Marketers should design communications for direct mails carefully so that they do not waste their own money, energy, resources, and their recipients' time. Direct and digital marketers design communications for sending communications for sending mails, e-mails, and mobile advertisements. Those direct and digital marketers are successful who do permission-based communications only to those customers who express consent in receiving them (Hamidi & Moradi, 2017).

6.2. Telephone Marketing

Direct marketers prefer telephone marketing as a communication channel because of its low cost (Sullivan, 2010). Telephone marketing provides customers with benefits including purchasing convenience and increased information about different offerings. However, telemarketers should design their communications well. The messages should be crisp and to the point. Telemarketers cause customer resentment when they call customers without prior appointment or consent and when they call customers at inconvenient times. All these result in unsolicited outbound telephone marketing (FTC, 2009). Many customers view such communications as junk phone calls, intrusions into their privacy, and get annoyed.

Many countries take initiatives in curbing unwanted telemarketing efforts of direct marketers by enforcing regulations. Such regulations protect the privacy and security of customers (Clifford, 2009). For example, in 2003, USA responded with the National Do Not Call Registry which is managed by the FTC (2009). The registry allows individuals not interested in receiving and responding to unsolicited phone calls to opt out. The legislation bans most telemarketing calls to the registered phone numbers. Individuals can register themselves for Do Not Call Registry at http://www.donotcall.gov or by calling the helpline number 888-382-1222. Fines of $11000 per violation are imposed on those

companies who do not comply with the regulations (FTC, 2009). The initiative has been successful since its inception and has generated results (Wasserman, 2009).

The telemarketing business gets hurt by Do Not Call Registry. However, two forms of telemarketing – inbound consumer telemarketing and outbound B-to-B telemarketing are strong and growing (Sullivan, 2010). Non-profit and political groups employ telemarketing effectively for communicating and for raising funds. The regulations have forced direct marketers to change, refine, and innovate their communications. Now-a-days, rather than practicing push marketing, direct marketers practice pull marketing. Direct marketers provide opt-in calling systems from where individuals can get useful information about offerings. Individuals interested in receiving such information may opt to receive communications through phone or e-mail. Since options are provided to individuals, the initiative is not considered as intrusive. The initiative generates better returns to direct marketers because individuals communicate with marketers willingly (Hamidi & Moradi, 2017). On the other hand, direct marketers who practice push marketing and violate do-not-call regulations experience backlash from customer activist groups. Such groups may flood the violating company's phone system with return calls and messages (Hamidi & Moradi, 2017).

Governments of countries enact business legislations to protect customers. Such regulations penalize marketers who follow unfair business practices. Otherwise, unethical marketers would manufacture shoddy products, invade consumer privacy, mislead consumers in their advertising, and deceive consumers through their packaging and pricing (Levy, 2011). Various agencies define rules and regulate unfair business practices to protect customers (Klie, 2012).

Government regulations look after the welfare of the society at large. Such regulations protect individuals against unrestrained business practices. Profitable business activities of direct marketers are not always beneficial for the general public and do not always create a better quality of life. Regulators try to ensure that direct marketers take responsibilities for their own actions. Marketers should also be aware of the social costs of their production and products (Birkner, 2011).

Direct marketers should be aware of the various agencies set up to ensure safety and security of consumers and should abide by the regulations enforced by such agencies. In the U.S., Congress has established federal regulatory agencies like the FTC, the FDA, the Federal Communications Commission, the Consumer Product Safety Commission, and many others (Napolitano, 2012). Government agencies are authorized to formulate and enforce laws and direct marketers should abide by the laws which can have a major impact on the operations and consequently, marketing performance.

6.3. Mobile Marketing

Direct marketers use mobile marketing extensively now-a-days as an effective communication channel. This is made possible due to the popularity and widespread usage of mobile phones. However, direct marketers should act responsibly while communicating through mobile phones. Consumers view mobile marketing with suspicion (Glanz, Larson, & Lehren, 2014). Weary customers may become frustrated and irritated because of irresponsible and unwanted mobile communications. One mobile marketing expert comments, "If you are interrupted every two minutes by advertising, not many people want that. The industry needs to work out smart and clever ways to engage people on mobile" (Miller & Sengupta, 2013).

6.4. Internet Marketing

Company websites are storehouses of information for direct and digital marketers. Consumer privacy and security are of prime importance in internet marketing because information is readily accessible on the internet. Some companies are conscious about the apprehensions of consumers. They show genuine concern and respond well to consumer privacy and security issues (Martin & Murphy, 2017). Many companies are proactive in taking initiatives while others are reactive and follow regulations formulated by the specific industry. TRUSTe is a non-profit, self-regulatory organization which works with other companies and audit the privacy and security issues. Some of its clients include Yahoo!,

Apple, Facebook, Disney, Microsoft, and AT&T (Clifford, 2009). TRUSTe provides its privacy seal to those companies which comply with its privacy and security standards. Certificates issued by TRUSTe are recognized because such certificates provide assurance and build confidence for consumers.

Consumers dislike their online activities being tracked by direct and digital marketers. So, governments, are also considering implementing a do not track option for consumers online like the do not call option for unsolicited phone calls (Singer, 2012).

6.5. E-Mail Marketing

E-mail marketing is used as a communication channel extensively by direct and digital marketers because of its low cost. However, there are issues with the usage of e-mail marketing (Magill, 2009). Individuals view unwanted and unsolicited e-mail messages as spam e-mails. Unsolicited e-mails flood the inboxes of individuals. This causes irritation and frustration for individuals (Magill, 2009). Research shows that spam e-mails account for more than 90 percent of all e-mails which get delivered to the inbox of an individual (Trosclair, 2010). Although sometimes intrusive in nature, direct and digital marketers aim at adding value to consumers through e-mail marketing.

E-mail marketing is intrusive in nature and marketers should practice permission-based e-mail marketing. Companies should send promotional e-mails only to those individuals who express explicit interest in receiving such e-mails. Many companies understand the requirements and preferences of their customers and configure their e-mail systems accordingly. For example, Amazon.com suggests a number of "we thought you would like to know" messages to customers based on their preferences and past buying behavior (Trosclair, 2010). Marketers delight customers by delivering the required products even before customers show explicit interest. Similarly, StubHub redesigned its e-mail communication system. It was done so that only those customers who express explicit interest receive promotional offers (Tsai, 2008).

Online ticket merchant, StubHub started building awareness among people with its batch-and-blast e-mail campaigns. The campaigns helped StubHub to understand the importance and value of targeting its customers with relevant e-mails. StubHub allows its customers to opt-in for receiving e-mails during registration, purchases, and while signing in on StubHub website. Such initiatives allow StubHub to target appropriate customers with relevant offers. This required aligning customer data with the communications done. Such messages yielded immediate, positive, and stunning results for StubHub (Tsai, 2008). Because of such measures, e-mail click-through rates jumped 30 percent and ticket sales increased by 79 percent even when StubHub sent fewer promotional e-mails to relevant customers. One StubHub marketer commented, "The results speak for themselves. These new targeted campaigns are driving 2500 percent more revenue per e-mail than our average marketing campaign" (Tsai, 2008).

7. DISCUSSIONS

The paper focused on the various public policy issues in direct and digital marketing. Companies adopt a number of unfair direct and digital marketing practices in collecting information and intelligence from their customers and also to attract their customers. Direct and digital marketers and their customers usually enjoy mutually rewarding relationships. However, sometimes the activities of marketers present a darker side. The aggressive and sometimes shady tactics of a few direct and digital marketers can bother or harm customers and give the entire industry a bad reputation. Abuses range from simple excesses that irritate consumers to instances of unfair practices or even outright deception and fraud. Direct and digital marketers have been accused of invading consumer privacy and internet security issues. Such concerns call for strong actions by marketers and public policy makers to curb direct marketing abuses. Both direct and digital marketers and customers want the same things – honest and well-designed marketing offers targeted only toward customers who will appreciate and respond to them.

7.1. Managerial Implications

Unethical and inappropriate actions cannot be controlled only by developing and enforcing regulations and codes of ethics. Companies and managers are responsible for protection of consumers. They should understand and realize the ethical issues and the security and privacy concerns of customers. Each company and its managers must accept responsibility for policing the conduct and reporting of its own marketing research to protect the interests of customers and also of its own. Companies should take preventive measures against misuse of consumer information. Various organizations, agencies, and governments develop codes of conduct and ethics for marketing practices to be followed by direct and digital marketers. They also try to ensure that marketers abide by codes of conduct. New laws and their enforcements to restrict unethical and illegal activities of marketers will continue to increase. Direct and digital marketers should be aware of the regulations when planning for their products and marketing programs. Company managers should also be conversant with the major laws protecting consumers, competition, and society. They should understand the implications of the laws at the local, state, national, and international levels and should abide by those laws.

7.2. Contribution of the Paper

The contribution of the paper lies in the fact that an in-depth discussion of the various practices adopted by direct and digital marketers was done. The discussions have both theoretical and managerial implications. Academicians may conduct a critical analysis of the various practices followed, laws and regulations enforced, and suggest improved strategies to implement the best ethical practices. The discussions will sensitize managers in an organization about the importance of being ethical while dealing with customers. The discussions will also sensitize both practicing managers and academicians about the initiatives taken by governments of different countries and regulatory bodies to protect consumer rights. Efforts were made to include the relevant and the latest literature related to the marketing practices adopted by direct and digital marketers. However, the field of formulating public policies and ethical practices for customers is an evolving field with developments happening regularly. Researchers and practicing managers require keeping themselves updated about the latest trends and developments in the field of public policy and the roles played by ethical practices in direct and digital marketing.

8. CONCLUSION

The paper discussed the various aspects of direct and digital marketing, collection of marketing information, generation of marketing intelligence, and the ethical issues related to direct and digital marketing. The paper focused on privacy of consumers – concerns of consumers with respect to privacy and security in the digital age, invasion of consumer privacy and protection of consumer privacy. It focused on the various ethical issues related to consumer privacy. Remedial actions should be adopted by marketers to ensure the safety and security of customers. It discussed the various preventive measures adopted by different authorities so that consumer privacy is maintained. Finally, the paper focused on the initiatives taken by companies to ensure privacy, safety, and security of customers. The roles of governments and different regulatory bodies are discussed. Companies will be able to win customer belief and trust if they implement codes of ethics properly and assure the safety and security of customers.

Companies capture a lot of information about customers and try to influence their customers through various direct and digital marketing channels. Customers have concerns about the security and privacy of their personal information shared. Again, companies have to collect information and intelligence from customers to gain a competitive edge over others. This is inevitable with competition getter intense and tougher. All organizations should act responsibly to major public policy and ethical issues concerning direct and digital marketing practices, issues of intrusion on consumer privacy, and

to enforcing and abiding by the regulations developed to protect customers. This will help marketers in building trust and belief in the minds of customers and in developing customer relationships.

8.1. Future Research Directions

Researchers may study the initiatives taken by governments, regulatory bodies and agencies, and direct and digital marketers and the ethical issues related to the practices adopted in capturing marketing information and collecting marketing intelligence. Based on the analysis of the existing policies and initiatives, researchers might suggest new policies. Practitioners and marketers may evaluate the various practices adopted by direct and digital marketers, understand the negative impact created on customers, and suggest corrective measures, and rules and regulations which need to be incorporated by marketers to ensure that the best ethical practices are followed. This will help companies in building and developing trust in the minds of consumers and serve them better.

REFERENCES

Acquisti, A., John, L., & Loewenstein, G. (2012). The impact of relative judgments on concern about privacy. *JMR, Journal of Marketing Research*, *49*(2), 160–174. doi:10.1509/jmr.09.0215

Advertising Age (2013, February 4). Facebook to make Targeted Ads more transparent for Users.

Appuzo, M., & Perlroth, N. (2014). US Discloses Some Data Disclosure Rules. *New York Times.*

Asllani, A., & Halstead, D. (2015). A multi-objective optimization approach using the RFM model in direct marketing. *Academy of Marketing Studies Journal*, *19*(3), 49.

Atsmon, Y., Child, P., Dobbs, R., & Narasimhan, L. (2012). Winning the $30 trillion decathlon: Going for gold in emerging markets. *The McKinsey Quarterly*.

Best, R. J. (2013). *Market-Based Management* (6th ed.). Upper Saddle River, NJ: Prentice Hall.

Birkner, C. (2011, May 15). Mom's the Word. *Marketing News*.

Bonfrer, A., & Dréze, X. (2009). Real-time evaluation of e-mail campaign performance. *Marketing Science*, *28*(2), 251–263. doi:10.1287/mksc.1080.0393

Bush, M. (2010, April 26). My Life seen through the Eyes of Marketers. *Advertising Age*.

Bussey, J. (2013). Taming the spies of web advertising. *Wall Street Journal*.

Byron, E. (2006, September 19). Estee Lauder tests web-ad waters. *Wall Street Journal*.

Clifford, S. (2009, March 16). Many see privacy on the web as big issue, survey says. *New York Times*.

Clifford, S. (2010, January 26). A little 'i' to teach about online privacy. *New York Times*.

Duhigg, C. (2007, May 20). Telemarketing thieves sharpen their focus on the elderly. *New York Times.*

Duhigg, C. (2012, February 16). How companies learn your secrets. *New York Times*.

Dumenco, S. (2013). *Microsoft: 'Your Privacy is our Priority.' NSA: 'LOL!* New York: Advertising Age.

Federal Trade Commission (FTC). (2009). *Biennial Report to Congress: Pursuant to the Do Not Call Registry Fee Extension Act of 2007*. Retrieved from http://www.ftc.gov

Glanz, J., Larson, J., & Lehren, A. W. (2014). Spy Agencies Tap Data Streaming from Phone Apps. *New York Times, New York*.

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. *American Economic Review: Papers & Proceeding*, *102*(3), 349–353. doi:10.1257/aer.102.3.349

Hamidi, H., & Moradi, S. (2017). Analysis of consideration of security parameters by vendors on trust and customer satisfaction in e-commerce. *Journal of Global Information Management*, *25*(4), 32–45. doi:10.4018/JGIM.2017100103

Hauser, J. R., Urban, G. L., Liberali, G., & Braun, M. (2009). Website morphing. *Marketing Science*, *28*(2), 202–223. doi:10.1287/mksc.1080.0459

Ikonen, P., Luoma-aho, V., & Bowen, S. A. (2017). Transparency for sponsored content: Analyzing codes of ethics in public relations, marketing, advertising and journalism. *International Journal of Strategic Communication*, *11*(2), 165–178. doi:10.1080/1553118X.2016.1252917

Internet Crime Complaint Center. (2016). Internet Crime Complaint Center. Retrieved from www.ic3.gov

Kane, K. (2015, October 26). The $24 Billion Data Business that Telcos don't Want to Talk about. *Advertising Age*.

Kang, C. (2013). Infant iPad Seats Raise Concerns About Screen Time for Babies. *Washington Post.*

Klie, L. (2012). Gen X: Stuck in the middle. *CRM Magazine*, *16*(2), 24–29.

Learmonth, M. (2009, January 13). Since Incoming Regulation, Online Ad Groups Unite. *Advertising Age*.

Levy, P. (2011). Segmentation by generation. *Marketing News*, *45*(6), 20–23.

Lilien, G. L. (2011). Bridging the academic-practitioner divide in marketing decision models. *Journal of Marketing*, *75*(4), 196–210. doi:10.1509/jmkg.75.4.196

Lohr, S. (2010, April 30). Privacy concerns limit online ads, study says. *New York Times*.

Magill, K. (2009, October 20). E-mail ROI still stunning, still slipping: DMA. *Direct Magazine*.

Malcolm, H. (2013, April 21). Millenials Don't Worry about Online Privacy. *USA Today*.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. doi:10.1007/s11747-016-0495-4

Michaels, D., & Lunsford, J. L. (2006, December 4). Ad-sales woes likely to continue. *Wall Street Journal*.

Miller, C. C., & Sengupta, S. (2013). Selling Secrets of Phone Users to Advertisers. *New York Times.*

Miners, Z. (2014, November 12). Your Control of Your Personal Info is all but Dead, Pew Respondents Fear. *PC World.*

Moore, E. S., & Rideout, V. J. (2007). The online marketing of food to children: Is it just fun and games? *Journal of Public Policy & Marketing*, *26*(2), 202–220. doi:10.1509/jppm.26.2.202

Moraes, C., & Michaelidou, N. (2017). Introduction to the special thematic symposium on the ethics of controversial online advertising. *Journal of Business Ethics*, *141*(2), 231–233. doi:10.1007/s10551-015-2754-6

Napolitano, M. (2012). RFID surges ahead. *Logistics management, 51*(4).

Neff, J. (2006, May 14). Axe Cuts Past Competitors, Claims Market Lead. *Advertising Age*.

O'Leary, N. (2010, March 29). Does Viral Pay? *Adweek*.

Ohm, P. (2012, August 23). Don't Build a Database of Ruin. *HBR Blog Network*.

Rafaeli, A., Erez, A., Ravid, S., Derfler-Rozin, R., Treister, D. E., & Scheyer, R. (2012). When customers exhibit verbal aggression, employees pay cognitive costs. *The Journal of Applied Psychology*, *97*(5), 931–950. doi:10.1037/a0028559 PMID:22582725

Ransom, D. (2010, May 17). When the customer is in the neighborhood. *Wall Street Journal*.

Singer, N. (2012, July 21). Consumer Data, but Not for Consumers. *New York Times*.

Steel, E. (2009, June 26). Web privacy efforts targeted – facing rules, ad firms to give, consumers more control. *Wall Street Journal*.

Stone, B., & Jacobs, R. (2007). *Successful Direct Marketing Methods* (8th ed.). New York: McGraw-Hill.

Sullivan, E. A. (2009). Targeting to the Extreme. *Marketing News*, *15*, 17–19.

Sullivan, M. (2012, June 26). Data Snatchers! The Booming Market for Your Online Identity. *PC World.*

Swartz, J. (2010, July 22). Small firms dive into social media. *USA Today*.

Symantec. (2010). *The State of Spam and Phishing: Home of the Monthly Report – April 2010*. Retrieved from http://www.symantec.com/business/theme.jsp?themeid_state_of_spam

The Drum. (2016, February 9). BBC Newsround Uncovers Widespread Underage Social Media Usage.

Topolsky, J. (2011, December 11). Online Tracking Is Shady – but It Doesn't Have to Be. *Washington Post*.

Trosclair, C. (2010). *Direct Marketing, Advertising and ROI: Commercial E-Mail Delivers Highest DM Return on Investment*. Suite101. Retrieved from http://advertising.suite101.com/article.cfm/direct-marketing-advertising-and-roi

Tsai, J. (2008). *How Much Marketing Is Too Much?* DestinationCRM. Retrieved from http://www.destinationcrm.com

Vega, T. (2010, October 4). Ad Group Unveils Plan to Improve Web Policy. *New York Times*.

Wasserman, T. (2009). *New FTC Asserts Itself*. New York: Brandweek.

Wilbur, K. C., & Zhu, Y. (2009). Click fraud. *Marketing Science*, *28*(2), 293–308. doi:10.1287/mksc.1080.0397

Pratap Chandra Mandal is an Assistant Professor (Marketing) at the Indian Institute of Management, Shillong, India. He has completed graduate degree from the reputed Indian Institute of Technology, Kharagpur (IIT Kharagpur), India (Bachelor of Technology in Mechanical Engineering), post-graduate degree from Vinod Gupta School of Management, IIT Kharagpur (master's in business administration), PhD (Marketing) from Vinod Gupta School of Management, IIT Kharagpur. His research concerns customer relationship management, customer satisfaction, services marketing, marketing intelligence, and qualitative methods in management. He is the editor-in-chief of two international journals and is on the editorial board of journals like the Journal of Global Marketing. Pratap has won several prestigious scholarships and awards throughout his academic career.