Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa

Bernard Hamann
BCom(Law) LLB
Academic Associate, University of Pretoria

Sylvia Papadopoulos
BLC(UP) LLB(UP) LLM (UP)
Senior Lecturer, University of Pretoria

OPSOMMING

Direkte Bemarking en Spam Deur Middel van Elektroniese Kommunikasies: 'n Ontleding van die Regulerende Raamwerk in Suid-Afrika

Hierdie artikel weerlê die feit dat die reguleering van "spam" en direkte bemarking aanlyn nie holistiese aandag geniet nie en dat die gefragmenteerde benadering in terme van die Wet op Elektroniese Kommunikasies en Transaksies 25 van 2002, Wet op Verbruikers-beskerming 68 van 2008 en die Wet op Beskerming van Persoonlike Inligting 4 van 2013 ongewens is. Dit het die gevolg dat verbruikers onvoldoende beskerming geniet en 'n onvermoë van die reg om "spam" en direkte bemarking aanlyn effektief te beheer.

Terwyl aanlyn direkte bemarking en "spam" tot 'n mate oorvleuel is "spam" 'n wyer konsep as direkte bemarking. Dit is belangrik om in gedagte te hou dat nie alle direkte bemarking "spam" is nie, en nie alle "spam" direkte bemarking is nie. Die beperking van die regulering van "spam" tot kommersiële kommunikasies of selfs die meer noue konsep, kommunikasies wat met direkte bemarking betrekking het, is nie voldoende nie omdat daar dan steeds baie verskillende tipes "spam" is wat nog ongereguleerd sal bly.

Die artikel argumenteer dat hoewel onlangse regulatoriese veranderinge kan gesien word as 'n verbetering op die vorige posisie in sekere aspekte, is daar nog meer aspekte wat onaangeraak bly en daar is 'n paar bepalings wat nuwe probleme skep. Ten spyte van die onlangse veranderinge in die regulatoriese omgewing is dit waarskynlik dat verbruikers steeds blootgestel gaan word aan 'n deurlopende stroom van nuusbriewe, meningsopnames, godsdienstige boodskappe, politieke inhoud, virus waarskuwings en virus bedrog, nuus, ketting briewe, haat-pos en noukeurige vervaardigde elektroniese kommunikasies wat bedrieglike of misleidende inhoud bevat.

1 Introduction

From a consumer protection point of view, spam and direct marketing are regulated by certain industry-specific self-regulatory guidelines and

codes of conduct,[1] section 45 of the Electronic Communications and Transactions Act[2] (the ECT Act), as well as through newer legislation such as the Consumer Protection Act[3] (the CPA). Once it is fully in force, the Protection of Personal Information Act[4] (the PPI Act)[5] will repeal section 45 of the ECT Act and replace it with chapter 8, sections 69-71, entitled "The rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making."[6] Despite the PPI Act's intention to repeal section 45 of the ECT Act, on the 26th of October 2012 the Department of Communications published the proposed Electronic Communications and Transactions Amendment Bill[7] (the draft ECT Act Amendment Bill) wherein it is suggested that section 45 be retained, or re-enacted, albeit in an amended form.[8]

The purpose of this article is firstly, to present a brief cursory overview of the abovementioned changing legislative paradigm for spam and direct marketing via an electronic communication and secondly, to critically examine the changes that new legislation has or will introduce within that framework. The article builds on previous research published[9] but is distinguished due to the fact that the final version of the PPI Act differs materially to previous versions published[10] and takes into account the recently published draft ECT Act Amendment Bill [2012].

1 Such as The Code of Banking Practice available at http://bit.ly/1bxMKXQ; The Direct Marketing Association codes for Interactive and Direct Marketing available at http://bit.ly/169NdRK; and The Wireless Application Service Providers Association (WASPA) codes of conduct, advertising rules and a dispute resolution mechanism for members and consumers of the mobile services industry available at http://bit.ly/1gK1XJ9 (accessed 2013-08-27).
2 Act 25 of 2002.
3 Act 68 of 2008.
4 Act 4 of 2013.
5 The Protection of Personal Information Act 4 of 2013 was enacted in terms of GN 912 in GG 37067 of 26 November 2013. In accordance with s115, the PPI Act will commence on a date determined by the President by proclamation in the GG which has to date not transpired.
6 See the schedule to the PPI Act which will also repeal ss 50 & 51 of the ECT Act.
7 Electronic Communications and Transactions Amendment Bill [2012].
8 GN 888 in GG 35821 of 26 Oct 2012.
9 Papadopoulos "Are we about to cure the scourge of spam? A commentary on current and proposed South African legislative intervention" 2012 *THRHR* 223-240 and Papadopoulos and Snail (Ed) Cyberlaw@SA III: *The law of the internet in South Africa* (2012) 63-93.
10 The previous version of the PPI Bill [B9-2009] was published in GG 32495 of 14 Aug 2009.

2 Direct Marketing vs Spam

2 1 Introduction

Unsolicited electronic communications range from bothersome to destructive, irritating to offensive, they are an abuse of resources and they can be a threat to email and internet security.[11]

While online direct marketing and spam do overlap to some degree, there are notable differences. It will become evident to the reader that spam is a wider expression than direct marketing and therefore it is important to keep in mind that not all direct marketing is spam and not all spam is direct marketing. With this in mind, this article aims to focus on the current legislative trend, which has opted to regulate direct marketing only.

2 2 Direct Marketing

From a marketing perspective, direct marketing is a system of marketing where the marketer communicates directly with a customer with the goal that the interaction will exact a measurable response and/or transaction.[12]

From a legal perspective, South African legislation defines direct marketing in section 1 of the CPA and section 1 of the PPI Act, as an approach to a person (or data subject in the case of the PPI Act), either in person or by mail or electronic communication, for the direct or indirect purpose of promoting, offering to supply, in the ordinary course of business, any goods or services or to request a donation of any kind.[13]

Practically therefore, in terms of these definitions, any method that can be used to deliver an electronic communication to an existing or potential customer for the direct or indirect purpose of promoting, offering to supply in the ordinary course of business, any goods or services or to request a donation of any kind, would amount to direct marketing online, including but not limited to:

---

11 Buys and Cronje (Eds) Cyberlaw@SA II: *The law of the internet in South Africa* (2004) 160; Van der Merwe, Roos, Pistorius & Eiselen Information and Communication Technology Law (2008) 190.

12 Yordaan "Factors motivating consumers to engage in direct purchasing" 2005 *South African Journal of Psychology* 346; Dibb, Simkin, Pride & Ferrell *Marketing concepts and strategies* (2012) 491.

13 The CPA refers to "an approach to a person" while the PPI relates to "an approach to a data subject". For the purposes of this article the definition of electronic communication is important. In section 1 of the CPA it is defined as "… a communication by means of electronic transmission, including by telephone, fax, SMS, wireless computer access, email or any similar technology or device" and in section 1 of the PPI Act as "… any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient".

- Mobile cellular text and video messaging (SMS or MMS) which is sent directly to the user's device;
- Mobile device applications (Apps) often contain interactive advertisements that appear inside the app;
- Email marketing;
- Search engine optimisation, where meta-tags (keywords written in computer code, which are invisible to the end-user and describe the contents of websites that are recognised by search engines) are used to associate specific websites with specific keywords in order to target people searching for those keywords using search engines like Google. The more often a keyword appears in the hidden code of a website, the higher the search engine will rank the website in the displayed search results, that is, delivered as website or communication by electronic transmission;[14]
- Pay-per-click advertising is similar to search engine optimization in that this form of advertising also uses keywords that consumers are searching for to deliver the electronic communication (website) directly to the searcher. The difference is that with pay-per-click advertising, advertisers bid on certain keywords and the advertiser willing to pay the most for a keyword will ensure a prominent placement in the search result listings that will be displayed first. The advertiser only pays if the consumer clicks on the link;[15]
- Social media marketing;[16]
- Affiliate marketing;[17]
- Banner advertising (mobile and internet), includes static banners on websites and pop up adverts and are a form of interactive advertisement that appears next to or over existing website content;
- Voicemail marketing, that is, where an advertisement is recorded on a personal voice mailbox; and
- Couponing, where manufacturers and retailers make coupons/discounts available for online electronic orders which can be available on company websites, social media, texts or emails and a methodology which is gaining popularity in South Africa in the so-called "daily-deal" websites which offer online deals each day. Customers sign up to receive notices of discounted offers or to receive coupons.[18]

It is submitted that all of these amount, in one way or another, to direct marketing via an electronic communication as defined above.

---

14 Papadopoulos *et al* 205.

15 For e.g. see Google Adwords. Google Adwords "See how it works". Available at http://bit.ly/1arOsNu (accessed 2013-11-05).

16 Stokes *eMarketing – The Essential Guide to Digital Marketing* (2011) 334, available at: http://bit.ly/173skTv (accessed 2013-10-16). Such as Facebook.com, Twitter.com & Pinterest.com. which provide platforms for direct marketers to communicate directly with potential customers by creating content to which customers can respond.

17 Stokes 224. Affiliates promote products and services for each other and get some form of payment upon the occurrence of a specified event.

18 For e.g. see www.groupon.co.za (accessed 2013-10-16).

However, in order for direct marketing to be successful, marketers need to address a target audience and, in order to accomplish that, they need information in the form of names, prospects and/or business leads, together with certain other relevant information such as contact details in the form of phone numbers, addresses and email addresses; demographic details and purchase habits/history or preferences.[19] This information is electronically compiled in a number of ways such as spoofing,[20] harvesting,[21] dictionary attacks,[22] spyware,[23] cookies[24] and

19 McDaniel, Lamb & Hair *Introduction to Marketing* (2013) 185-186, 275, 281; Dibb *et al* 25, 29.

20 Email spoofing may appear in different forms, but all have a similar result: i.e. a user receives email that appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information such as passwords. Tladi "The regulation of unsolicited commercial communications (SPAM): is the opt-out mechanism effective?" 2006 *SAMLJ* 181.

21 Information can be harvested (collected) when people make their email addresses public by placing advertisements online, inquiring about offers, services or products, participating in news rooms, chat rooms and the like, or entering an email address for a legitimate transaction. This information is easily harvested, collated and sold as a database, mostly without an Internet user's knowledge or consent. Geissler *Bulk Unsolicited Electronic Messages* (SPAM): a South African perspective (LLD dissertation 2004 (UNISA)) 36.

22 Software is also available that can randomly generate millions of random addresses or numbers and messages are sent out *en masse*, entering the in-boxes of email addresses that are functional in a particular domain such as for e.g. "mweb.co.za". Many of these addresses have very slight variations such as joesoap@mweb.co.za, joesoap1@mweb.co.za, joesoap2@ mweb.co.za, etc. The software then records which addresses are functional or "live" and email lists are generated and sold. Papadopoulos *et al* 86; Tladi 2006 *SAMLJ* 181; Geissler 36-37.

23 Spyware is software that is surreptitiously installed on a computer that performs certain behaviors, generally without appropriately obtaining your consent first, such as: advertising; collecting personal information and changing the configuration of your computer. Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. Spyware programs can collect various types of personal information, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web-browser activity, or diverting advertising revenue to a third party. Tladi 2006 *SAMLJ* 181.

24 A cookie is a file that a website can store on an Internet user's computer's hard-drive. It allows a website to store information on a user's computer and later retrieve it. Cookies usually contain the name of the website that sent the cookie, an Internet Protocol (IP) address, an expiry date, a time and date when the cookie was created, a user's preference for language or preferred currency, and it may also contain information about the user's e-mail address, and general Internet browsing habits and even information on a user's common keystrokes and mouse movements, postal address (particularly when personal information is entered for the completion of an online order form). Ebersohn "Internet law: cookies, traffic data and direct advertising practices" (2004) *SAMLJ* 741, 742.

phishing.[25]

Whether or not our legislative framework is sufficient to regulate all the practices that are related to direct marketing and information collection or compilation falls outside the scope of this paper.

Direct marketing does have an important role in the economy. Marketing has the function of facilitating exchange by creating utility. Utility is created by matching the supply of a product or service with the demand for that product or service, and facilitating the conclusion of the transaction that benefits both the supplier and the consumer.[26] Responsible marketing and related advertising practices can therefore be a very useful tool for consumers.

2 3 Spam

Spam can be in the form of direct marketing, but it is wider than just direct marketing, as it may also take the form of solicitation for questionable products, or services, or contain fraudulent or deceptive content. It can also include hoaxes, virus warnings, urban legends, jokes, chain letters, newsletters, opinion surveys, requests for support or donations and hate mail, that is, non-commercial electronic communications. Spam has also been used to distribute viruses and malicious code.[27]

There are three main trends that can be identified in legislative descriptions for spam: Firstly, "unsolicited electronic messages" (UEM); secondly, "unsolicited commercial electronic messages" (UCE) and thirdly, "unsolicited bulk electronic messages" (UBE).[28]

The drafters of the ECT Act chose to regulate, not prohibit, the sending of UCE to consumers,[29] while the CPA and the PPI chose to limit their protection to direct marketing, arguably a more restrictive version of UCE.[30]

---

25 Phishing is the name given to online identity theft implemented by sending an e-mail or other communication that deceptively claims, or appears to be, from an established and legitimate company (usually a bank). Its aim is to try and deceive users into disclosing their personal information, such as credit card numbers or banking passwords. Frequently these messages or the websites that they link to, also try to install malicious code. This information obtained by phishers is used to access bank accounts and withdraw money, or to open new bank or credit card accounts in the victim's name, causing major financial losses to those involved. OECD *Anti-spam toolkit of recommended policies and measures* (2006) 21-22.

26 McDaniel & Darden *Marketing* (1987) 4-5.

27 Papadopoulos *et al* 85; Geissler 18, 88-90.

28 Geissler 28-32.

29 ECT Act s45.

30 CPA s1 & PPI Act s1.

The unsolicited element of an UCE communication implies that there is no prior relationship between the sender and the recipient and that the recipient has not explicitly given consent to receive the communication.[31] It is also a communication that is commercial in nature that seems to relate to messages whose primary purpose is to advertise or promote goods or services.[32] Therefore, any communication that is classified as non-commercial would not be regulated under an UCE definition. This would include, but is not limited to, communications such as newsletters, opinion surveys, religious messages, political content, virus warnings and virus hoaxes, urban legends, news, chain letters and hate-mail.[33] More importantly, any carefully crafted electronic communication that contains fraudulent or deceptive content will, more than likely, fall through the regulatory net as a non-commercial communication.

An UCE definition therefore concentrates on message content rather than the sender's motivation for sending the message.[34] The main reasons advanced for using an UCE definition include: The fact there are no threshold numbers of messages that need to be sent before it qualifies as "spam" and non-commercial messages may be constitutionally protected under the right to freedom of expression and therefore using an UCE definition avoids legal issues that may arise in this arena.[35]

None of the legislation discussed in this article included the *bulk* requirement, as an alternative to commercial, as can be found in some foreign jurisdictions. Therefore, a single UCE communication may be classified as spam.[36]

Geissler argues that the real issue with spam is not about content but the method of delivery. Bulk implies that the message could be a single message sent to a very large number of recipients, or it could be separate but identical copies of a message that are sent to a large number of recipients. The main problem with a bulk requirement is determining the threshold for how many copies constitute a bulk mailing and within what time period they should all be sent.[37]

Geissler's arguments in favour of an UBE definition include that often the contents of an UCE communication are not objectionable and that the focus should be on the harm that is caused, that is, the fact that it is sent in large quantities rather that the motivation for sending the communication.[38] She finally concludes that legislation regulating or

31 Buys *et al* 160; Geissler 24-25.
32 The Federal Communications Commission Consumer Facts: CAN-SPAM Act "Unwanted text messages and e-mail on wireless phones and other mobile devices." Available at http://fcc.us/1fG1rur (accessed 2013-10-01).
33 Buys *et al* 160.
34 Geissler 25.
35 *Idem* 25, 29.
36 Buys *et al* 161.
37 Geissler 26-28.
38 *Idem* 30.

prohibiting spam should include the requirements of "unsolicited" and "bulk", that is, an UBE definition rather than an UCE definition. An argument the authors are in agreement with.

3 The Changing Landscape

3 1 The Electronic Communications and Transactions Act 25 of 2002

3 1 1 Application

The ECT Act applies to all electronic transactions and data messages except those excluded by the Act itself or its schedules.[39] Under the provisions of section 42 and the rest of chapter VII it is clear that section 45 will only apply to an "electronic transaction", where one party is a "consumer".[40]

An "electronic transaction" is not defined in the ECT Act, but a "transaction" is either of a commercial or non-commercial nature.[41] It is assumed, that "electronic transactions" include transactions where the use of data[42] is a basic component of the transaction.[43]

A consumer is defined as "… any natural person who enters or intends entering into an electronic transaction with a supplier, as the end-user of the goods or services offered by that supplier".[44]

This definition excludes the operation of the chapter VII consumer protection provisions in all business-to-business (B2B) transactions and some business-to-consumer (B2C) transactions where the consumer is a natural person but not the end-user of the goods or services acquired.[45]

It is recognised that juristic persons are often in the same practical position as a natural person consumer, and therefore a strong case could be made to include at least some of these parties in the definition of a "consumer" as is the case under the CPA.[46]

3 1 2 Regulation

Section 45 of the ECT Act states that senders can send any electronic communication provided that, if the communication is a commercial communication, the sender must give the person receiving the

39 ECT Act s4 & schs 1 & 2.
40 Papadopoulos *et al* 65.
41 ECT Act s1.
42 ECT Act s1 definition where data means electronic representations of information in any form.
43 Papadopoulos *et al* 65.
44 ECT Act s1.
45 Van der Merwe *et al* 182.
46 Papadopoulos *et al* 85. See par 3.2.1 (c) below.

communication, the option to opt-out of receiving further communications and, if a request is made by the consumer, the source where the contact details were obtained must be revealed. A failure to comply with these requirements is an offence in terms of section 89(1), with penalties that include fines and imprisonment of up to twelve months.[47] Finally, it confirms that no agreement is concluded where a consumer fails to respond to the unsolicited communication.

3 1 3 Commentary

It's pointed out that for the opt-out or unsubscribe mechanism to be effective, two things are necessary: Firstly, that the spammer respects the call to opt-out; and secondly, that the consumers have faith in using this function.[48] This is not a realistic viewpoint in the regulation of spam.[49]

Some of the further criticisms of section 45 include:[50]

(a) It's not stipulated how the opt-out mechanism should be made available, therefore most spam doesn't have an opt-out link or if it does, it's dysfunctional;

(b) Spammers disguise or falsify their headers, that part of an email that tells us who sent the email, the sender's email address, time, date, and etcetera, and a person cannot opt-out because they are unable to trace or identify the real spammer. This is problematic because this practice is not prohibited or penalised;

(c) If a person uses the opt-out mechanism or they request information on where the spammer obtained the address, the recipient confirms that the address is alive and functional, with the result that even more spam will be sent, often from a number of new sources;

(d) The onus is always on the consumer to request spammers to stop or to obtain information to lay a complaint which in turn means if the consumers don't exercise their rights, the spammers can continue to send the spam and remain unsanctioned; and

(e) Finally, most spam originates from outside of South African jurisdiction, which makes enforcement of these rights very difficult, and the result is that few, including under-resourced law enforcement offices, will take the time, effort or money to locate and litigate against an offender for a maximum penalty of twelve months in jail.

It is therefore clear that the opt-out mechanism and section 45 of the ECT Act is ineffective in dealing with the problems of spam.

47 ECT Act s89.
48 Papadopoulos *et al* 86; Tladi 2006 *SAMLJ* 186-187.
49 Papadopoulos *et al* 86; Van der Merwe *et al* 190-191; Tladi 2006 186-187; Geissler 121-131; Buys *et al* 165-166.
50 Tladi 2006 *SAMLJ* 186-187.

3 2 The Consumer Protection Act 68 of 2008

3 2 1 Application

The CPA applies to each transaction occurring in South Africa, unless it is exempted and includes the promotion, performance or supply of goods or services, the goods and services themselves as well as goods that are a part of certain exempted transactions.[51]

This means that most entities supplying goods or services in South Africa and the transactions that they enter into with the consumers will fall within the ambit of the Act. The supplier is defined as the person who markets (promotes or supplies) any goods or services, while a service provider is the person who promotes, supplies or offers to supply a service.[52] Therefore the CPA mainly regulates the marketing of goods and services to consumers.[53] The consumer includes both natural person consumers and small to medium-sized juristic person consumers whose asset value or annual turnover at the time of the transaction is less than the monetary threshold of two million rand, calculated in accordance with the schedule,[54] to whom goods or services are marketed, who have entered into transactions with suppliers, in the ordinary course of business of the supplier. It may also include a user, recipient or beneficiary of the goods or services and a franchisee.[55]

To get a precise delineation of the scope of application of this Act, it is necessary to define some of the other key concepts used in section 5(1), which include the terms "transaction", "goods" and "services":

(a) 'Transaction' refers to a transaction, in the ordinary course of business, which is an agreement between two or more persons for the supply or potential supply of goods or services, the supply of any goods to or at the direction of a consumer or the performance of any services by or at the direction of the consumer in exchange for consideration. Consideration would be anything of value, given and accepted, in exchange for the goods or services.[56] For the online consumer it could typically include electronic credit, tokens and tickets, money, property,

51 CPA s5(1). Under s5(1)(d) and s5(5) if any goods are supplied within the Republic to any person in terms of a transaction that is exempt from the application of the CPA, the goods and importer or producer, distributor or retailer are still subject to ss60 & 61 which relate to safety monitoring, recall and strict product liability. The exemptions are listed in s5(2) and relate to goods and services promoted to the state, where the consumer is an exempt juristic person, transactions exempted by the Minister, credit agreements under the NCA, services under an employment contract, etc..

52 CPA s1.

53 CPA s5(7). It also regulates the relationship between franchisors and franchisees.

54 See GN 294 in GG 34181 of 2011-04-01.

55 CPA s1 where a "juristic person" includes – (a) a body corporate; (b) a partnership or association; or (c) a trust as defined in the Trust Property Act, 1988 (Act No. 57 of 1988).

56 CPA s1.

awards, undertakings, loyalty credit and the rights to assert a claim.[57] Under section 5(6) there are certain arrangements that may also be considered 'transactions' between a 'supplier' and a 'consumer' under the Act. These 'deemed transactions' include the supply of goods or services in the ordinary course of the supplier's business, to any members of a club, trade union, association or society and this is true even if the service or goods are provided free of charge.[58]

(b) Goods and services include anything marketed for human consumption; any tangible object including any medium on which anything is or may be written or encoded; any literature, music, photograph, motion picture, game, information, data, software, code or other intangible product written or encoded on any medium, or a licence to use any such intangible product; a legal interest in land or any other immovable property, other than an interest that falls within the definition of "service" in this section; and gas, water and electricity.[59] While services include work; undertakings; the provision of: Education, information, advice, transportation, accommodation, entertainment; access to electronic communication infrastructure, events, premises, activities, facilities; the use, rental, and right of occupancy, and etcetera.[60]

Despite the very wide-ranging and broad definitions discussed above, the CPA does not apply to everyone or everything. The exemptions to the Act are listed in sections 5(2)(a)-(g) and sections 5(3)-(4) and relate to goods and services promoted to the State where the consumer is an exempt juristic person, transactions exempted by the Minister, credit agreements under the NCA (the CPA does however still apply to the goods and services sold in terms of a such a credit agreement), services under an employment contract, and the provision of education, information, advice, consultations, banking services or related financial services that are regulated under the Financial Advisory and Intermediary Services Act,[61] the Long-term Insurance Act[62] and the Short-term Insurance Act.[63]

Finally, the CPA does not, in general, apply to pre-existing transactions and agreements except to the limited extent set out in item 3 of Schedule 2 to the Act.

57 CPA s1, where consideration also includes cheques, negotiable instruments, credits or debits, electronic chips, labour, barter, coupons, undertakings, promises or agreements.
58 S5(6) also regulates transactions that relate to franchising agreements. It is assumed by the authors that franchise agreements fall outside the typical scope of online consumer law or E-commerce law and, therefore, the provisions directly applicable to franchising have not been included in this discussion.
59 CPA s1.
60 *Ibid*.
61 37 of 2002.
62 52 of 1998.
63 53 of 1998.

3 2 2 Regulation

The CPA has placed a great deal of emphasis on honest, fair and responsible conduct when marketing goods and services.

"Direct marketing" has the following pertinent elements:

- It is an approach to a person;
- either in person or by mail or electronic communication;
- with the direct or indirect purpose of promoting or offering to supply any goods or services;
- in the course of business;
- or to request a donation.[64]

An "electronic communication" for the purposes of "direct marketing" under the CPA is a communication by means of electronic transmission including telephone, fax, sms, wireless computer access, email or similar technology or device.[65]

To regulate direct marketing, section 11 of the CPA sets out the consumer's right to restrict unwanted direct marketing. Regulation 4 of the CPA Regulations sets out the practical rules for controlling direct marketing communications.[66]

In essence, the section relating to the consumer's right to restrict unwanted direct marketing is welcome relief and long overdue. It sets out that a consumer has the right to:

- Refuse to accept;
- require another person to discontinue; or
- pre-emptively block any approach or communication if the approach or communication is primarily for the purpose of direct marketing.[67]

In order to facilitate this, the National Consumer Commission,[68] will establish a registry where a person may register a pre-emptive block against direct marketing communications and any person authorizing, directing or conducting any direct marketing must implement appropriate procedures to facilitate demands to stop further communications.[69]

Once the registry is established, Regulation 4(3)(c), provides that a consumer may register:

64 See CPA s1 for definition of "direct marketing".
65 CPA s1.
66 See GN 293 in GG 34180 1 April 2011.
67 CPA s11(1) (a)-(c)A.
68 Established by CPA s85.
69 *Idem* s11(2)-(4).

(a) his or her name, identification number, passport number, telephone number, facsimile number, email address, postal address, physical address, a website uniform resource locator (URL);

(b) other global address for any website or web application or site on the World Wide Web;

(c) any combination of the media or addresses contemplated in paragraphs (i) and (ii) above;

(d) a pre-emptive block for any time of the day or any day of the year; or

(e) a comprehensive prohibition for any medium of communications, address or time whatsoever in his or her sole discretion, as the factor which triggers the pre-emptive block contemplated in section 11(3) of the CPA.

Most importantly, a direct marketer must, without exception, assume that a comprehensive pre-emptive block has been registered by a consumer unless the administrator of the registry has given written confirmation that the pre-emptive block has not been registered.[70]

Section 32(2) of the CPA contains a dire warning for direct marketers in that, when any person who has marketed goods and left these goods with the consumer without requiring or arranging for payment, those goods become unsolicited goods to which section 21 applies. Section 21 allows consumers under certain circumstances, to keep the goods without an obligation to pay.[71]

3 2 3 Commentary

The CPA's field of application is wider than that of the ECT Act's section 42 in that small to medium-sized juristic persons are protected and no distinction is made between natural persons whether end users or not.

The scope of the CPA's protection granted to consumers differs slightly from the ECT Act's section 45 because, with the CPA, the protection is granted for direct marketing via an electronic communication as well as requests for donations of any kind, whereas the ECT Act relates only to UCE. UCE is arguably slightly wider than just a direct marketing electronic communication.

The consumers' right to restrict unwanted direct marketing and to pre-emptively block any approach or communication if the approach or communication is primarily for the purpose of direct marketing is welcome relief and long overdue.

However, reflecting on the criticisms of section 45 of the ECT Act in paragraph 3.1.3 above, it is clear that a number of issues remain problematic, such as the limitation of the protection to the narrower

70 Reg 4(3)(g).
71 CPA s21.

concept of direct marketing and the fact that the problem of falsified headers is not addressed.

3 3 The Protection of Personal Information Act 4 of 2013

3 3 1 Application

South Africa has enacted its first comprehensive data protection legislation.[72] The PPI Act applies to the processing of personal information entered into a record by or for a responsible party by making use of automated or non-automated means; provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.[73] This Act applies to all public and private bodies.[74]

Of particular importance for the field of application of the Act are the definitions of "processing" and "personal information". Section 1 of the PPI Act defines "personal information" as:

> … information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to – (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

72 Which was first conceived of by the SALRC "Privacy and data protection" Discussion Paper 109, Project 124, available at www.doj.gov.za/salrc (accessed 2013-11-05). Available at http://bit.ly/1bxNLiC (accessed 2013-11-05). The commencement date has to still be announced in the GG.

73 PPI Act s3.

74 PPI Act s1 defines a "*private body*" as "… (a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity; (b) a partnership which carries or has carried on any trade, business or profession; or (c) any former or existing juristic person, but excludes a public body" and a "*public body*" as "… (a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or (b) any other functionary or institution when – (i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or (ii) exercising a public power or performing a public function in terms of any legislation".

Whilst "processing" is designated as any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

> … (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.[75]

Processing is so widely defined that it is clearly intended to cover any action that could possibly be executed in respect of personal information.

However, this Act will not apply to the processing of personal information that is done in the course of a purely personal or household activity; that has been de-identified to the extent that it cannot be re-identified again; processing by or on behalf of a public body for national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information.[76]

The Act is also not applicable where the processing takes place for exclusively journalistic, literary or artistic purposes to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression. Where a responsible party, who processes personal information for exclusively journalistic purposes is, by virtue of office, employment or profession, subject to a code of ethics that provides adequate safeguards for the protection of personal information, such code will apply to the processing concerned to the exclusion of the Act and, any alleged interference with the protection of the personal information of a data subject that may arise as a result of such processing must be adjudicated as provided for in terms of that code.[77]

Finally, the Regulator may exempt a responsible party from the application of the Act if satisfied that in the circumstances of the case, the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could

75 PPI Act s1 definition of "processing".
76 PPI Act s6.
77 *Idem* s7.

result from such processing.[78] The Regulator may however, impose reasonable conditions in respect of any exemption granted.[79]

3 3 2 Regulation

The PPI will repeal and replace amongst others, section 45 of the ECT Act.[80] This section will be replaced with Chapter 8, sections 69–71, setting out the rights of data subjects regarding direct marketing via unsolicited electronic communications, directories and automated decision making.

The PPI Act is an improvement on section 45 of the ECT Act, in-so-far as it prohibits the processing of personal information for direct marketing purposes unless the data subject has given consent to the processing (that is, an opt-in system); or is, subject to subsection (3), a customer of the responsible party.[81]

"Consent" is defined as any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.[82]

In terms of section 69(3), a responsible party may therefore only process the personal information of a data subject who is a customer of the responsible party if the responsible party:

> … (a) has obtained the contact details of the data subject in the context of the sale of a product or service; (b) for the purpose of direct marketing of the responsible party's own similar products or services; and (c) if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details either: (i) at the time when the information was collected; or (ii) on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

Section 69(4) of the PPI Act also requires any communication for direct marketing to contain the details of the identity of the sender or the person on whose behalf the communication has been sent; and an address or other contact details to which the recipient may send a request that such communications cease.

The data subject who is a subscriber to a printed or electronic directory of subscribers that is available to the public or obtainable through

78 *Idem* s37(1). The public interest referred to includes: (a) the interests of national security; (b) the prevention, detection and prosecution of offences; (c) important economic and financial interests of a public body; (d) fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c); (e) historical, statistical or research activity; or (f) the special importance of the interest in freedom of expression.
79 PPI Act s37(3).
80 PPI Act sch..
81 *Idem* s69(1).
82 *Idem* s1.

directory enquiry services, in which his, her or its personal information is included,

> … must be informed, free of charge and before the information is included in the directory –
>
> (a) About the purpose of the directory; and
>
> (b) about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.[83]

The data subject must, furthermore, be given a reasonable opportunity to object to the use of the personal information or to request verification, confirmation or withdrawal of such information if he, she or it has not initially refused such use.[84]

A subscriber is any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services.[85]

On automated decision making, section 71 stipulates that no one may be subject to a decision that has legal consequences, or which affects them to a substantial degree, if it is taken solely on the basis of the automated processing of personal information intended to provide a profile of certain aspects of his or her personality or personal habits such as performance at work, credit worthiness, reliability, location, health, personal preferences or conduct.

The provisions of section 71(1) do not apply if the decision has been taken in connection with the conclusion or execution of a contract and:

- The request of the data subject in terms of the contract has been met;
- appropriate measures have been taken to protect the data subject's legitimate interests; or
- it is governed by a law or code in which appropriate measures are specified for protecting the legitimate interests of data subjects.[86]

The appropriate measures, referred to above must:

---

83 PPI Act s70.

84 PPI Act s70(2), but, in terms of s70(3), ss (1) & (2) do not apply to editions of directories that were produced in printed or off-line electronic form prior to the commencement of this section and in terms of s70(4), if the personal information of data subjects who are subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the information protection principles prior to the commencement of this section, the personal information of such subscribers may remain included in this public directory in its printed or electronic versions, after having received the information required by ss1.

85 PPI Act s70(5).

86 PPI Act s71(2).

- Allow for an opportunity for a data subject to make representations about such a decision; and
- require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her so that representations in this respect can be made.[87]

3 3 3 Commentary

The opt-in model requiring prior consent before sending direct marketing material as adopted by the PPI Act, is definitely an improvement on the ECT Act opt-out model, as are the provisions on directories and automated decision making.

It is noted with disappointment however, that section 69(2) is included in the PPI Act. This section allows a responsible party to approach a data subject once, to request consent for the sending of direct marketing material, provided that consent has not previously been withheld.

This allowance is strongly opposed due to its scope for abuse and because, in essence, it reverts back to an opt-out model. In fact, by allowing a responsible party to process personal information "once" to make the approach to get consent, the prohibition in section 69(1) is reduced to a second level protection mechanism. That is, it only becomes relevant after the approach has been made. It is also contrary to the position established in the CPA where a direct marketer must, without exception, assume that a comprehensive pre-emptive block has been registered by a consumer.[88]

The definitional variances between the ECT Act,[89] the CPA[90] and PPI for electronic communication[91] should be carefully considered and harmonised as far as possible. One example will suffice to illustrate the point. The PPI limits its prohibition on the processing of personal information to an electronic communication for direct marketing in the form of text, voice, sound or image that is sent over an electronic communications network. Direct marketing online may not limit its activities to the sending of text, sound, voice or image. It also includes collecting data through software and cookies which are data files. This sort of processing is also not protected under the automated decision making provisions because they don't necessarily have a legal consequence attached to them. It is therefore suggested that

87 PPI Act s71(3).
88 Reg 4(3)(g).
89 ECT Act s1 "electronic communication" means a communication by means of data messages.
90 CPA s1 where an "electronic communication" means communication by means of electronic transmission, including by telephone, fax, SMS, wireless computer access, email or any similar technology or device.
91 PPI Act s1 where it is any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

the wider CPA or ECT Act definitions which would be sufficiently wide to include actions like data collection via software and the communication of data files be used instead.

A number of the criticisms of section 45 of the ECT Act have also not been adequately addressed in either the PPI or CPA. For example, section 69(4) does not stipulate what, how or where contact details should be displayed for the purposes of requesting a sender to cease sending any further communications. Neither the PPI nor the CPA outlaw the disguising of headers in electronic communications, as is the trend in other jurisdictions. Finally, consideration should be given to extraterritorial reach of national laws.

3 4 The Proposed Draft ECT Act Amendment Bill [2012]

3 4 1 Application

Essentially, the scope of application for the consumer protection provisions of the ECT Act remain unchanged with the exception of a welcome change to the definition of a "consumer" and a clarification on the definition of an "electronic transaction".

The first notable change contained in the ECT Act Amendment Bill is to change the definition of a "consumer" to resemble that in the CPA Act. Thus, in terms of the application of the consumer protection provisions of chapter 7 of the ECT Act, they would protect both natural person consumers and small to medium-sized juristic person consumers whose asset value or annual turnover, at the time of the transaction, is less than the monetary threshold of two million rand, calculated in accordance with the schedule,[92] to whom goods or services are marketed, who have entered into transactions with suppliers in the ordinary course of business of the supplier. It may also include a user, recipient or beneficiary of the goods or services and a franchisee.[93]

The amendment also introduces a definition for an "electronic transaction" which was previously undefined and left open to speculation. This definition confirms and clarifies the application of chapter 7.[94]

92 The determination of threshold in terms of the CPA of 2008 (Act no 68 of 2008) appeared, in the Government Gazette No 34181, GN No 294 on 2011-04-01. The CPA does not apply to a transaction where the consumer is a juristic person, whose annual turnover or asset value, at the time of the transaction, equals or exceeds the monetary threshold of two million rand calculated in accordance with the Schedule to the Regulation.

93 CPA s1 & Van Eeden (2009) 41.

94 An electronic transaction shall mean a transaction conducted using electronic communications.

3 4 2 Regulation

The ECT Act Amendment Bill proposes that section 45 be retained or re-enacted and amended to read as follows:

(1) No person may send unsolicited communications without the permission of the consumer to whom those unsolicited communications are to be sent or are in fact sent.

(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.

(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to a fine not exceeding R1 million or imprisonment for a period not exceeding 1 year.

The ECT Act Amendment Bill also defines an unsolicited communication, in relation to a data message regarding goods or services, to mean that the data message has been transmitted to a consumer by or on behalf of a supplier without the consumer having expressly or implicitly requested that data message.

3 4 3 Commentary

This "new" section 45 proposes to prohibit anyone from sending unsolicited data messages without consent. At first glance, such a wide definition may infringe on the constitutionally protected right to freedom of expression. However, if one reads the definition of "unsolicited communication" it becomes clear that it is only a data message regarding goods and services, which is essentially the same as an UCE, and therefore this does not materially alter the current position.

4 Conclusion

The authors submit that spam and direct marketing online have not been given holistic attention, hence the fragmented approach we find in the ECT Act, CPA, PPI and the ECT Act Amendment Bill. This will result in inadequate protection for consumers and an inability to effectively control spam or regulate online direct marketing.

In trying to enforce the regulatory framework in an online environment the enforcer will have to consider: The different fields of applications for each Act; the different definitions for terms like "electronic communication"; and more importantly, the overlapping and sometimes conflicting web of legislative provisions applicable to direct marketing or unsolicited commercial electronic communications.

While, for the rest, we have to just live with the continuous stream of newsletters, opinion surveys, religious messages, political content, virus warnings and virus hoaxes, urban legends, news, chain letters, hate-mail and any carefully crafted electronic communication that contains

fraudulent or deceptive content that will more than likely fall through the regulatory net as a non-commercial communication.